UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
FACULDADE DE FILOSOFIA E CIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

JUAN BERNARDO MONTOYA-MOGOLLÓN

https://orcid.org/0000-0001-6697-2986

MARÍLIA
2021

JUAN BERNARDO MONTOYA-MOGOLLÓN

Digital Diplomatics and Digital Forensics: Subsides to Ensure Authenticity of Born-Digital Records

Diplomática e Forense Digital: Subsídios para Garantir a Autenticidade de Documentos de Arquivo Natos Digitais

Doctoral Dissertation presented to the *Programa de Pós-Graduação em Ciência da Informação da Faculdade de Filosofia e Ciências* of *Universidade Estadual Paulista Júlio de Mesquita Filho - UNESP* as a requirement for the defense.

Area of concentration: Information, technology and knowledge. Research line 2: Information production and organization.

Advisor: Prof. Sonia Maria Troitiño Rodriguez

MARÍLIA
2021

Juan.mogollon@unesp.br

M798d

Montoya-Mogollón, Juan Bernardo
Digital Diplomatics and Digital Forensics : Subsides to Ensure Authenticity of Born-Digital Records / Juan Bernardo Montoya-Mogollón. -- Marília, 2021
182 p. : il., tabs., fotos

Tese (doutorado) - Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, Marília
Orientadora: Sonia Maria Rodriguez Troitiño

1. Digital Diplomatics. 2. Digital Forensics. 3. Born-Digital Records. 4. Authenticity. 5. Digital Preservation. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Filosofia e Ciências, Marília. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Juan Bernardo Montoya-Mogollón

Digital Diplomatics and Digital Forensics: Subsidies to Ensure Authenticity of Born-Digital Records
Diplomática e Forense Digital: Subsídios para Garantir a Autenticidade de Documentos de Arquivo Natos Digitais

Doctoral Dissertation presented to the *Programa de Pós-Graduação em Ciência da Informação da Faculdade de Filosofia e Ciências* of *Universidade Estadual Paulista Júlio de Mesquita Filho - UNESP* as a requirement for the defense. Area of concentration: Information, technology and knowledge. Research line 2: Information production and organization.

Chair of Supervisory Committee:

_____
Sonia Maria Troitiño Rodriguez, Dra.
Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP)

Reading Committee:

_____
José Augusto Chaves Guimarães, Dr.
Universidade Estadual Paulista (UNESP)

_____
Marcia Cristina de Carvalho Pazin Vitoriano, Dra.
Universidade Estadual Paulista (UNESP)

_____
Daniel Flores, Dr.
Universidade Federal Fluminense (UFF)

_____
José Francisco Guelfi Campos, Dr.
Universidade Federal de Minas Gerais

Marília, SP, 30 de julho de 2021.

For Esperanza Mogollón Rico, Juan Bernardo Montoya Calderón and the rest of family that waited for me for these almost seven years.

ACKNOWLEDGEMENTS

Finally, I am here writing the final words of this work. A work that I can be proud to have arrived at this moment. There was many, many people that made it possible to be here sharing these final thoughts of acknowledgement.

It is tough to name each person that support me through all these seven years of constantly learning, and if I name the people that were part of this process, I would be being unfair because, I would certainly be forgetting someone.

I have to make just one exception to highlight the importance of my supervisor Sonia Troitiño throughout this course. I want to recognize her tireless efforts from the first time that we meet to review this work in 2017, when I was just a forming the project (I still have that drawing with all the annotations and sketches that she kindly made).

The support that I received even started from in my country of birth, Columbia, in the end of the 2014, where it was possible to make the first online admission interview to enter to the the *Programa de Pós-graduação em Ciência da Informação da Faculdade de Filosofia e Ciências* of *Universidade Estadual Paulista Júlio de Mesquita Filho* - UNESP.

Then, I had the opportunity to travel to Brazil and see this amazing country that contributed in my professional life, meanly at the UNESP and their different courses with a new perspective of education, that with all the limitations (as some Brazilians friends often say) is a model of education that should be considered in the other Latin-American countries. When I attended a congress in Londrina, Paraná, I heard professor Mario Barité acknowledge the education of Brazil, mainly at the post graduate level, and to said that this State Policy, in the last 50 years, has made a strong impact, which allows people from other countries to able to study here. I still agree with this comment by professor Barité.

Along with the improvement of the project, I have had the essential resources of the grant #2017/20143-1 and #2018/19129-7, of São Paulo Research Foundation (FAPESP) to continue researching on my doctoral dissertation, along with the scientific articles and presentations in several academic events in different cities and countries. These sorts of experiences were relevant to grow in my personal and professional life.

In 2019, I had the experience that improved my ongoing research at the University of British Columbia – UBC with the Research Internships Abroad – FAPESP resources. I had the great pleasure to meet the most influential academics in Archival Science that provided me academic insights and experiences that guided this current work. In addition to meeting the professionals, I also met colleagues at the Information School at the UBC, international students, and other people with which we could share our culture. That was important to balance my life in an unknown and mystic country.

Upon may return to Brazil in 2020 from Vancouver and I encountered a new scenario of a pandemic disease in the world, that definitely changed my perspective of life. Despite that and with all the limitations that it entails, I could continue with my work and during this year and half, the motivation still remains.

Last but not least, I want to thank the constantly support of Dafnes Moneim Deiab Aly and her family in all this time.

Montoya-Mogollón, J. B. **Digital Diplomatics and Digital Forensics: Subsidies to Ensure Authenticity of Born-Digital Records.** Marilia: 2021. 183f. Tese (Doutorado) Programa de Pós-graduação em Ciência da Informação, Faculdade de Filosofia e Ciências, Universidade Estadual Paulista - UNESP, Marilia, 2021.

RESUMO

Diante das dificuldades que ainda existem ao gerenciar, conservar, preservar e dar acesso aos documentos de arquivo natos digitais, nesta tese de doutorado são abordados os estudos oferecidos pela Diplomática digital e Forense digital, para tentar confrontar esses dilemas. A hipótese fundamenta-se, na possibilidade de aplicar os conceitos dessas duas ciências, ao longo do ciclo de vida dos documentos de arquivo natos digitais, como garantia de autenticidade e preservação. O objetivo geral visa identificar e caracterizar as contribuições oferecidas, tanto pela diplomática como pela forense digital, dentro do contexto arquivístico, administrativo e legal. Aborda-se também, os subsídios teóricos e práticos dessas duas ciências, para que os documentos de arquivo alcancem os suficientes requisitos, como garantia do meio de prova nos diversos contextos em que são requeridos. Do mesmo modo, aprofunda-se na questão da preservação de longo prazo desses documentos digitais, devido à fragilidade dos sistemas onde são armazenados e aos permanentes riscos de obsolescência, tanto de hardware como de software. A aplicação da Diplomática digital auxilia no processo de análise da autenticidade, por meio dos tradicionais elementos externos e internos da forma documental. A Forense digital por sua vez, fornece métodos e ferramentas tecnológicas para que a integridade dos dados se mantenha intacta, com o propósito de ser apresentados em diversos cenários, além dos administrativos e arquivísticos. A metodologia empregada caracteriza-se, por ser de natureza qualitativa com análise teórica, e descritiva-exploratória. Foram analisadas algumas teorias e princípios arquivísticos partindo inicialmente da revisão bibliográfica, para a delimitação do objeto de estudo e o aprimoramento do embasamento científico. Os resultados obtidos nas experiências nacionais e internacionais permitiram estabelecer a possibilidade de vincular e criar uma ciência consolidada, chamada de Diplomática Forense Arquivística Digital, como resposta aos desafios surgidos nestes contextos. A conclusão, dá-se na necessidade de continuar aprofundando nas pesquisas internacionais em andamento, principalmente em relação à Forense digital, a qual está produzindo interessantes respostas na criação, manutenção e preservação de documentos digitais confiáveis.

PALAVRAS-CHAVE: Diplomática Digital. Forense Digital. Documento de Arquivo Nato Digital. Autenticidade. Preservação Digital.

ABSTRACT

In view of the difficulties that still exist in managing, conserving, preserving and giving access to digital archival records, this thesis addresses the studies offered by the Digital Archival Forensics Diplomatics, in an attempt to confront these dilemmas. These studies aim to analyze and discuss the maintenance of authenticity in institutional routines and processes, as well as the potential source of evidence in possible legal and legal scenarios. The hypothesis is based on the possibility of applying the concepts of these two sciences throughout the life cycle of born-digital records, as a guarantee of authenticity and preservation. The general objective is to identify and characterize the contributions offered, both by digital Diplomatics and digital Forensics, within the archival, administrative and legal context. It also addresses the theoretical and practical subsidies of these two sciences, so that records meet the sufficient requirements, as a guarantee of the means of proof in the different contexts in which they are required. Likewise, in the long-term preservation of these digital records, due to the fragility of the systems where they are stored and the permanent risks of obsolescence, both in hardware and software. The application of digital Diplomatics supports in the authenticity analysis process through the traditional external and internal elements of the documentary form. Digital Forensics, in turn, provides technological methods and tools so that the integrity of data remains intact, with the purpose of being presented in different scenarios, in addition to archival or administrative ones. The methodology used is characterized by being qualitative in nature with theoretical analysis, and descriptive-exploratory. Some archival theories and principles were analyzed, starting initially from the bibliographical review, for the delimitation of the study object and the improvement of the scientific basis. The results obtained in national and international experiences allowed establishing the possibility of linking and creating a consolidated science, called Digital Archival Forensic Diplomatics, as a response to the challenges arising in these contexts. The conclusion arises from the need to continue deepening the ongoing international research, especially in relation to digital Forensics, which is producing interesting answers in the creation, maintenance and preservation of reliable digital records.

KEYWORDS: Digital Diplomatics. Digital Forensics. Born-Digital Records. Authenticity. Digital Preservation.

RESUMEN

Ante las dificultades que aún existen al gerenciar, conservar, preservar y dar acceso a los documentos de archivo nacidos digitales, en esta tesis de doctorado son abordados los estudios ofrecidos por la Diplomática digital y la Forense digital, para intentar enfrentar esos dilemas. La hipótesis es fundamentada en la posibilidad de aplicar los conceptos de esas dos ciencias mencionadas, a lo largo de del ciclo de vida de los documentos de archivo nacidos digitales, como garantía de autenticidad y preservación. El objetivo general es construido para poder identificar y caracterizar las contribuciones dentro del contexto archivístico, administrativo y legal. También, se aborda los subsidios teóricos y prácticos ofrecidos, para que los documentos de archivo alcancen los suficientes requisitos como subsidio para la garantía del medio de prueba en los diversos contextos donde son requeridos. Estos estudios tienen como objetivo analizar y verificar la autenticidad en las rutinas y procesos institucionales, así como la examinación de fuente de prueba en posibles escenarios jurídicos y legales. Igualmente, en la preservación a largo plazo de esos documentos digitales, debido a la fragilidad en los sistemas donde son almacenados y a los permanentes riesgos de obsolescencia, tanto de hardware como de software. La aplicación de la Ciencia Diplomática digital ayuda en el proceso de análisis de la autenticidad por medio de los tradicionales elementos externos e internos de la forma documental. Del mismo modo, se profundiza en la cuestión de la preservación a largo plazo de esos documentos digitales, debido a la fragilidad de los sistemas donde se encuentran almacenados y a los permanentes riesgos de obsolescencia tanto de hardware como de software. La aplicación de la Diplomática digital auxilia en el proceso de análisis de autenticidad por medio de los tradicionales elementos externos e internos de la forma documental. La forense digital por otro lado, ofrece métodos y herramientas tecnológicas para que la integridad de los datos se mantenga intacta, con el propósito de que sean presentados en diversos escenarios, además de los administrativos y archivísticos. La metodología aplicada se caracteriza por ser de naturaleza cualitativa con análisis teórica, y descriptiva-exploratoria. Fueron analizadas algunas teorías y principios archivísticos partiendo inicialmente de revisión bibliográfica para la delimitación del objeto de estudio y mejoramiento de la base científica. Los resultados obtenidos en las experiencias nacionales e internacionales permitieron proponer la creación de una Diplomática Forense Archivística Digital, como respuesta a los desafíos surgidos en estos contextos. La conclusión a la que se llegó, se coloca en la necesidad de continuar profundizando en las investigaciones internacionales, principalmente en relación con la Forense digital, la cual está produciendo interesantes caminos en la creación y conservación y preservación de documentos digitales confiables.

PALABRAS CLAVE: Diplomática Digital. Forense Digital. Documento de Archivo Nacido Digital. Autenticidad. Preservación Digital.

LIST OF ILLUSTRATIONS

LIST OF FIGURES

LIST OF IMAGES

LIST OF TABLES

SUMMARY

1 INTRODUÇÃO

A motivação deste trabalho de doutorado começou no ano de 2012, na atuação de projetos de tratamento documental na empresa *Iron Mountain*[1]. O cargo exercido era o de técnico de gestão documental, no qual era realizado projetos de levantamento e aplicação de tabelas de temporalidade e de planos de classificação, em entidades privadas. As dificuldades enfrentadas nesses anos eram a falta de interesse por parte de alguns colaboradores, quando era abordado o tema gestão documental no interior da organização, e a posterior transferência dos documentos físicos para o armazenamento nas próprias instalações da *Iron Mountain*.

Outro problema que se colocava era o de analisar os documentos digitais armazenados em diferentes plataformas digitais. Nos projetos de gestão documental realizados, era necessário realizar entrevistas com os funcionários das empresas para avaliar os documentos produto das atividades administrativas. Nessa etapa de entrevistas era necessário insistir na questão desses documentos digitais, já que alguns desses funcionários não os consideravam como um formato relevante. Segundo eles, esses registros eram mais fáceis de gerenciar nos sistemas tecnológicos da própria organização ou na nuvem (*cloud computing)*, além de não gerar problemas de espaço físico comparados aos documentos em papel. Essa situação não era diferente no âmbito público.

Em 2015, se deu início o mestrado em Ciência da Informação na Universidade Estadual Paulista “Júlio de Mesquita Filho”, em Marília, Brasil. O interesse em aprofundar nas complexidades do documento de arquivo nato digital (também conhecido como de arquivo nascido digital ou documento arquivístico digital)[2] começou a ser cada vez mais latente e nesse estudo foi

[1] *Iron Mountain Incorporated (NYSE: IRM)* é uma empresa global dedicada a armazenar, proteger e gerenciar informações e ativos. Para maiores informações, ver: https://www.ironmountain.com.br/about-us

[2] Esta última definição encontra-se no Glossário do Conselho Nacional de Arquivos -CONARQ e a Câmara Técnica de Documentos Eletrônicos – CTDE: “Documento Arquivístico Digital: Documento digital reconhecido e tratado como um documento arquivístico” (CONARQ; CTDE, 2015, p.21). Não entanto, esse conceito é definido de forma genérica pelo CONARQ. Deste modo, para os propósitos desta tese é usado uma definição mais próxima das práticas

analisado, como esses documentos digitais eram gerenciados no contexto organizacional.

Na dissertação de mestrado, “A emergência de uma “adequada” produção e organização de documentos arquivísticos digitais em organizações” (MONTOYA-MOGOLLÓN, 2017), foi desenvolvido um estudo sobre os documentos de arquivo natos digitais em organizações privadas, com o propósito de proteger e perpetuar a memória organizacional e institucional[3]. O propósito da dissertação foi elaborar um estudo que estabelecera boas práticas na criação, conservação, preservação, acesso e uso, desses documentos nos ambientes mencionados.

A presente pesquisa de doutorado continua com o estudo dos documentos de arquivo digitais, em especial, com os documentos natos digitais, isto é, documentos produzidos e gerenciados nos sistemas ou repositórios digitais. Neste processo analisa-se a possibilidade de verificar a completude, confiabilidade e autenticidade desses documentos, tanto em relação às rotinas administrativas, quanto aos seus nos contextos legais, já que se entende que ainda existem dificuldades na admissibilidade do suporte digital. Para abordar o problema em questão, foi necessário vincular os estudos da Diplomática digital e à Forense digital, como ciências centrais que tentam subsidiar elementos de análise para atingir a autenticidade nos diferentes contextos em que os documentos digitais são administrados.

Desse modo, é necessário primeiro destacar a discussão entorno da Diplomática digital: “[...] um estudo contemporâneo de uma ciência secular que analisa a natureza, gênese, características formais, estrutura, transmissão e consequências legais dos documentos de arquivo [...]” (DURANTI, 2010, p.109, tradução nossa)[4], para determinar sua autenticidade. Com o estudo da Diplomática digital, o quesito da autenticidade é analisado através de dois elementos necessários: integridade e identidade. A integridade refere-se à completude e solidez do documento para que não seja modificado e/ou

arquivísticas por meio do termo “documento de arquivo nato ou nascido digital”.

[3] Repositório institucional em que se encontra armazenado o trabalho acadêmico: https://repositorio.unesp.br/handle/11449/149809

[4] *[…] Digital Diplomatics, a contemporary development of a centuries-old discipline that studies the nature, genesis, formal characteristics, structure, transmission and legal consequences of records […]* (DURANTI, 2010, p.109).

corrompido de forma mal-intencionada. A identidade refere-se aos atributos dos documentos que os caracteriza e distingue de outros documentos.

Devido a seu caminho histórico e contribuição para outras ciências, a Diplomática tem tido um lugar notável dentro da Arquivologia desde a segunda metade do século 20. É destacável a adaptação da Diplomática desde o século 17, dado que criou uma metamorfose que iniciou no estudo da autenticidade dos próprios documentos diplomáticos, definidos por Juan Carlos Galende Díaz e Marciano García Ruipérez (2003, p.21, tradução nossa), como uma

> testemunha escrita que tem, ao mesmo tempo, um caráter histórico-jurídico, uma forma de redação determinada e não está destinado diretamente a dar fé da veracidade de um fato ou de constituir uma prova dele mesmo, mas antes garantir, a adequada transmissão de um fato, de uma mensagem, de uma vontade..., conforme sua natureza e à categoria exigida pela administração ou pela lei[5].

Quando analisado a definição do documento no campo jurídico, ele tem uma acepção diferente do caráter diplomático. Neste sentido, o documento jurídico é "[...] qualquer testemunha escrita, legalmente válido, destinado para ser prova jurídica de um fato (GALENDE-DÍAZ; GARCÍA-RUIPÉREZ, 2003, P.22, tradução nossa). [...]"[6]. Complementando a anterior definição, Sylvio do Amaral (1978, p.2), destaca que "[...] a noção de documento, para efeitos jurídicos, é restringida à peça escrita que condensa graficamente o pensamento de alguém[...]".

Por último, quando é analisado o documento no âmbito da arquivística, ele é definido como "um documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência" (CONARQ, 2020, p.24). Essas três definições escritas anteriormente são relevantes para entender como cada umas das ciências caraterizadas aqui trabalham com o conceito de documento.

Com as três categorias descritas é possível analisar como a Diplomática na atualidade, em grande parte se volta para três correntes e usos: 1. A

---

[5] *Es un testimonio escrito que tiene, a la vez, un carácter histórico-jurídico, una forma de redacción determinada y no está destinado directamente a dar fe de la veracidad de un hecho o constituir una prueba del mismo sino más bien a garantizar la adecuada transmisión de un hecho, de un mensaje, de una voluntad..., conforme a su naturaleza y a la categoría exigida por la administración o por la ley* (Galende-Díaz; García-Ruipérez, 2003, p.21).

[6] "[…] *Se considera* ***documento jurídico*** *cualquier testimonio escrito, legalmente válido, destinado a ser prueba jurídica de un hecho* […]" (Galende-Díaz; García-Ruipérez, 2003, p.22).

Diplomática Arquivística, como é reconhecida nos estudos canadenses da Luciana Duranti e seu grupo *International Research on Permanent Authentic Records in Electronic Systems* - InterPARES, em que a Diplomática usa os elementos clássicos como apoio nas atividades arquivísticas; 2. A Diplomática Contemporânea, caracterizada como uma transição (ou "evolução") da Diplomática clássica, e algumas vezes relacionada com, 3. A Tipologia Documental, um modelo inovador surgido na Espanha e aprofundado desde os anos 80 nas atividades arquivísticas no Brasil.

Desta forma, o uso da Tipologia Documental vem sendo integrada no contexto brasileiro, por conta de uma melhor adaptação nos processos arquivísticos, ao ultrapassar o estudo interno do documento e, "[..] agregando ao seu objeto o estudo de componentes relativos ao conjunto orgânico [...] (TROITIÑO, 2010, p.85). Esses estudos são discutidos e aprofundados por autores como, Vicenta Cortés Alonso (1986), Antonia Heredia-Herrera (1991), Ana Maria Camargo (2000), Heloísa Bellotto (2002; 2004), Ana Celia Rodrigues (2008), Marcia Pazin (2011) e Sonia Maria Troitiño (2012), entre outros.

Para o propósito desta tese, foi escolhido o conceito de Diplomática digital, já que por meio desta denominação é possível estabelecer um diálogo abrangente entre as ciências analisadas (a Diplomática e a Forense), além de valorizar os estudos nacionais e internacionais em andamento. No entanto, sem desconhecer os avanços que a Tipologia Documental tem atingido nos estudos arquivísticos no Brasil.

Feito a delimitação da Diplomática, passa-se a estudar a contribuição fornecida pela Forense digital. Uma ciência constituída por elementos da Ciência da Computação e do Direito. O caráter computacional permite analisar métodos de verificação da prova digital assegurando a integridade dos dados e da cadeia de custódia. A contribuição do Direito por outra parte, confere suficientes elementos legais para que os documentos digitais possam ser admissíveis como prova no âmbito da lei.

Assim, a abordagem dos documentos digitais por parte dos peritos forenses determina algumas vantagens, uma vez que este suporte necessita da confiança na integridade dos dados nos diferentes cenários que são requeridos. A contribuição da Forense digital estabelece mecanismos na verificação de autenticidade de documentos nesse suporte digital. A estrutura

teórica e prática que está fornecendo esses estudos, permite analisar a natureza e composição dos documentos digitais e, além disso, dos sistemas e repositórios onde eles são gerenciados.

Os estudos da Forense digital estão contribuindo para as pesquisas arquivísticas em países como Estados Unidos, Canadá e Inglaterra. Sua interação com as abordagens da Diplomática digital, em específico, no decorrer das fases do projeto científico do *International Research on Permanent Authentic Records in Electronic Systems* - InterPARES[7] e do *Digital Records Forensics Project* - DRFP[8], estão gerando interessantes subsídios para a área da Arquivologia.

Além dos projetos mencionados acima, destaca-se a produção de outros estudos acadêmicos e científicos no final do século 20, como por exemplo o *"Recordkeeping Functional Requirements Project"*[9] (1993-1996), liderado por Richard J. Cox e James Williams, e desenvolvido na Escola de Ciência da Informação da Universidade de Pittsburgh. Este projeto ofereceu, profícuos resultados de pesquisas, em relação com o gerenciamento e preservação dos documentos digitais. O tempo de execução desse projeto foi consideravelmente menor (três anos), em relação ao projeto de InterPARES. Não obstante, foi um dos projetos fundacionais no relacionado ao estudo de documentos eletrônicos, como foram denominados na década de 1980 e 1990.

As pesquisas da Universidade de Pittsburgh estabeleceram certa similaridade às do projeto do InterPARES, em relação ao quesito da preservação. O projeto de Pittsburgh por exemplo, além de focar seus estudos no próprio documento digital, chamava a atenção para preservar seus metadados como atividade suprema, para garantir a autenticidade tanto nas rotinas administrativas como de preservação. Para isso, destacavam seus autores, devia existir uma adequada criação e manutenção dos documentos digitais, os quais deviam cumprir uma série de requisitos, como por exemplo,

---

[7] Para maiores informações, ver: http://www.interpares.org/

[8] Para maiores informações, ver: http://www.digitalrecordsforensics.org/#:~:text=The%20Digital%20Records%20Forensics%20(DRF,of%20the%20Vancouver%20Police%20Department

[9] Para maiores informações, ver: https://web.archive.org/web/19991218001620/http://www.sis.pitt.edu/~nhprc/Pub1.html

ser abrangentes, identificáveis (delimitados), completos (determinados no seu conteúdo, estrutura e contexto), e autorizados (BEARMAN; SOCHATS, 1996).

Por outro lado, destaca-se também algumas diferenças entre os dois projetos mencionados. O projeto InterPARES centrava seus estudos nos próprios documentos de arquivo e seus atributos, enquanto o da Universidade de Pittsburgh*,* além de considerar a natureza interna do documento, chamava a atenção nos requisitos funcionais para estabelecer um correto gerenciamento arquivístico como prova das transações administrativas. Da mesma forma, sua preservação a longo prazo. Como destacado por Alf Erlandsson (1996), existia outra marcada diferença entre os dois projetos:

> A maior diferença entre os dois projetos é a visão que se tem na custódia a longo prazo dos documentos eletrônicos. Enquanto o projeto de Pittsburgh conclui que os documentos eletrônicos podem ser melhor mantidos ao longo do tempo pelos órgãos de origem, mas sob controle estrito das autoridades de arquivo, o projeto da UBC deixa clara a distinção entre documentos correntes/semicorrentes e documentos inativos, e conclui que a autenticidade pode apenas ser garantida quando os documentos inativos estão sob uma custódia independente por arquivistas, em uma instituição de arquivo (p.45, tradução nossa) [10].

Segundo os estudos do projeto de Pittsburgh, os documentos digitais são prova (*evidence*) de transações, e por esse motivo devem ser gerenciados adequadamente desde sua própria criação. Devem servir como provas dessas transações. Na perspectiva do projeto InterPARES, a questão da prova como atributo dos documentos não aparece tão visível, pelo menos nos seus primeiros anos de análise.

Assim, o projeto de Pittsburgh respeitava a tradição do ciclo de vida documental e a separação dos documentos por fases. No entanto, estavam interessados conjuntamente, nos resultados das pesquisas na Austrália relacionadas ao projeto do modelo contínuo fundado por Peter J. Scott e desenvolvido por Frank Upward, Sue McKemmish, e os colegas da faculdade de Monash (ERLANDSSON, 1996). O modelo do *Records continuum* é um

---

[10] *The most fundamental difference between the two projects is, however, their view on the long-term custodianship of electronic records. While the Pittsburgh projects concludes that electronic records can best be maintained over time by the originating body but under strict control from the archival authorities, the UBC project makes a clear distinction between the current/semicurrent records and inactive records and concludes that authenticity can only be guaranteed when the inactive records are under independent custodianship by professional archivists in an archival institution.* (ERLANDSSON, 1996, p.45).

interessante estudo, que determina a continuidade do documento de arquivo sem fases ou ciclo de vida determinados previamente. Seus autores ressaltam que os documentos já nascem com um valor histórico, e esse valor não pode ser dado no processo da avaliação documental (ERLANDSSON, 1996).

Embora seja considerado a relevância dos estudos desenvolvidos pelos projetos da Universidade *de* Pittsburgh, do *Records Continuum* e outros modelos de colaboração científica, que contribua com um ideal gerenciamento, conservação, preservação e uso dos documentos de arquivo nato digitais, este estudo toma como base teórica em especial, as pesquisas desenvolvidas no projeto InterPARES. Entretanto, em determinados momentos, são abordados outros projetos acadêmicos que aprimoram a discussão sobre documentos digitais.

Desta forma, para delimitar o campo de estudo é necessário entender a definição dos documentos de arquivo natos digitais. O projeto InterPARES 3, (2007-2012, tradução nossa) em seu glossário, define esses documentos como "aqueles documentos que deixaram de ser analisados, como acontecia no suporte analógico, primeiro, pela sua forma fixa"[11], isto é, a qualidade do documento para manter o escrito completo e sem alterações. Segundo, pelo seu conteúdo estável, que determina que o documento digital de arquivo "[...] deve manter sempre a mesma apresentação que tinha quando foi "salvo" pela primeira vez [...]" (RONDINELLI, 2011, p.227).

A forma fixa e conteúdo estável são complementados com elementos arquivísticos, tais como: 1) o vínculo arquivístico, a relação que cada documento de arquivo estabelece com outros documentos; 2) o contexto identificável, isto é, a ação no qual o documento de arquivo participa: jurídico-administrativo, de proveniência, procedimental, documental e/ou tecnológico. Alf Erlandsson (1996), define essa também essa questão do contexto como as circunstâncias de criação; e, 3) as pessoas envolvidas na ação ou criação desse documento (MACNEIL, 2002; DURANTI; THIBODEAU, 2006; RONDINELLI, 2011; TOGNOLI, 2014).

Embora alguns autores usem o termo "documento eletrônico" como sinônimo de "documento digital" (RONDINELLI, 2007; JIMENE, 2010;

---

[11] *Fixed form: n., The quality of a record that ensures its content remains complete and unaltered.* (INTERPARES 3, 2007-2012).

MARTINS, 2015), decidiu-se adotar o de “documento digital” como termo preferencial, por acreditar que este se adaptar melhor a este problema de pesquisa. Assim, foi empregado a definição de documento digital de Rogers (2015, p.11): “aquele documento que se encontra codificado em dígitos binários ou em valores de zeros e uns”. Por outro lado, a definição de documento eletrônico é mais abrangente. Ele é: [...] qualquer documento analógico ou digital que é transportado por um condutor elétrico e requer o uso de equipamentos eletrônicos para ser entendido por uma pessoa (por exemplo, uma máquina fax) [...] (DURANTI, 2009, p. 44, tradução nossa)[12]. Rosely Curi Rondinelli (2011, p.226), esclarece melhor essa diferença:

> Assim, segundo a Câmara Técnica de Documentos Eletrônicos (2011), documento eletrônico é um “documento codificado em forma analógica ou em dígitos binários, acessível por meio de um equipamento eletrônico.” Em outras palavras, pode-se dizer que todo documento digital é eletrônico, mas nem todo documento eletrônico é digital. Um exemplo seria uma fita cassete cujo som, embora necessite de um equipamento eletrônico para ser ouvido, não se apresenta codificado em bits.

Portanto, a proposta desta pesquisa de doutorado é estudar os conceitos teóricos estabelecidos pela Diplomática digital e pela Forense digital e determinar, como esses conceitos contribuem para garantir a completude, confiabilidade e autenticidade, nos documentos de arquivo natos digitais, desde o momento da sua criação, até seu acesso e/ou recuperação. Para isso, se trabalhou conjuntamente com outras ciências que complementam, as duas anteriormente mencionadas, as quais analisam a importância do documento digital, para dar maior riqueza acadêmica ao problema de pesquisa.

São elas: 1) A Arquivologia, que é a principal área de atuação e contribui na produção e organização dos documentos de arquivo sem deixar de lado o aspecto tecnológico; 2) A Diplomática digital, que analisa a forma e conteúdo dos documentos digitais nessa busca pela autenticidade; 3) A Forense digital, que junta o conhecimento da Ciência da Computação e do Direito; 4) A Ciência da Informação, que dá relevância na informação nos diferentes contextos em que ela se manifesta; 5) O Direito, que é uma ciência que fornece elementos

[12] *[…] In contrast to a digitally encoded representation of an object or physical process, an analogue representation resembles the original. InterPARES defines an electronic record as any analogue or digital record that is carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person (e.g., a fax) [...]* (DURANTI, 2009, p. 44*).*

legais, tanto para a Diplomática como para a Forense, dentro do sistema jurídico determinado; e por último, 6) A História, como uma ciência transversal para entender as bases fundacionais e epistemológicas das ciências abordadas na nossa pesquisa acadêmica.

1.1 IDENTIFICAÇÃO DO PROBLEMA DA PESQUISA, HIPÓTESES E OBJETIVOS

partindo do pressuposto de que por meio da Diplomática digital e da Forense digital é possível verificar a autenticidade dos documentos de arquivo natos digitais, desde a criação até sua recuperação e acesso, a questão central a resolver neste estudo de doutorado é, de que forma a junção das duas ciências mencionadas podem verificar a autenticidade no suporte digital?

Destaca-se a sobrevivência da Diplomática pela sua versatilidade e adaptação nos últimos três séculos de história, assim como ter fornecido elementos de análise para outras áreas do conhecimento. Observa-se no curso histórico da Diplomática, um caminho produtivo estabelecido particularmente em três momentos significativos.

Primeiro, na fundação da própria ciência quando foi publicado o tratado, *"De re diplomatica libri VI"* de Dom Jean Mabillon (1681*)* – erudito que analisou os elementos internos e externos da forma documental para verificar a autenticidade dos documentos solenes, chamados de diplomas. Segundo, na junção da Diplomática e da Arquivologia em meados do século 20, que consolidou e ampliou o conceito diplomático de autenticidade por meio dos elementos da forma documental, junto a três princípios: 1. o respeito aos fundos ("*respect des fonds*"). Segundo Michel Duchein (1983, p.72, tradução nossa): [...] Os fundos estão constituídos por documentos criados por uma entidade no curso das suas atividades, qualquer que seja seu objeto [...][13]; 2. a organicidade, a qual é a relação estabelecida entre os documentos; e, 3. o

[13] […] *The fonds is made up of all the papers created by an agency in the course of its activities, whatever their object* […] (DUCHEIN, 1983, p.72). A consideração deste autor é relevante já que em alguns países o princípio de respeito aos fundos e proveniência são considerados sinônimos, como aparece por exemplo, no glossário arquivístico de Richard Pearce-Moses (2005, p.317). Neste caso, Duchein explica a função de cada conceito e suas marcadas divergências.

contexto arquivístico, isto é, o contexto no qual o documento é gerado e gerenciado.

Terceiro, na articulação da Diplomática digital com a Forense digital. Uma relação já acontecida na fundação da Diplomática de Mabillon. A "*Diplomática Forense*" surgiu, segundo Manuel Romero-Tallafigo (1994), quando a Diplomática superou seu sentido antiquário e medievalista e entrou no mundo jurídico. No entanto, desde o próprio título do tratado de Mabillon é lido essa questão do forense ("*Forensemque*")[14], o qual se encontra no decorrer desse texto junto com outros termos similares, como por exemplo *"Forensibus"* (tribunais) (MABILLON, 1681, p.257). Ambos os termos estão relacionados com esse sentido jurídico apontado por Romero-Tallafigo.

No decorrer da história, essa proximidade entre a Diplomática e a Forense foi se desvanecendo, da mesma forma que foi se afastando de outras ciências. Já no século 20, a Diplomática adquire relevância nas práticas administrativas e arquivísticas, ao se consolidar definitivamente no campo da Arquivologia, como é colocado por Robert Henri-Bautier (1961). No final do mesmo século, o paradigma digital colocou novos desafios para a Diplomática, devido principalmente, na necessidade de analisar a composição interna dos documentos digitais, com o objetivo de ser gerenciados nos processos administrativos e arquivísticos. No início dos anos 2000, a Forense digital entrou em cena para fornecer elementos de análise e complementar os estudos dessa Diplomática digital.

Levando em consideração o escrito acima, a Diplomática foi redefinida como subsídio para fins arquivísticos no final do século 20, com o propósito de acompanhar as complexidades emergidas no documento digital. No século 21, a Forense digital, está sendo empregada por parte dos arquivistas, como uma ciência que estabelece no seu *corpus* teórico, a ciência da Computação e o Direito. Isto possibilita categorias de análise para assegurar e melhorar em primeiro lugar, a integridade e autenticidade do documento digital, além dos

---

[14] Título completo do tratado: *De re diplomatica libri vi. in quibus quidquid ad veterum instrumentorum antiquitatem, materiam, scripturam, & stilum: quidquid ad sigilla, monogrammata, subscriptiones, ae notas chronologicas; quidquid inde ad antiquariam, historicam,* ***forensemque*** *disciplinam pertinet, explicatur & illustratur/Accedvnt Commentarius de antiquis regum Francorum palatiis. Veterum scripturarum varia specimina, tabulis LX comprehensa. Nova ducentorum, & amplius, monumentorum collectio. Operā & studio domni Johannis Mabillon, Presbyteri ac Monachi Ordinis S. Benedicti è Congregatione S. Mauri*.

sistemas tecnológicos em que são gerenciados esses documentos, e a garantia de que seja admissível como prova em diversos cenários: técnicos, administrativos, arquivísticos, e legais, entre outros.

Quando se analisa cada ciência de forma isolada é possível estudar, com maior clareza, a função que cada uma estabelece dentro do domínio arquivístico. A Diplomática digital, por um lado, visa analisar a forma documental por meio dos elementos externos e internos, as anotações feitas nos documentos, o meio em que a informação é fixada e o contexto em que o documento participa. Por outro lado, a Forense digital analisa a composição do documento digital mantem a integridade dos fluxos de bits, estabelece a cadeia de custódia e assegura a autenticidade no processo de criação e gerenciamento no contexto arquivístico.

Assim, os pressupostos estabelecidos nesta pesquisa de doutorado estão baseados na possibilidade de vincular a Diplomática digital e a Forense digital, como subsidio na verificação de autenticidade dos documentos de arquivo natos digitais, tanto para seus objetivos arquivísticos, como para ser apresentados em outros contextos que sejam requeridos.

Portanto, baseado na hipótese de que as metodologias advindas tanto da Diplomática digital como da Forense digital fornecem elementos de análise para garantir a autenticidade do documento de arquivo nato digital e sua preservação no tempo, o objetivo geral desta tese visa identificar e caracterizar as contribuições oferecidas por essas duas ciências dentro do contexto arquivístico, administrativo e legal e sua articulação para o estabelecimento da autenticidade do documento de arquivo nato digital. Do mesmo modo, é analisado os subsídios teóricos e práticos gerados por estas duas ciências, para que os documentos de arquivo garantam os suficientes requisitos como subsidio para a garantia do meio de prova, nos diversos contextos em que são requeridos.

Seguido do objetivo geral descrito, os objetivos específicos estão relacionados com cada um dos capítulos que foram desenvolvidos nesta tese, os quais estão elencados da seguinte forma:

- Estudar os elementos que compõem o documento de arquivo nato digital;

- aprofundar no papel da Diplomática e da Forense como um processo histórico e epistemológico, até a abordagem do documento de arquivo nato digital;
- analisar os conceitos teóricos e práticos da Diplomática digital e da Forense Digital, para mapear como as duas ciências podem servir de subsídio para as latentes dificuldades que se apresentam na Arquivologia no ambiente digital;
- abordar a definição de autenticidade como um conceito central dentro da Diplomática digital, da Forense digital e da Arquivologia

Desta forma, o primeiro objetivo se encontra descrito no segundo capítulo, o qual concentra a importância do documento de arquivo nato digital. Seu gerenciamento, preservação, acesso e/ou uso, como elemento essencial dentro das práticas arquivísticas. O segundo objetivo se enquadra nos capítulos que correspondem na função e atuação dos estudos da Diplomática e da Forense, respectivamente. O terceiro objetivo estabelece uma relação próxima com o anterior objetivo, estendendo sua análise no contexto digital. O quarto objetivo é relevante ao ser aplicado de forma transversal na tese, perpassando os limites de verificação de autenticidade, para atingir a fidedignidade (completude, confiabilidade e autenticidade) documental.

1.2 JUSTIFICATIVA DA PESQUISA

Nesta complexidade do mundo digital se faz necessário de ciências que agreguem elementos para enfrentar dificuldades relacionadas à preservação da nossa memória digital. Além do alto risco de perda de informações digitais em poucos anos, a fragilidade dos registros digitais faz com que as informações sejam modificadas de forma consciente ou inconsciente. Isso pode gerar problemas de proteção de dados[15], transparência, responsabilidade, entre outras.

Como escrito no começo deste capítulo, é preciso analisar as dificuldades para gerenciar documentos de arquivo natos digitais e os sistemas

[15] Quando há problemas com a integridade dos dados, existe o grande risco de vulnerar direitos cidadãos. Um exemplo disto, aconteceu na Colômbia em 2021, quando foram publicadas informações privadas de imigrantes por parte do "*Ministerio de Relaciones Exteriores"* desse país: https://lasillavacia.com/bache-seguridad-amenazo-los-datos-extranjeros-y-cancilleria-no-sabia-79749

e repositórios onde esses documentos estão armazenados. Estudos voltados para a Diplomática digital e a Forense digital oferecem interessantes respostas na busca por estabelecer ideais documentos digitais. Esses estudos são relevantes porque ainda existem incertezas de como organizar os documentos digitais que se encontram armazenados em: 1) computadores e/ou sistemas digitais que contêm declarações humanas; 2) em computadores e/ou sistemas digitais que não contêm declarações humanas, feitos com o *output* de um programa informático, configurado para processar dados seguindo um algoritmo predefinido; e, 3) em documentos armazenados e gerados em computadores, os quais são uma combinação dos dois primeiros processos mencionados (DURANTI; THIBODEAU, 2006).

Outro ponto considerado enquanto justificativa, foi a relevância de outros de estudos inovadores, como foi observado no *1st International Caparica Conference in Translational Forensics*[16] em Caparica-Portugal. Nesse evento acadêmico, foi percebido um número de pesquisas aplicadas principalmente em estudos forenses das áreas tradicionais: Medicina, Biologia, Justiça, Criminologia, Redes Sociais e Psicologia. A contribuição do trabalho apresentado, discutiu os estudos em andamento da Diplomática e Forense digital como contribuição para a Arquivologia, o qual se mostrou pioneiro para esse evento, no que diz respeito à criação e ao tratamento de documentos burocráticos e administrativos (MONTOYA-MOGOLLÓN; TROITIÑO, 2018).

Com esse tipo de experiências acadêmicas referenciadas anteriormente e a literatura científica, continua-se com a possibilidade de vincular a Diplomática digital e a Forense digital, para reforçar a questão de autenticidade nos documentos de arquivo natos digitais. As pesquisas nestas duas ciências estão produzindo significativos resultados em países da América do Norte, o que torna necessária a discussão e vinculação com países no contexto latino-americano. A justificativa deste trabalho, então, é fundamentada na realização de uma pesquisa que contribui com estudos acerca dos documentos digitais colaborando para que eles sejam completos, confiáveis e autênticos, dentro de um sistema igualmente confiável a longo prazo.

[16] Em: https://www.bioscopegroup.org/wp-content/uploads/2020/03/FORENSICS2017.pdf

1.3 METODOLOGIA DA PESQUISA

Este trabalho de doutorado é caracterizado por ser de natureza qualitativa com análise teórica, e caráter descritivo-exploratório. Foram analisadas algumas teorias e princípios arquivísticos, partindo inicialmente da revisão bibliográfica para a delimitação do objeto de estudo e aprimoramento do embasamento científico. Posteriormente, organizou-se a compilação dos dados obtidos na revisão bibliográfica com o propósito de apresentar os resultados da discussão teórica, para então, responder questões relacionadas com a aplicação da Diplomática digital e da Forense digital, no documento de arquivo nato digital. Essas duas ciências foram analisadas e entendidas no contexto da Arquivologia e da Ciência da Informação, para verificar como são utilizadas para o assunto da autenticidade.

O levantamento bibliográfico sobre os temas investigados foi realizado, principalmente, a partir de três fontes de pesquisa:

1. O acervo bibliográfico de bibliotecas nacionais e internacionais. Dentre as nacionais, se deu início na biblioteca da Universidade Estadual Paulista – UNESP, que tem convênios virtuais e físicos com uma rede de bibliotecas estaduais como, por exemplo, a Universidade de São Paulo – USP e a Universidade Estadual de Campinas – UNICAMP, entre outras; e as municipais, com o acervo bibliográfico da Biblioteca da Universidade de Marília – UNIMAR e a biblioteca do Centro Universitário Eurípides de Marília – UNIVEM. Entre as bibliotecas internacionais foi explorado o acervo bibliográfico da rede de bibliotecas da Universidade da Colúmbia Britânica – UBC, em Vancouver, Canadá.

2. Os portais de pesquisa e bases de dados nacionais e internacionais, como a Base de Dados Referenciais de Artigos em Periódicos em Ciência da Informação – BRAPCI, *Scientific Electronic Library Online - SciELO Brasil*, *Web of Science, SCOPUS, Library and Information Science Abstracts – LISA,* que a própria UNESP tem convênios para que seus pesquisadores tenham acesso gratuito dentro da universidade ou em qualquer outro lugar do mundo por meio da *Virtual Private Network* – V.P.N. *(*Rede Virtual Privada) e o *Eduroam (Education roaming),* iniciativa da comunidade internacional de educação para

que os pesquisadores tenham acesso às redes *wifi* das universidades dentro e fora do país.

3. A literatura publicada nas páginas de internet do projeto da *International Research on Permanent Authentic Records in Electronic Systems – IntePARES (*1999-2018*)*, a qual fornece a produção científica da Arquivologia, e o *Digital Records Forensics Project* (2008-2011), o qual conserva e disponibiliza a literatura científica nas temáticas que são abordadas nesse projeto, entre as quais estão: Bibliografia da Diplomática Arquivística, Bibliografia Jurídica, e Bibliografia da Forense digital (tradução nossa)[17].

Desse terceiro ponto, destaca-se a experiência acadêmica internacional realizada no ano 2019 na Universidade da Colúmbia Britânica - UBC, por meio dos recursos econômicos da FAPESP, através da Bolsa de Estágio de Pesquisa no Exterior- BEPE. Nesse intercâmbio acadêmico, foi essencial o acompanhamento acadêmico dos professores e pesquisadores da Escola de Informação da UBC, entre os quais se destacam, as contribuições de Luciana Duranti e Corinne Rogers. As experiências acadêmicas vivenciadas na UBC como estudante internacional permitiu confrontar algumas hipóteses, em especial, em relação com a Forense digital e sua possível adaptação nos processos arquivísticos no Brasil.

Como resultado das experiências acadêmicas nacionais e internacionais, aliada ao desenvolvimento do projeto em questão, foi elaborada uma tese com o objetivo de contribuir para os desafios no gerenciamento e preservação do documento de arquivo nato digital. Para tanto, o trabalho foi estruturado em seis capítulos que discutem os elementos discutidos anteriormente: o uso da Diplomática e Forense digital como subsídio para a análise nos documentos de arquivo natos digitais.

Assim, no primeiro capítulo se detalha a parte introdutória e os limites do presente estudo de doutorado. Nessa mesma seção foi exposta os problemas da pesquisa, as hipóteses, o objetivo geral e os objetivos específicos, a justificativa e, por fim, a metodologia.

---

[17] Para maiores informações, ver: *Archival Diplomatics Bibliography, Legal Bibliography, Digital Forensics Bibliography (DRFP, 2008-2011).:* http://www.digitalrecordsforensics.org/drf_biblio_db.cfm

No segundo capítulo se discute sobre a complexidade do documento de arquivo nato digital. Analisa-se a definição desse conceito e suas diferenças com outros termos como, dados e informação. Da mesma forma, a questão dos metadados como atributos essenciais desses documentos digitais, mantidos em cada fase do ciclo de vida. A verificação de autenticidade e preservação a longo prazo por meio da cadeia de custódia e de preservação, em repositórios arquivísticos que garantam essa autenticidade.

No decorrer da pesquisa destaca-se o quesito da autenticidade como um elemento primordial. Precisamente esse conceito de autenticidade é abordado de forma transversal desde o segundo capítulo, com o intuito de analisar sua importância nos documentos digitais e a forma como ela deve ser complementada com os conceitos de completude e confiabilidade, com o intuito de alcançar a almejada fidedignidade nos processos arquivísticos.

Após refletir e discutir sobre o documento de arquivo nato digital, no terceiro capítulo é elaborado um estudo relacionado com a construção histórica e consolidação da Diplomática. A fim de compreender a natureza de uma ciência que verifica o quesito da autenticidade nos documentos de arquivo, é discutido os primórdios da própria ciência e a figura histórica do seu fundador, Jean Mabillon. É explicado, de que forma o trabalho de Mabillon contribuiu para vincular em séculos posteriores, a História e a Arquivologia. Destaca-se com o anterior, a pertinência desse processo de historicização da Diplomática, para entender a sua relação com os documentos de arquivo, tanto no estabelecimento da crítica histórica como também na construção dos elementos essenciais das práticas diplomáticas.

É necessário destacar que neste capítulo três, se contextualiza também, sua importância para a Arquivologia no século 20. Do mesmo modo, como essa construção histórica pode ser entendida no século 21, na atuação da proposta Diplomática Forense Arquivística Digital - DFAD.

Feito a contextualização da Diplomática e sua adaptação na realidade digital, se passa a refletir no quarto capítulo, sobre a importância da Forense digital e sua contribuição para a Diplomática digital. Aborda-se a Forense de forma similar à feita na Diplomática desde seu processo fundacional, para observar a “evolução” e a forma como esses estudos analisam os problemas dos documentos de arquivo natos digitais. No decorrer deste capítulo são

explorados os principais conceitos construídos no núcleo da ciência: as Ciências Computacionais e o Direito. Como ponto final, são analisadas as complexidades da Forense digital e sua incorporação na Diplomática digital, entendendo algumas barreiras que devem ser superadas, entre elas, alguns conceitos similares, porém com aplicações diferentes.

Com a visão geral dos quatro capítulos abordados, explora-se, no quinto capítulo, a incorporação da DFAD nas atividades relacionadas com os documentos de arquivo natos digitais. Para isso, é discutido os conceitos estabelecidos em cada uma das ciências abordadas, suas restrições e possibilidades na nossa atualidade e realidade.

No sexto capítulo se dão as conclusões da tese, e por fim, as referências usadas.

Deste modo, com a construção dos capítulos mencionados é possível abordar de forma abrangente, a proposta da criação da DFAD[18]. Portanto, pretende-se abordar os problemas surgidos com administração de documentos de arquivo natos digitais e subsidiar possíveis soluções aos dilemas surgidos dentro da Arquivologia no contexto digital. É importante ressaltar, que já existem alguns estudos sobre a Forense digital trabalhados no Brasil, porém, ainda são escassos, estudos que vinculem a Forense com a Arquivologia.

[18] Houve inicialmente uma aproximação por parte de Luciana Duranti (2009, p.40), ao propor a Forense Digital de Documentos de Arquivo (*Digital Records Forensics*). No entanto, acredita-se que é preciso continuar aprimorando o nome de forma mais abrangente. O anterior, com o objetivo de criar um diálogo entre as três ciências exploradas nesta tese. Desse modo, a justificativa de nomeá-la como “Diplomática Forense Arquivística Digital – DFAD”, corresponde a uma contextualização nos processos arquivísticos brasileiros, visto que empregar as ciências de forma isolada, principalmente a Forense digital, pode gerar certas ambuiguidades, por acreditar que seja um estudo voltado para áreas diferentes da Arquivologia.

1 INTRODUCTION

The motivation for approaching this doctoral research started in the year 2012 at an international company called Iron Mountain[19]. The position was a technician in records management, on projects related to records retention and disposal schedules. The main issue faced at that time was the lack of interest in records, from the administrative workers, especially related to born-digital records management. Documental interviews with the staff about digital records elucidated that most employees did not talk of this sort of digital support because they thought that traditional or paper records approach was more important.

Another problem that arose was that of analyzing digital documents stored on different digital platforms. In the document management projects carried out, interviews had to be conduct with company employees to evaluate the documents resulting from administrative activities. At this stage of interviews, it was necessary to insist on the issue of these digital documents, as some employees did not consider them to be a relevant format. According to them, these records were easier to manage in the organization's own technological systems or in the cloud (cloud computing), to not generating physical space problems compared to paper documents. This situation was no different in the public sphere.

The master's degree in Information Science at São Paulo State University in Marília sparked interest in delving into the complexities of born-digital records. The objective was to analyze how digital records are managed in the organizational context.

The master´s thesis, "The Emergence of a "Appropriate" Production and Organization of Digital Records in Corporations"[20]. included a study that

---

[19]"Iron Mountain Incorporated (NYSE: IRM) is a global business dedicated to storing, protecting, and managing, information and assets". At: https://www.ironmountain.ca/en/about-us

[20] Master's thesis*: A emergência de uma "adequada" produção e organização de documentos arquivísticos digitais em organizações. Available at: https://repositorio.unesp.br/handle/11449/149809*.

discussed the creating, production, and organization of digital records in private corporations and their preservation to guarantee organizational, institutional, and social memory. The purpose was to apply best practices in the creation, maintaining, preservation, access, and use of digital records in that environment.

This doctorate research continues with the research about the nature of digital records mainly with born-digital records, documents created in and by digital systems. This process analyzed the possibility to investigate their accuracy, reliability, and authenticity in the stewardship routines as well as in legal and legal contexts, because some difficulties remain in the admissibility of digital records, due to their lack of trustworthiness as reliable records. To try to approach this problem, research in Diplomatics and Forensics studies will be the central knowledge areas, which can ensure the trustworthiness in any context.

Thus, it is necessary to highlight the discussion around the digital Diplomatics, “a contemporary development of a century-old discipline that studies the nature, genesis, formals characteristics, structure, transmission, and legal consequences of records” (DURANTI, 2010, p.109), to verify their authenticity. With digital Diplomatics, the issue of authenticity continues to be the most relevant principle with two necessary elements: integrity and identity. Integrity refers to the completeness and soundness of the record, without being corrupted or modified in a malicious form. The identity refers to the attributes of the records characterized and distinguished from other records.

Due to its historic path and its contribution to a series of disciplines, Diplomatics has had a notable place in Archival Science, primarily, in the second half of the 20th century. The adaptation of Diplomatics is worth exploring beginning in the 17th century, given that it created a metamorphosis that began in the study of the authenticity of diplomatics documents themselves, defined by Juan Carlos Galende Díaz and Marciano García Ruipérez (2003, p.21, our translation), as,

> […] a written testimony that has, at the same time, a historical-juridical character, a determined form of writing and is not intended directly to confirm the veracity of a right or to constitute a principle of the same, but more likely to guarantee the proper transmission of a person, of a message, of a

> volunteer..., according to its nature and the category required by the administration or by Law (GALENDE-DÍAZ; GARCÍA-RUIPÉREZ, 2003, p.21, our translation)[21].

However, when analyzing the definition of the record in the legal field, it has a different meaning from the diplomatic character. In this sense, the legal document is [...] any written witness, legally valid, intended to be legal evidence of a fact [...] (GALENDE-DÍAZ; GARCÍA-RUIPÉREZ, 2003, p.22, our translation). Complementing the previous definition, Sylvio do Amaral (1978, p.2, our translation) highlights that "[...] the notion of record, for legal purposes, is restricted to the written piece that graphically condenses someone's thought [...]"[22].

Finally, when the record is analyzed in the context of Archival Science, it is defined as "a record produced (prepared or received), in the course of a practical activity, as an instrument or result of such activity, and retained for action or reference" (CONARQ, 2020, p.24)[23]. These three definitions written above are relevant, because it is necessary to understand how each of the sciences characterized here work the concept of record.

The three described categories are possible to analyze how Diplomatics is currently used in three uses: 1. Archival-Diplomatics as referenced in Canadian studies by Luciana Duranti and her International Research on Permanent Authentic Records in Electronic Systems Project– InterPARES, which applies the classic elements as support to Archival activities; 2. Contemporary Diplomatics, characterized as a transition (or "evolution") Classic Diplomatics and sometimes related to 3. Documentary Typology, a innovate model created in Spain, and explored in Brazil in the 1980s.

Therefore, the use of Documentary Typology has been integrated in the Brazilian context for a better adaptation in the archival processes, when surpassing the analysis of the internal document and, "[…] adding to the object

[21] […] *un testimonio escrito que tiene, a la vez, un carácter histórico-jurídico, una forma de redacción determinada y no está destinado directamente a dar fe de la veracidad de un hecho o constituir una prueba del mismo sino más bien a garantizar la adecuada transmisión de un hecho, de un mensaje, de una voluntad..., conforme a su naturaleza y a la categoría exigida por la administración o por la ley* (GALENDE-DÍAZ; GARCÍA-RUIPÉREZ, 2003, p.21).

[22] "[...] *a noção de documento, para efeitos jurídicos, é restringida à peça escrita que condensa graficamente o pensamento de alguém* [...]" (AMARAL, 1978, p.2).

[23] "*Um documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência*" (CONARQ, 2020, p.24)

of study, components related to the organically set […] (TROITIÑO, 2012, p.85, our translation)[24]. These studies are discussed and explored by authors, such as Vicenta Cortés Alonso (1986), Antonia Heredia-Herrera (1991), Ana Maria Camargo (2000), Heloísa Bellotto (2002; 2004), Ana Celia Rodrigues (2008), Marcia Pazin (2011), and Sonia Maria Troitiño (2012).

For the purpose of this doctoral dissertation, the name digital Diplomatics was chosen, since this name could establish a broad dialogue between Diplomatics and Forensics, as well as valuing the ongoing national and international research. However, the advances that Documentary Typology reach in Brazilian Archival Science is not ignored.

On the other hand, the objective of digital Forensics is to develop methods for verification of digital evidence, by ensuring data integrity and chain of custody, through applying forensics tools. This science shares elements from Computer Science and Law. For this reason, digital Forensics might perform the data analysis within the framework of the Law.

Thus, the approach to born-digital records by Forensics creates a series of advantages, because this sort of support needs to trust in the data integrity in the various scenarios. Thus, the contributions of digital Forensics are relevant to establish a threshold that fits the born-digital records. The theoretic and practical framework provided by this field of knowledge allows analysis of the nature and composition of digital records, in addition to the digital systems where they are managed.

Digital Forensics is not a new science, with many studies in countries like the United States, Canada, and England. The interaction with Diplomatics, especially during the phases of the scientific of The International Research on Permanent Authentic Records in Electronic Systems project– InterPARES[25], and the Digital Records Forensics Project – DRFP, is producing interesting outcomes for Archival studies.

Along with the projects above mentioned, the production of other scientific projects in the end of the 20th century includes the “Recordkeeping

[24] “[...] *agregando ao seu objeto o estudo de componentes relativos ao conjunto orgânico* [...]”(TROITIÑO, 2010, p.85).

[25] http://www.interpares.org/

http://www.digitalrecordsforensics.org/#:~:text=The%20Digital%20Records%20Forensics%20(DRF,of%20the%20Vancouver%20Police%20Department

Functional Requirements Project (1993-1996)"[26] led by Richard J. Cox and James Williams and developed at the School of Information at the University of Pittsburgh. This project provided interesting research results related to the management and preservation of digital records. The runtime was considerable shorter (three years) compared to the InterPARES project. However, it was one of the foundational projects about the study of electronics records, as it was called in the 1980s and 1990s.

The research at the University of Pittsburgh established several similarities to InterPARES, mainly in the question of preservation. The Pittsburg project for example, in addition to investigating in the digital record itself, focused its research on preserving its metadata as supreme activity to assure authenticity of both the administrative and preservation routines. For this, the authors explained that there should be an adequate creation and maintenance of digital records, which have to comply a series of requirements, such as, being comprehensive, identifiable (bounded), complete (containing content, structure, and context), and authorized (BEARMAN; SOCHATS, 1996, p.3).

On the other hand, differences exist between the two mentioned projects. The InterPARES project focuses on the research in the digital records itself and their attributes. On the other hand, the Pittsburgh project, besides considering the internal nature of digital records, emphasized in the functional requirements to establish proper records management as evidence of administrative transactions. as well as the long-term preservation. Alf Erlandsson (1996, p.45) explained another relevant difference between the two projects:

> The most fundamental difference between the two projects is, however, their view on the long-term custodianship of electronic records. While the Pittsburgh projects concludes that electronic records can best be maintained over time by the originating body but under strict control from the archival authorities, the UBC project makes a clear distinction between the current/semicurrent records and inactive records and concludes that authenticity can only be guaranteed when the inactive records are under independent custodianship by professional archivists in an archival institution.

According to the research of Pittsburg project, the digital records are evidence of transactions and for this reason should be properly managed from their creation. Digital records should be useful as evidence of those

[26] https://web.archive.org/web/19991218001620/http://www.sis.pitt.edu/~nhprc/Pub1.html

transactions. From the perspective of the InterPARES project, this point is not clear, at the least in the first years of research.

The Pittsburg project respected the tradition of the documentary cycle of life and the separation of records by phases. However, they were also interested in the outcomes of research in Australia related with the Model Continuum project, founded by Peter J. Scott and developed by Frank Upward, Sue McKemmish, and the colleagues at the Faculty of Monash (ERLANDSSON, 1996). The Records Continuum Model is an alternative project, which determines the continuity of record without previously determined phases or life cycle. The authors explain that the records are created with a historical value, and this value cannot be given in the record assessment process (ERLANDSSON, 1996).

While still considered the importance of these sort of studies developed for the University of Pittsburg, Records Continuum, and other projects with scientific foundations, that contribute to an ideal management, maintenance, and preservation of born-digital records, this doctoral dissertation uses as its scientific base, especially, the research developed by the InterPARES project. However, sometimes other kinds of academic projects will be addressed to improve the discussion around digital records.

Thus, to delimitate the study object of this work, it is necessary to define “born-digital records”. InterPARES 3 project (2007-2012) in its glossary defines these as records “which is no longer analyzed exclusively by the fixed form[27] (as happened in the analogic context)”. The quality of a record must ensure that its content remains complete and unaltered. The content much remains stable, either unchangeable or changeable according to fixed rules, that is, endowed with bounded variability (INTERPARES 3, 2007-2012); and […] must always maintain the same presentation as it had when it was first “saved” […] (RONDINELLI, 2011, p.227)[28].

These elements are accompanied by other characteristics considered from the foundations by Diplomatics to verify the authenticity in the digital

---

[27] *Fixed form: n., The quality of a record that ensures its content remains complete and unaltered.* (INTERPARES 3, 2007-2012).

[28] “[...] *deve manter sempre a mesma apresentação que tinha quando foi “salvo” pela primeira vez* [...]” (RONDINELLI, 2011, p.227).

environment, such as: 1) archival bond (the network of relationships that each record has with the records belonging in the same archival aggregation); 2) identifiable context (defined as the action in which the record participates) (MACNEIL, 2000; MACNEIL, 2002; DURANTI; THIBODEAU, 2006; RONDINELLI, 2011; TOGNOLI, 2014). According to Heather MacNeil (2000, p.95), the context refers to:

> […] The final component of a record is its context, which refers to the framework of action in which the record participates. Four contexts are relevant to non-electronic and electronic records alike: the juridical-administrative context (i.e., the legal and organisational system in which the creating body belongs), the provenancial/context (i.e., the creating body, its mandate, structure, and functions), the procedural/context (i.e., the procedure in the course of which the record is generated), and the documentary context (i.e., the internal structure of the archival fonds of which the record forms apart). This last context represents the totality of all the archival bonds existing within a creator's fonds. While it is clearly impossible for any single record to fully communicate these contexts, it is possible to provide clues and pointers to them through the other identified components. For example, the name of the creator (identified under persons) is a pointer to the record's provenancial context; an annotation, such as the classification code (identified under archival bond), is a kind of shorthand for the record's administrative, procedural and documentary context.

Ultimately, 3) the people involved in the action or creation of the record (MACNEIL, 2002; DURANTI; THIBODEAU, 2006; RONDINELLI, 2011; TOGNOLI, 2014).

Although some research uses the term “electronic record” as a synonym of a “digital record”, this dissertation uses the second term because it is more adaptable and used in the explored research problem. “Digital record” meanings the encoding in binary digits or in values of zeros and ones. The electronic records, on the other hand, is more comprehensive defined as: “[…] as any analog or digital record that is carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person (e.g., a fax*)* […]”

(DURANTI, 2010, p. 44). Rosely Curi Rondinelli (2011, p.226, our translation) [29] clarifies this idea:

> […] According to The Technical Chamber of Electronic Records (2010), the electronic record is a record codified in "analog form or in binary digits". In other words, it is possible to say that every digital record is an electronic record, but not every electronic record is a digital record. For instance, the cassette tapes whose sound needs electronic equipment to be heard is not codified in bits.

Therefore, the purpose of this doctoral dissertation is to study the theoretical concepts established by digital Diplomatics and Forensics and determine how these concepts help to guarantee the accuracy, reliability, and authenticity in born-digital records, from their creation, until their access and recovery. For this, other sciences are explored that complemented, the two mentioned sciences, which analyzed the relevance of digital record intended to provide a high academic value to the research problem.

The relevant sciences are: 1. Archival Science, because it is a science that supports the production of records and their organization, without losing sight of the technological usefulness; 2. Digital Diplomatics, because it analyzes the form and content of the digital record in the pursuit of its authenticity; 3. Digital Forensics, because it is an area that joins Forensics and Computational Science to analyze the digital source of evidence; 4. Information Science, for providing relevance to the information in their different contexts; 5. Law, as a contribution of the concepts and elements to Archival Diplomatics activities, and their importance within systems of law; and 6. History, which will be important to understand the foundational background of each science discussed here and their epistemological elements.

---

[29] *Assim, segundo a Câmara Técnica de Documentos Eletrônicos (2011), documento eletrônico é um "documento codificado em forma analógica ou em dígitos binários, acessível por meio de um equipamento eletrônico." Em outras palavras, pode-se dizer que todo documento digital é eletrônico mas nem todo documento eletrônico é digital. Um exemplo seria uma fita cassete cujo som, embora necessite de um equipamento eletrônico para ser ouvido, não se apresenta codificado em bits* (RONDINELLI, 2011, p.226).

1.1 IDENTIFICATION OF THE RESEARCH PROBLEMS, HYPOTHESIS, AND OBJECTIVES

Assuming that through digital Diplomatics and digital Forensics it is possible to verify the authenticity of born-digital records, from their creation to their retrieval and access, the central question to be resolved in this doctoral study is how to the combination of the two sciences mentioned can verify the authenticity of the digital support?

The versatility of Diplomatics highlights not only how it has survived and adapted in its more than three centuries of history but also how it provides core elements to other knowledge areas. The history of Diplomatics includes a productive pathway in three huge periods.

First, its foundation was in the 17th century when Don Jean Mabillon wrote his famous treatise*, "De re diplomatica libri VI"* (1681*)*. By establishing the internal and external elements to obtain the authenticity of formal documents, called diplomas. Second, Diplomatics join with Archival Science in the 20th century, by consolidating and broadening the diplomatic concept of authenticity with the foundational elements of documentary form, along with three principles: 1) the "*respect des* fonds". According to Michel Duchein (1983, p.72), "[…] *The fonds is made up of all the papers created by an agency in the course of its activities, whatever their object* […]"; 2) The organically relationship, which is the relationship with other records; and finally, 3) the archival contexts, which is the context where it is created and managed.

Third, in the articulation of digital Diplomatics to digital Forensics, a relationship already happened in the foundation with the Diplomatics of Mabillon. The "*Forensics* Diplomatics" arose according to Manuel Romero-Tallafigo (1994), when Diplomatics surpassed the antiquarian and medievalist sense and started to perform in juridical contexts. However, the title of Mabillon's treatise contains the Latin word "*Forensemque*"[30], which could be

[30] Full title of the treatise*: De re diplomatica libri vi. in quibus quidquid ad veterum instrumentorum antiquitatem, materiam, scripturam, & stilum: quidquid ad sigilla, monogrammata, subscriptiones, ae notas chronologicas; quidquid inde ad antiquariam, historicam, forensemque disciplinam pertinet, explicatur & illustratur / Accedvnt Commentarius de antiquis regum Francorum palatiis. Veterum scripturarum varia specimina, tabulis LX comprehensa. Nova ducentorum, & amplius, monumentorum collectio. Operā & studio domni Johannis Mabillon, Presbyteri ac Monachi Ordinis S. Benedicti è Congregatione S. Mauri.*

related to that mentioned juridical element, along with other similar terms, such as "*Forensibus*" (courts) (MABILLON, 1681, p.257).

In the course of history, the proximity between Diplomatics and Forensics, was vanishing, the same way that it was separating from other sciences. In the 20th century, Diplomatics acquires relevance in new administrative and archival practices, consolidating in the field of Archival Science, as stated by Robert Henri-Bautier (1961). In the end of that century, the digital paradigm placed new challenges for Diplomatics, mainly in the necessity to analyze the internal composition of digital records, intended to be managed in the administrative and archival processes. In the beginning of 21st century, digital Forensics entered the scene to provide analysis elements and to complement the studies of digital Diplomatics.

Taking in account the above, Diplomatics studies were redefined as support to Archival purposes in the end of 20th century, with the objective to accompany the complexities of digital record. In the 21st century, digital Forensics is being performed by archivists, as a science that establishes in its theoretical core, Computer Science and Law. That allows analysis categories to assure and improve first the integrity and authenticity of digital records, in addition to the technological systems, where the records are managed, and guarantee admissibility as evidence in various contexts: technical, administrative, archival, and legal.

Thus, the assumptions established in this doctoral research are based on the possibility of linking Digital Diplomatics and Digital Forensics, as a subsidy in verifying the authenticity of born-digital records, both for their archival purposes and for being presented in other contexts that are required.

Second, the consolidation to join Diplomatics with Forensics is proposed to construct a unified science called, "Digital Archival Forensics Diplomatics - DAFD" [31].Therefore, the intention is to address the issues arising with the born-digital records management and to provide possible solutions to these issues

[31] There was initially an approximation by Duranti (2009, p.40) to call this science such as "Digital Records Forensics". However, it is possible to continue to improve the search for a more encompassing definition, with the intention to create a fruitful dialogue among the three sciences here analyzed. Therefore, the justification to name this science as DAFD, corresponds to contextualize the Brazilian Archival processes. For this reason, it was necessary first to individualized the study of each science and then, to unify and assemble each science into a unified science, with the objective of avoiding ambiguities if just individual sciences are analyzed without connections.

established in Archival Science in this digital era. While some research related with digital Forensics already exists, this sort of studies connected to Archival Science are scarce.

Each science will be analyzed individually to clarify the function that each science establishes in the Archival domain. On the one hand, digital Diplomatics aims to analyze the documentary form by the extrinsic and intrinsic elements, the annotations made on records, the support which the information is fixed, and the context in which the record participates. On the other hand, digital Forensics analyzes the internal composition of the digital record, maintains the integrity of bitstreams, establishes the chain of custody, and assures the authenticity in the creation and management process of the Archival context. Thereby, the formation of DAFD reinforces their theoretical and practices grounds in the ascertaining of born-digital records, along with the technological systems of management and preservation.

Thus, based on the hypothesis that the methodologies arising from both digital Diplomatics and Forensics provide elements of analysis to ensure the authenticity of the born-digital record and its preservation over time, the general objective of this dissertation aims to identify and characterize the contributions offered by these two sciences within the archival, administrative, and legal context and its articulation for the establishment of the authenticity of the born-digital record. Likewise, the theoretical and practical foundations created by these two sciences are analyzed, so that digital records are guaranteed to have the sufficient requirements as evidence, in any context which they be required.

Following the general objective described, the specifics objectives are related to each one of chapters developed in this doctoral dissertation, which are listed thus:

- Study the elements that compose born-digital records.
- Explore in the role of Diplomatics and Forensics as a historical and epistemological process, until the approaching of the born-digital record.
- Analyze the theoretical and practical concepts of digital Diplomatics and Forensics to map how both sciences can be useful to the latent difficulties that are presented in Archival Science in the digital context.
- Address the definition of authenticity as a central concept in Diplomatics, Forensics, and Archival Science.

Therefore, the first objective is placed in the second chapter, which concentrates the relevance of the born-digital record. Its management, preservation, access, and/or use, as foremost element within the archival practices. The second objective is placed in the third and fourth chapter that correspond to the functions and performs studies of Diplomatics and Forensics, respectively. The third objective establishes a relation with the previous objective, extending the analyze to the digital domain. The fourth objective about authenticity is applied in a transversal manner in this doctoral dissertation, surpassing the bounds of authenticity verification to reach documentary trustworthiness (accuracy, reliability and authenticity).

1.2 RESEARCH JUSTIFICATION

In this complexity of the digital world is necessary of sciences that add elements to tackle the difficulties related to the preservation of our digital memory. In addition to the high risk of losing the digital information in few years, the fragility of digital records leads to the information being modified conscious or unconsciously. This can generate issues with data protection[32], transparency, accountability, etc.

As written in the beginning of this chapter, it is necessary to analyze the difficulties in the of management born-digital records, the systems, and the repositories where these records are storage. Sciences such as digital Diplomatics and Forensics offer some contributions to achieve this goal. They are relevant because uncertainties remain about how to organize digital records, such as 1) records stored on computers, which contain human statements; 2) records generated on computers, which do not contain human statements and are made with the output of a computer program configured to process data following a predefined algorithm; and 3) records stored and generated on computers, which are a combination of the first two (DURANTI; THIBODEAU, 2006).

Another interesting aspect considered as justification was the importance of other innovative studies, as was observed in the First International Caparica

[32] An example of this took places in Colombia in 2021, where privacy information of immigrants was published by the Colombian Ministry of Foreign Affairs: https://lasillavacia.com/bache-seguridad-amenazo-los-datos-extranjeros-y-cancilleria-no-sabia-79749

Conference in Translational Forensics in Caparica, Portugal[33]. In that academic event, a large percentage of applied research in Forensics studies were from traditional areas such as Medical Forensics, Biology, Criminology, Legal, Virtual Social Networks, and Psychology Forensics. At that place, an innovative work was presented in which digital Forensic is already contributing to areas such as Archives, specifically for bureaucratic or administrative records (MONTOYA-MOGOLLÓN; TROITIÑO, 2018).

This sort of referenced academic experiences and scientific literatures elucidates the possibility to link digital Diplomatics and Forensics to ascertain the authenticity of born-digital records. The justification for this work is based on the need for research that contributes to the studies about digital records, to help make them authentic, reliable, and complete, within an equally reliable system over the long term.

1.3 RESEARCH METHODOLOGY

This research has a qualitative theoretical and descriptive-exploratory type nature, starting from the bibliographic research to define the study topic and improve the scientific base. Subsequently, the compilation of the data obtained in the bibliographic review was analyzed. To present the results of the theoretical discussion, questions related to the application of digital Diplomatics and digital Forensic in born-digital records will be analyzed. The two sciences must be analyzed and understood in the context of the Archival and Information Science, to verify the authenticity and reliability of born-digital records. The bibliographic survey on the topics investigated came mainly from three research sources:

1. Bibliographical collection from national and international libraries. The national libraries include São Paulo State University, in Marilia (UNESP), which has online and physical agreements with state libraries networks such as the University of Sao Paulo – (USP), Campinas State University (UNICAMP) and the Federal University of São Carlos (UFSCAr). Municipal university libraries such as the Marilia University (UNIMAR) and the Marilia University Center

[33] In: https://www.bioscopegroup.org/wp-content/uploads/2020/03/FORENSICS2017.pdf

Euripides (UNIVEM) were also searched. The main international library consulted was the bibliographic collection at the University of British Columbia – UBC library network[34].

2. The explored research portals and national and international databases include the *Base de Dados Referenciais de Artigos em Periódicos em Ciência da Informação* (BRAPCI); Scientific Electronic Library Online - SciELO Brazil; Web of Science; SCOPUS; Library and Information Science Abstracts - LISA. These databases have agreements with UNESP through the Virtual Private Network (VPN) and the Eduroam (Education Roaming), both at the University and abroad.

3. Literature is available on the website of International Research on Permanent Authentic Records in Electronic Systems – InterPARES (1999-2018), which publishes scientific production related to Archival Science. The Digital Records Forensics Project – DRFP (2008-2011) provides scientific literature related to the areas explored in this doctoral dissertation, among which are: “Archival Diplomatics Bibliography, Legal Bibliography, and Digital Forensics Bibliography” (DIGITALRECORDSFORENSICSPROJECT, 2021).

This third item was possible due to studies performed at the University of British Columbia – UBC, in 2019, due to the scholarship for an international academic experience grant from the São Paulo Research Foundation – FAPESP. The motivation to research at the UBC School of Information was due to their ongoing research, related to digital Diplomatics and digital Forensics, along with the scholars that belong to the institution, especially professors Luciana Duranti and Corinne Rogers.

The international gathered experiences at the UBC as a Visiting International Research Student (VIRS) in 2019 helped enhance some hypotheses of the doctoral project, especially concerning the digital Forensics and how to adapt it to Brazilian Archival processes.

As a result of the national and international experiences previously outlined, the intentions of this work are to intended to develop a work that continues to help improve the born-digital records issues, a source of trustworthiness, able to be preserved over time and sufficiently reliable in

[34] UBC Library: http://www.library.ubc.ca/.

different legal systems. The work is structured in six chapters that analyze the complexities of the born-digital record.

The first chapter outlines the introduction and the boundaries of this research. This section describes the constraints and affordances of the study, the research problems, the hypothesis, the general and specific objectives, the justification, and the methodology.

The second chapter discusses the complexity of born-digital records and defines born-digital records. The definition of this concept is analyzed as well as its differences with other terms, such as data and information. The importance of metadata as relevant attributes of these digital records that must be keep in the documentary cycle of life is explored. The relevance of chain of custody and preservation, the role of trusted repositories, and, their maintenance and preservation over the time is analyzed.

During the research, the issue of authenticity stands out as a key element. The concept of authenticity is addressed in a traverse manner from the second chapter, with the objective to analyze its relevance in digital records and the form it should be complemented with the concepts of accuracy and reliability, with the aim to achieve the desired trustworthiness in the Archival processes.

The third chapter is a study about Diplomatics since its foundation until the present. This chapter analyzes the importance of Dom Jean Mabillon as an archivist and historian as well in the establishment of the historical criticism and the essential elements of diplomatic practices, and how his work helped to link the Archival Science and History. This chapter also discussed the importance of the digital Diplomatics to approach the born-digital records. This third chapter contextualizes the relevance of Diplomatics studies to Archival Science in the 20th century as well as how this historical framing can be understood in the 21st century, in performing DAFD.

After the contextualization of Diplomatics and its integration to the digital domain, the fourth chapter discusses the relevance of Forensics and its contribution to Diplomatics. Forensics is addressed in a similar form to Diplomatics, from its foundational process to observe its “evolution” and the form that these studies analyze the difficulties of born-digital records. This chapter explores the main concepts and sciences built in the core of Forensics:

Computer Science and Law. Finally, the complexities were discussed of digital Forensics and the incorporation to Diplomatics, understanding some barriers that need to be overcome, among them, some similar concepts but with different uses.

With the overview of the previous four chapters covered, the fifth chapter analyzes the possible incorporation of DAFD in the activities related with born-digital records. Here, the concepts established in each science are discussed. The constraints and affordances in the current and national reality.

The sixth chapter outlines the conclusions of this doctoral dissertation and the seven chapter lists the references used.

2 BORN-DIGITAL RECORDS

> […] It is unlikely that the authors of any of these statements mean that “records” and "evidence" are synonyms, in the way that (for example) “water” and “H_2O” have identical meanings. When evidence is required, whether by a judge, and historian, or anyone else, other things besides records can be abduced. In court, a blood-stained weapon or a piece of DNA may provide evidence, as may oral testimony. Patterns in the soil provide archaeologist with evidence of human habitation; observation of birds supplied evidence for Darwinian theory of evolution. Evidence can be found in architecture, landscape, urban topography, and museum objects. None of these are records as archivists and records managers normally understand them. (YEO, 2007, p. 320).

As written in the introduction chapter, the digital record definition was chosen instead of electronic record, as some other researchers have used (BEARMAN, 1993; COOK, 1992; 2007; ROBERTS, 1994; ERLANDSSON, 1996; HEDSTROM, 1997). The justification to use the digital records definition is that this term fits better this research proposal, understanding the term digital as the evolution that started when electronic systems created electronic records, which were called, until in the mid-1990s, machine readable records (DURANTI, 2019, s.3). As electronic systems work through electrical pulses that produce digital records encoded in bit formats of zeros and ones (0s and 1s) (ROGERS, 2016, p.35), the term digital records began to be used in the decade 2000.

With this view, the meaning of “record” in archival matters and its difference from document, information, and data will be elucidated. To do this, three research perspectives will be explored that view the records in archival environments: 1. The Recordkeeping Functional Requirements Project; 2. The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) project; and 3. A perspective that perceives the record as a representation. The purpose of this comparison is to understand the complexity of the term and its approach by different realities.

The term “record” is defined as recorded information, that is, information fixed on a physic support. Recorded information is a by-product of transactional

business evidence (ROBERTS, 1994). On the other hand, “document” also means recorded information, but the main difference from record is that document does not participate in transactional business and has a wider definition and application.

Latin etymology of record is *recordatio*, signifying the faculty to remember. The physical mechanism to remember through an extern tool of the human being, in this case the creation of a technology to remember what the memory finds difficult to recall. Thus, Geoffrey Yeo (2007, p.31) wrote the following thought:

> An emphasis on memory is appropriate not least because it reflects the linguistic origins of the word *record*. In classical Latin, *recordatio* meant a mental recollection of something in the past. In early medieval England, it had come to mean a verbal statement or recollection formally presented as oral testimony, but as the courts of law began to recognize written procedures and documentary evidence the words *recordatio* and *recordum* came to be used for written documents […]; the original meaning survives in some European languages. In Italian, for example, *ricordi* are recollected thoughts, or *mementoes*, and the word *archivi* is normally used where records would be employed in English-Language professional discourse.

The impact of new technologies creates curiosity but then resistance to acceptance by society, as has occurred in contemporary times with digital technology. When a novel technological challenge appears, society sometimes has an initial rejection. This is well placed in the following quote of Plato’s Phaedrus (FARNAM, 2021) in his argument against writing:

> And so it is that you by reason of your tender regard for the writing that is your offspring have declared the very opposite of its true effect. If men learn this, it will implant forgetfulness in their souls. They will cease to exercise memory because they rely on that which is written, calling things to remembrance no longer from within themselves, but by means of external marks**.** What you have discovered is a recipe not for memory, but for reminder. And it is no true wisdom that you offer your disciples, but only the semblance of wisdom, for by telling them of many things without teaching them you will make them seem to know much while for the most part they know nothing. And as men filled not with wisdom but with the conceit of wisdom they will be a burden to their fellows[35].

Facing the unknown can often be scary, because it is not completely understandable to a human being.

[35] In: https://fs.blog/2013/02/an-old-argument-against-writing/

Returning to the discussion of record, other features that make up its framework in the archival activities, as pointed out by David Roberts (1994, p.17), are:

> • in any form, including data in computer systems,
> • created or received and maintained
> • by an organization or person
> • in the transaction of business or the conduct of affairs
> • and kept as evidence of such activity.

In the same paper, Roberts improves the characteristics that make up the digital record made by the Electronics Records Committee of International on Archives - ICA in 1993 with additional elements, such as:

> ‘A record is information created, collected or received in the initiation, conduct or completion of an institutional or personal activity.
> Records have the following requirements:
> • provide evidence (which is a by-product)
> • comprise content, context and structure
> • have integrity and immutability
> • are unique
> • exist regardless of physical format
> • lead to an outcome.
>
> All these attributes exist with electronic records, but for these contexts is more important, to establish a relationship in a system of records. (ROBERTS, 1994, p.24).

Complementing the point made above, Yeo (2008, p.124) names “better” records, those issued by natural persons that belong to an organizational environment. The existence of records created in personal archives is recognized, but the core of this research is the sort of records created/produced in institutional contexts. Therefore, the importance of the above quotation considers that the main characteristic of records is the “transaction of business or conduct of affairs”.

The concept of records and documents have similar weight. Other societies used the term archival documents. A passage from Michael Clanchy (2013, p.84) clarifies this, even though he does not make a clear distinction between document and record. He associates record with a legal or business activity:

> [...] One of the Thomas Becket's biographers, William Fitz Stephen, describes how he was a draftsman in his chancery, a subdeacon in his chapel, a reader in his law court, and on occasions a judge. In the chancery he would have a been

> familiar with letters and literary style, in the chapel with liturgical books, and in the law court with records of pleas.

On the other hand, the definition of “documents”, as was already pointed out, is also recorded information, but the difference is that document is a general concept where the record is seen as a class of documents. Thus, “all the records are documents, and contain therefore information and data, but not all the documents are records” (DURANTI, 2001, p.43). The following quotation clarifies this:

> […] a document may be distinguished from a record by the latter’s evidential quality in documenting the transaction of business. This distinction is most clearly drawn in the Keeping Archives definition of records, where records are recognised as a class of documents distinguished from other kinds of documents by their transactional origin and evidential qualities (ROBERTS, 1994, p.17).

This tie among record-evidence-business-transaction defines the core of records. Erlandsson (1996) termed the former elements as “recordness”. Recordness is a concept elaborated mainly by the Recordkeeping functional Requirements Project (1993-1996) carried out at the University of Pittsburg School of Information Sciences and lead by Richard J. Cox and James Williams[36].

The Pittsburg project perceived those ideal records must have three essential elements:

> Records consist of content, structure, and context. The three qualities must be captured and preserved together in order to meet the requirements for “recordness”. The content must be put together with data about structure and context. We may call these data “metadata” (i.e., data about data). If the metadata are lost the item loses its “recordness” (i.e., evidential value) and becomes “business un-acceptable” (useless as evidence). (ERLANDSSON, 1996, p.17)

Two points in the early quotation must be highlighted. First, although this does not appear clearly in elements of Diplomatics in several academic projects in the United States, various projects have been approached with a similar category at the moment to address the records issues: (data) structure, (data) content, and (data) media (BEARMAN, 1992, p.173). Second, the concept of “recordness” pointed to by Erlandsson is a foremost concept beyond records.

[36] To further information of this project, see: https://web.archive.org/web/19991218001620/http://www.sis.pitt.edu/~nhprc/Pub1.html

The importance of the “recordness” concept comes up in the digital environment, due to the impossibility of addressing digital records the same way as paper-based records. Recordness in this sense is the union of record with evidence of transactions. “Archivist and records managers must focus on evidence not information” (ERLANDSSON, 1996).

Evidence, in this sense, is another concept that appears again in the late 20th century with the arising of the digital record. The digital record is important to preserve depending on its evidence: Informational evidence, legal or organizational evidence, and historical evidence as highlighted by Erlandsson (1996).

However, the mean of information in the Archival sense is the message contained both in the records and in the document. The difference between record and information as explained by Sue McKemmish (1993, p.5-6), information is “[…] “an imposed subject matter”, a discrete origin, and a purpose "to inform, to perpetuate knowledge, to entertain, or to convey opinions, ideas and feelings [...]".

The definition of “data” is the smallest element that makes up all the framework of a record or document. This element has a relevant value in the digital world, but by the fact of being a little particle, oftentimes is not giving its due attention. Data is an important and one of the first elements that should be cared for and correctly manipulated to create reliable digital records.

Therefore, data should be managed, by establishing its acquisition, analysis, storage, retrieval, and distribution. It should be administered, by “the corporate service which assists the provision of information systems by controlling and/or coordinating the definitions (format and characteristics) and usage of reliable and relevant data” (ROBERTS, 1994, p.22), to take into account the high possibility of meeting integrity. These two data steps are relevant to records management because they allow accountability at the time to delivered information of quality, when society needs reliable information. Duranti (2001, p.53), explains other elements that should be followed to meet authenticity data so that they become meaningful records:

> Starting from the inevitable requirement to reproduce an electronic record, we can stipulate that demonstrating the authenticity of electronic records depends on verifying that (l) the right data was put into storage properly, (2) either nothing

> happened in storage to change these data or alternatively any changes in the data over time are insignificant, (3) all the right data and only the right data were retrieved from storage, (4) the retrieved data were subjected to an appropriate process, and (5) the processing was executed correctly to output an authentic reproduction of the record. Verifying that these technical requirements were satisfied is necessary, but not sufficient, to demonstrate the authenticity of an electronic record. It is obviously necessary because if any of these conditions is not satisfied, the result of the processing of retrieved data cannot be (asserted to be) the same as the electronic record from which the stored data were produced. It is not sufficient because there is nothing in it that applies specifically to a record. It would be accurate, then, to say that this technical verification is a method for demonstrating that a digital object produced from stored digital data is an authentic reproduction of a digital object that was stored. To be precise, we should not even refer to 'a digital object that was stored,' but to the digital object that was the source of the stored data.

The efforts to preserve the integrity of the data following the steps mentioned by Duranti are relevant to try to meet the desired records in the records management processes. However, the mechanism to reproduce reliable digital records the same way as analogical records is a difficult assignment because records on paper do not need systems to be understood and recognized. The records saved in the systems are a logical representation of bits, and the records manifested in the system also require another kind of representation to reproduce it for the human comprehension.

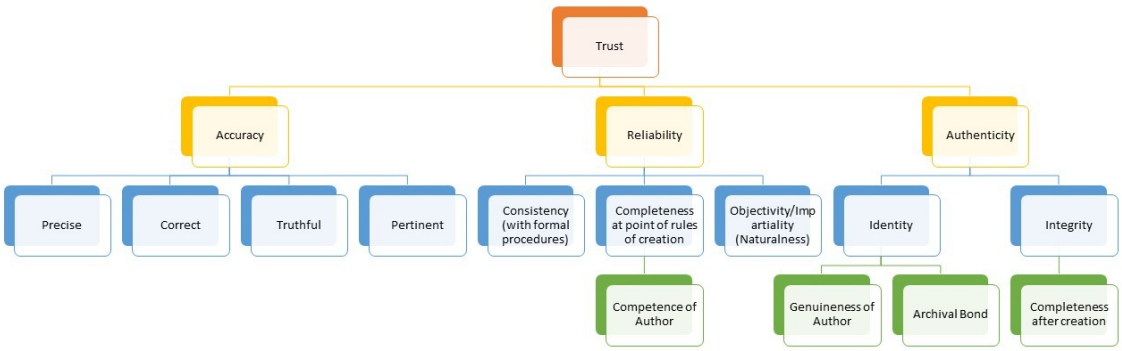
Nevertheless, achieving trustworthiness of these digital records is important beginning with the care of integrity of the mentioned data. Digital Forensics professionals understand this when asserting the value of data by analyzing the digital evidence in legal cases. According to David Bearman (1992, p.173), the data is relevant as well to analyze the provenance of digital records:

> The fundamental problem in the management of electronic records is to identify the functional provenance of records (e.g., the business purpose for which they were created), so as to be able to carry out an organizational retention policy. We cannot see electronic records except under software control, but the functional provenance of records may be *explicitly recorded as data* within the record by the record creator or system; *implicit in the system design* and revealed by analysis or by documentation which reveals the structural relations between data instances; or *discovered by links to the originating activity*, which is rep- resented by the source of the records, or more exactly by knowledge of the transaction communication path.

> Each of these three loci of functional provenance information (data content, data structure, and data context) provides documentation of what I have elsewhere called "evidential historicity" and can be contributed either by individual employees, the bureaucratic system, or the underlying technology.

The mentioned “trustworthiness” concept has three elements that deserved detail: 1. Accuracy, which means that the record must be precise, correct, truthful, and pertinent. 2. Reliability, which means that the record must have consistency (with the formal procedures), completeness for rules of creation by the competence of the author, and objectivity/impartiality (naturalness), and 3. Authenticity, which is accomplished when the record achieved the identity through the genuineness of the author and archival bond, and integrity through the completeness after the creation. This is outlined by Victoria Lemieux (2017) in figure 1:

Figure 1 – TAXONOMY OF TRUST



SOURCE: Lemieux *et al.* (2019, rendered by Alysha Joo)

Thus, the definition and delimitation of record, document, information, and data indicate how Diplomatics, Forensics, and Archival Science each work in relation to the studied object in the digital context. Digital Diplomatics analyzes the concept of “document” in an individual way to assure its authenticity through the documentary form (internal and external elements). Digital Forensics analyzes the data-integrity to achieve its mainly objective: to establish the digital evidence through the suitable technological tools. Archival Science analyzes the records and the organic relationship between them, with the aim of maintaining and preserving them over time. Archival Science researchers understand the relevance of establishing the relationship with

digital Diplomatics and digital Forensics, appropriating and adapting, scientific elements to better address digital records issues.

Thus, in relation with the written, the word “record” is a standard and accepted concept within Archival Science? This question seemingly does not have discussion, but it is necessary to define and limit it in archival studies with the purpose of avoiding possible mistakes. Therefore, other discussions can be addressed about the concept of records and their institutionalized permanence in Archival thought and practices.

The discussion is related to a third line of thought that approaches the definition of record besides the Pittsburg and InterPARES studies. Yeo (2007) explains that the “nature” of records beyond their evidence and information value. He outlined the categorization of records as a representation of reality as representations of activities of business transactions that happened in organizations. For this, the author argues that record representations must be: 1. Persistent: the capacity to endure beyond the immediate circumstance leading to its creation; 2. characterized as representation of activities, and “3. […] created by persons or devices that participated in or observed the represented activity or by persons authorized to act as their proxies” (YEO, 2007, p.338).

The standpoint of Yeo establishes the possibility to understand the concept of record in a deconstructed way. A process has been disused by other researchers including Heather MacNeil (2000) and Jennifer Meehan (2006). Another perspective of records is analyzed by Ana Maria Camargo (2003, p.14) taking the idea from Luiz Costa Lima (1986, p.197), who perceives the records as a “[…] neutral medium, without active properties, which does not interfere at all in the character of what it proves or witnesses”[37].

Thus, the records in Archival Science specifies the sort of documents that are outcomes of business transactions and should be managed by records management/archivists[38]. The tradition of archival studies in the USA and

---

[37] *Seria, portanto, uma espécie de meio neutro, sem propriedades ativas, que não interferiria em absoluto no caráter do que prova ou testemunha* (CAMARGO, 2003, p14).

[38] It is appropriate to highlights the explanation made by Corinne Rogers, when she explains that “Archivists” and “Records Management” in this case, accomplish the same function (ROGERS, 2015, p.7). Luciana Duranti and Patricia Franks (2019) also called them “records and archives professionals”. Therefore, these two professions will be used without distinction in this doctoral dissertation.

Canada more clearly separates records managers and archivists. This model is also applied in some Latin America countries. The first phase (records management) considers the records remaining in an active phase and are in constant transaction. The second phase (intermediary archive) considers the transfer of records to a semi-active repository, in which the transactions and uses decrease considerably, and they are maintained mainly for a foreseen security and/or consult. The third phase (historic archive) is considered when the records lose their primary value and acquire a second or historic value intended for any user.

This divides the lifecycle of the records to assess their relevance in three sorts of archival phases: Current, Semi-current and Archives. This model was created in the early of the 20th century, mainly with the records in paper-based format. In the 21st century, the model continues to be used for digital records. However, there is some resistance to this perspective, for example, the records continuum project in Australia, led by the ideas of Peter Scott:

> Terry Cook notes that "Peter Scott is the founder of the post-custodial revolution in world archival thinking", and that the origin of the Australian concept of records continuum, and consequently of their acceptance of the post-custodial solution, is based on Scott's theories and reinterpretation of provenance and rethinking of descriptive paradigms for archives.
>
> By taking the series concept "out of the archival cloisters" and applying it to current records in agencies, Cook believes that Australian archivists have been "helping to mend the Schellenbergian split between records managers and archivists, and between 'current' records and 'old archives" (ERLANDSSON, 1996).

The main resistance of the continuum researchers is that they did not perceive records produced and assessed to determine their historic value. The Australian group argued that from the creation of the records they have historic value (continuum value). This statement was written just to observe some differences between the two models (lifecycle and continuum), but the specific aim of this dissertation is not directly related to this matter so it will not be delved into it any further.

Ultimately, the "born-digital records" concept refers to the kind of records created/produced in digital system environments and not as a digitization process of paper-based records. When the record is created originally in paper format and then digitalized, this "new" digitized document is a copy and the

original is still the paper support. On the other hand, when the record is created/produced (born) originally in digital systems and then is reproduced in other analogical material, the original is still the digital medium. Therefore, the challenges increase to preserve this support in an accurate, reliable, and authentic form.

2.1 META-DATA: BEYOND THE DATA

The deep discussion in the previous section about born-digital records was necessary to explain how the metadata functions perform in these records. Metadata was not born with digital records. In the analogical world, several documents or files needed be identified through description features to facilitate their organization in several contexts. The novelty is that metadata became the foremost and most valuable tool for identifying, organizing, describing, maintaining, preserving, and accessing digital records. Corinne Rogers (2019) explained that metadata are the attributes of the records that demonstrate identity and integrity.

In the analog contexts, the metadata worked only as a functionality to describe the object. To address a door key, for example, we describe a series of features of this object to understand its elements of composition (features to describe this object – metadata): color, size, shape, material, use, etc. In digital environments, we are obligated to do that because rather than describing the digital object, its other rich affordances generate better and more reliable records to manage, preserve, and use.

The explanations of the concept in the Archival area have sometimes been fuzzy and meaningless to understand its relevance. The most standard and broad definition of metadata is “data about data” (PEARCE-MOSES, 2005, p.248). This kind of meaning does not help to appreciate the worth of the term in archival thought and creates some confusions. Its framework will be explored in an attempt to recognize how it is addressed in digital Forensics Archival Diplomatics activities, rather than to make commonplaces definitions. Doing this can illuminate the value of metadata in the records management and archival processes.

Separating the prefix “meta” from “data” allows recognition of how each word is perceived in a different manner. “Meta” is a word created and often used in the philosophy area. Its Greek etymological meaning is “after” or “beyond”, and as a prefix, it usually denotes comprehensive or transcending” (ETYMONLINE, 2021)[39], also, as the probes and studies about the nature of reality, including the relationship between mind and matter, substance and attribute (WORDPANDIT, 2020).

In some cases, concepts with this prefix shift the original meaning and become a new term in an abstraction process – e.g., (theory) metatheory, (physics) metaphysics, (fiction) metafiction, (language) metalanguage, and (cognition) metacognition. With that explanation, “meta-data” appears as a concept that implies something beyond the data. Therefore, metadata is not just “data about data”, it is a mechanism to represent it, in this case it is a representation about born-digital records with relevant information found “behind” or hidden from human eyes (conceptual approach).

Rogers (2019) states the metadata functions are established in the physical and logical layers. Therefore, if the metadata is well worked in both physical and logical layers, it could guarantee reliable records to users and an accountability of the information delivered.

At the same time, accompanying the statement of David Bearman and Ken Sochats (1995), a digital record is a “metadata encapsulated object”. To complement this idea, the authors imply that:

> These observables provided the foundation for the identification of a specific set of metadata which, when present, satisfies the informational needs of the specification. If this metadata is inextricably linked to, and retained with, the data associated with each business transaction it guarantees that the data object will be usable over time, be accessible only under the terms and conditions established by its creator, and have properties required to be fully trustworthy for purposes of executing business. Additional metadata retained in system and organizational accountability documentation assures full evidentiality.

In some cases, the metadata that contain digital record results are more important than the record itself. This is recognized when scholars retrieve a

[39] The Online Etymology Dictionary: https://www.etymonline.com/word/meta-#etymonline_v_14705

metadata source with the intention of solving specific cases. The following quote is an interesting example of how metadata is relevant in any environment:

> […] It seemed Magnotta was living a life of luxury. Trouble is, the pictures were all fake. Magnotta had searched the web for pictures that fit is storyline and photoshop his head on other people's bodies. This is the level of sickness that he has achieved. But the amateur investigators knew something that Magnotta didn't. You see digital pictures can contain in it metadata. This metadata can reveal the exact date and time the picture was taken, the making model of the camera, but more importantly, if the device has GPS capability. The picture can reveal the location in which the picture was taken, they were on Magnotta's trail, and they were closed […] (SWORD AND SCALE, e. 34, 2015).

The above lines are just an example of the use and reuse of metadata in any place intended to provide relevant outcomes. The metadata can be used for many purposes and the former quotation deals with the metadata of a photograph to determine the location of a specific individual.

Metadata is a relevant process in born-digital records addressed by Diplomatics, to identify and describe the intrinsic and extrinsic elements. However, this is just a part of Diplomatics method and does not determine all the Diplomatics framework, because this would be a reductionist or instrumental approach to this science.

Example of the discussion outlined previously is founded in the academic article by Caroline Williams: “Diplomatic attitude: From Mabillon to Metadata” (2005). The title of the paper is little unfair, because it seems to indicated that the heritage of Diplomatics as a consolidated science has been reduced as an instrumental tool to describe digital records. Nevertheless, the author is aware of this subject, when she recognizes the importance of Diplomatics and concludes that metadata can be used in a diplomatic form, but the underpinnings of Diplomatics makes this science more a comprehensive area than just a description function.

Thus, the metadata process performs the same way as the lifecycle of records, as outlined in the early section. Moreover, in the same form that the born-digital records have content, structure, and contexts, metadata should achieve these elements for the record to be considered a reliable source of evidence. In this regard, Berman and Sochats (1995) explain that:

> The functional requirements for recordkeeping dictate the creation of records that are comprehensive, identifiable (bounded), complete (containing content, structure and context), and authorized. These four properties are defined by the requirements in sufficient detail to permit us to specify what metadata items would need to describe them in order to audit these properties. This descriptive metadata cannot be separated from them or changed after the record has been created. Several additional requirements define how the data must be maintained and ultimately how it and other metadata can be used when the record is accessed in the future. The metadata created with the record must allow the record to be preserved over time and ensure that it will continue to be usable long after the individuals, computer systems and even information standards under which it was created have ceased to be. The metadata required to ensure that functional requirements are satisfied must be captured by the overall system through which business is conducted, which includes personnel, policy, hardware and software.

Thus, to establish trustworthy digital records that can be accepted in a determined domain, the respective metadata must be managed, including the administrative metadata, descriptive metadata, Dublin Core, Machine Readable Cataloguing - MARC, preservation metadata, and structural metadata. These types of metadata are explained thus:

> […] Typically metadata is organized into distinct categories and relies on conventions to establish the values for each category. For example, administrative metadata may include the date and source of acquisition, disposal date, and disposal method. Descriptive metadata may include information about the content and form of the materials. Preservation metadata may record activities to protect or extend the life of the resource, such as reformatting. Structural metadata may indicate the interrelationships between discrete information resources, such as page numbers.
>
> In terms of archives, MARC format and EAD are standards for structuring descriptive metadata about collections. Dublin Core is a standard for structuring metadata that is intended for describing web resources. (PEARCE-MOSES, 2005, p.248-249).

To assure accurate, reliable, and authentic born-digital records, all the processes must be recorded, and the metadata reinforces this process. For records management, the administrative, descriptive, and structural metadata should be applied. One example of the records management metadata is the Department of Defense (DoD) metadata, arises in the 90s.

To archival processes, preservation metadata should be applied. Table 1 further clarifies the types of metadata mentioned, the differences among

them, and the most used standards intended to create accurate, reliable, and authentic born-digital records.

Table 1 – TYPES OF METADATA

DESCRIPTIVE METADATA	ADMINISTRATIVE METADATA	STRUCTURAL METADATA
n. Information that refers to the intellectual content of material and aids discovery of such materials. *Notes:* Descriptive metadata allows users to locate, distinguish, and select materials on the basis of the subjects or 'aboutness' of the material. It is distinguished from information about the form of the material, or its administration. (*Puglia, Reed, and Rhodes 2004, p. 7*.): Descriptive metadata refers to information that supports discovery and identification of a resource (the who, what, when, and where of a resource). It describes the content of the resource, associates various access points, and explains how the resource is related to other resources intellectually or within a hierarchy. In addition to bibliographic information, it may also describe physical attributes of the resource such as media type, dimension, and condition (PEARCE-MOSES, 2005, p.113). **Standard Tools:** MARC 21 MODS Metadata Object Description Schema Dublin Core ONIX ONline Information eXchange EAD Encoded Archival Description	n. Data that is necessary to manage and use information resources and that is typically external to informational content of the resources. *Notes*: Administrative metadata often captures the context necessary to understand information resources, such as creation or acquisition of the data, rights management, and disposition. *(Puglia, Reed, and Rhodes 2004, p. 8):* Administrative metadata comprises both technical and preservation metadata and is generally used for internal management of digital resources. This metadata may include information about rights and reproduction or other access requirements, selection criteria, or archiving policy for digital content, audit trails, or logs created by a digital asset management system, persistent identifiers, methodology or documentation of the imaging process, or information about the source materials being scanned. In general, administrative metadata is based on the local needs of the project or institution and is defined by project-specific workflows. Administrative metadata may also encompass repository-like information, such as billing information or contractual agreements for deposit of digitized resources	*n.* information about the relationship between the parts that make up a compound object. *(IMLS Framework 2001):* Structural metadata can be thought of as the glue that binds compound objects together, relating, for example, to articles, issues, and volumes of serial publications, or the pages and chapters of a book. *(Puglia, Reed, and Rhodes 2004, p. 10):* Structural metadata might include whether the resource is simple or complex (multi-page, multi-volume, has discrete parts, contains multiple views); what the major intellectual divisions of a resource are (table of contents, chapter, musical movement); identification of different views (double-page spread, cover, detail); the extent (in files, pages, or views) of a resource and the proper sequence of files, pages, and views; as well as different technical (file formats, size), visual (pre- or post-conservation treatment), intellectual (part of a larger collection or work), and use (all instances of a resource in different formats – TIFF files for display, PDF files for printing, OCR files for full text searching) versions (PEARCE-MOSES,

	into a repository (PEARCE-MOSES, 2005, p.11). **Another Definition**: Administrative metadata relates to the technical source of a digital asset. It includes data such as the file type, as well as when and how the asset was created. This is also the type of metadata that relates to usage rights and intellectual property, providing information such as the owner of an asset, where and how it can be used, and the duration a digital asset can be used for those allowable purposes under the current license. The National Information Standard Organization (NISO) breaks administrative metadata down into three sub-types: **Technical Metadata –** Information necessary for decoding and rendering files. **Preservation Metadata –**Information necessary for the long-term management and archiving of digital assets. **Rights Metadata –** Information pertaining to intellectual property and usage rights (MERLINONE, 2021)[40]. **Standard Tools:** Preservation: PREMIS is: –Common data model for organizing/thinking about preservation metadata – Guidance for local implementations – Standard for exchanging information packages between repositories (PREMIS, 2010)[41].	2005, p.373). **Another Definition:** *(NISO and IMLS 2007, 58):* Structural metadata documents relationships within and among objects and enables users to navigate complex objects, such as the pages and chapters of a book. *(NISO and IMLS 2007, 83):* Structural metadata relates the pieces of a compound object together and/or bundles related objects into a package. For example, if a book is digitized as individual page images, structural metadata can record information concerning the order of files (page numbering) and how they relate to the logical structure of the book (table of contents) (SAA, 2021)[42]. **Another Definition:** In 1996, a metadata initiative known as the Warwick Framework first identified structural metadata as “data defining the logical components of complex or compound objects and how to access those components. By 2004, the National Information Standards Organization (NISO) discussed structural metadata in their standards. According to their definition in the z39.18 standard, “Structural metadata explain the relationship between parts of multipart objects and enhance internal navigation. Such metadata include a table of contents or list of figures and tables.

[40] In: https://merlinone.com/types-of-metadata/

		In his recent book *Metadata*, Richard Gartner touches on a more current role for structural metadata: “it defines structures that bring together simpler components into something larger that has meaning to a user.” He adds that such information “builds links between small pieces of data to assemble them into a more complex object (ANDREWS, 2017)[43]. **Standard Tools:** WAI-ARIA - Web Annotation Vocabulary -Document Components Ontology (DoCO)

SOURCE: Quoted from: (Richard Pearce-Moses, 2005; PREservation Metadata Implementation Strategies, 2010; Andrews. 2017; Dictionary of Archives Terminology, 2021; MerlinOne, 2021).

[41] In: https://www.loc.gov/standards/premis/premis-Vienna-pt1.pdf

[42] In: https://dictionary.archivists.org/entry/structural-metadata.html

[43] In: https://storyneedle.com/structural-metadata-key-to-structured-content/

Table 1 illustrates that the process of metadata describes how records management and archival activities deal with the three sorts of metadata: Descriptive, Administrative, and Structural metadata. The Administrative metadata contains the Technical, Preservation, and Rights Metadata. Ultimately, the standards tools of metadata were created to improve the Archival processes.

Finally, it is possible to map the entire process to create better born-digital records. The traditional goals of accuracy, reliability, and authenticity are more difficult to achieve in digital records than paper records. However, it is possible to establish the capacity to reproduce born-digital records with trustworthiness in the digital reality. Data, information, and record, along with the proper metadata could provide trust in records to serve society that increasingly needs reliable information for decision making. Records management specialists/archivists must provide these kinds of better records as part of our responsibility and accountability. For that, the nature of born-digital records and the form that these records are in within the digital systems must be understood.

For Archival Science and especially, digital records, metadata arises as a function to be considered for diverse purposes. To be a better tool, records management and archival policies must be established, to create metadata that increase its richness to be managed, maintained, and preserved.

2.2 LONG-TERM PRESERVATION

Born-digital records face challenges to be accepted as trustworthy documents, from their birth up their final disposition. Each phase of the lifecycle is relevant to establish their trustworthiness, that is, when records are created, their data accuracy and integrity must be guaranteed to become good records. When records are saved in digital systems, an automated chain of custody must be guaranteed to not corrupt the data integrity. When records are preserved as memory of any institution, tools of long-term preservation must be guaranteed to recovery trustworthy records in the near or distant future.

Thus, preservation following the explanations of Duranti (2019, s.47) must:

> […] ensure the physical and/or technological stabilization (for the purpose of extending its life indefinitely) and the protection of its intellectual content and relationships.
> Digital preservation (or “preservation of digital records”) is the process of maintaining digital materials authentic and accessible during and across different generations of technology over time, irrespective of where they are stored.
>
> Digital Preservation is a continuous process that begins with or even before records creation.

Although a series of preservation challenges exists, analog records could sometimes be preserved even without records management policies or technological tools, as realized in physical archives or places where the records are kept. When paper-based records are created, many times no plan is established for mechanisms to support their physical preservation. However, the difficulties increase for digital records.

Three main attributes of physical records that are not qualities of the digital records are: 1 – physical records are intelligible directly by the human eye (in born-digital records or mere digital records are only possible to understand in the conceptual layer); 2 – they can more early be maintained and preserved in archives even in difficult environmental conditions, in facilities with problems of adequate archival custody, or with policies that impact records and archival management, etc.; and 3 – it is easy to identify if some change was made in physical records, because they are a kind of object that does not require a mediator such as a computer to be understood (MONTOYA-MOGOLLÓN; TROITIÑO RODRIGUEZ, 2019, p.49).

In addition, digital records rarely survive without the intervention of professionals or systems intended to accomplish the goal of preservation. The justification of this doctoral dissertation arises in the possibility to apply Diplomatics, Forensics, and Archival Sciences in an attempt to encounter scientific answers for the complexities of born-digital records and their preservation issues. Each chapter details how both Diplomatics and Forensics contribute to this matter. Diplomatics can identify, through the formal characteristics of born-digital records, if they could be approached as trustworthy. Forensics on the other hand, can exam both born-digital records and digital systems to protect the data-integrity and keep this integrity

throughout their lifecycle. Finally, Archival Science, continues the process by applying and assessing the trustworthiness of archival, administrative, legal, or to any other activity.

For the aforementioned, Diplomatics had to borrow the knowledge of digital Forensics (along with other sciences) to provides some solutions. Archival professionals use these elements to improve archival activities. These professionals do not need to be specialists in computing systems or digital Forensics to understand the behavior of records, within the digital systems. Digital Forensics is a source of knowledge to better understand the composition of digital records to enhance archival affairs. In the same way, archivists are not diplomatists for using the knowledge of Diplomatics.

Hence, long-term preservation in digital contexts is relevant and a hard assignment because it is the final stage in the life cycle of records but must be taken care of from the first stage. If the data-integrity is assured from the creation/production and through its several transactions, data can remain reliable with a minimum or without tainted information for the future in trusted archival repositories. For this reason, Diplomatics and Forensics deal with the complicated assignments to ascertain the reliability of records from records-creation, passing through records-keeping until the preservation process.

Digital preservation process is different from analog preservation, and their accompanying must be permanent. Therefore, a series of preservation strategies, such as emulation, refreshing, and migration, are necessary to reduce the corruption or loss of relevant information. Kenneth Thibodeau (2002, p.18-19) states about the emulation and migration process:

> Emulation strives to maintain the ability to execute the software needed to process data stored in its “original” encodings, whereas migration changes the encodings over time so that we can access the preserved objects using state-of-the-art software in the future.

Another strategy of preservation is refreshing, which means to transfer data from an obsolete medium to a new medium with the same features. Other strategies of preservation are replication, which entails the duplication of data, and encapsulation: “[…] the idea that preserved objects should essentially be self-describing, linking content with all the information required for it to be

deciphered and understood […]" (DAY, 2006, p.188). Encapsulation strategy is the core of the model Open Archival Information System – OAIS.

The idea of "original" disappeared in digital environments, because they are representations of bitstreams that produce digital records for human understanding. The professionals understood that it is not possible to preserve the concept of original digital records, but it is only possible to preserve the possibility to reproduce digital records (THIBODEAU, 2002, p.19).

Both digital Diplomatics and digital Forensics are providing grounds to improve the preservation in Archival practices. An example of software to improve the mechanisms to preserve the born-digital records is the OAIS model materialized in platforms of preservation as Access to Memory (ATOM).

2.3 CHAIN OF PRESERVATION

The main form to secure the integrity of born-digital records is addressed by two mechanisms: Chain of Custody (CoC) and Chain of Preservation (CoP). In Forensics, the chain of custody is applied in the creation and keeping of digital records, in other words, it is used in the first two phases of lifecycle. On the other hand, the chain of preservation is a mechanism that cares for the integrity of records when they are transfer from recordkeeping systems to preservation systems. The relevance of the chain of preservation arises in the accountability to preserve records avoiding the tainted and/or malicious modification of data and as a mechanism to perpetuate so that the correct information can be used by any user.

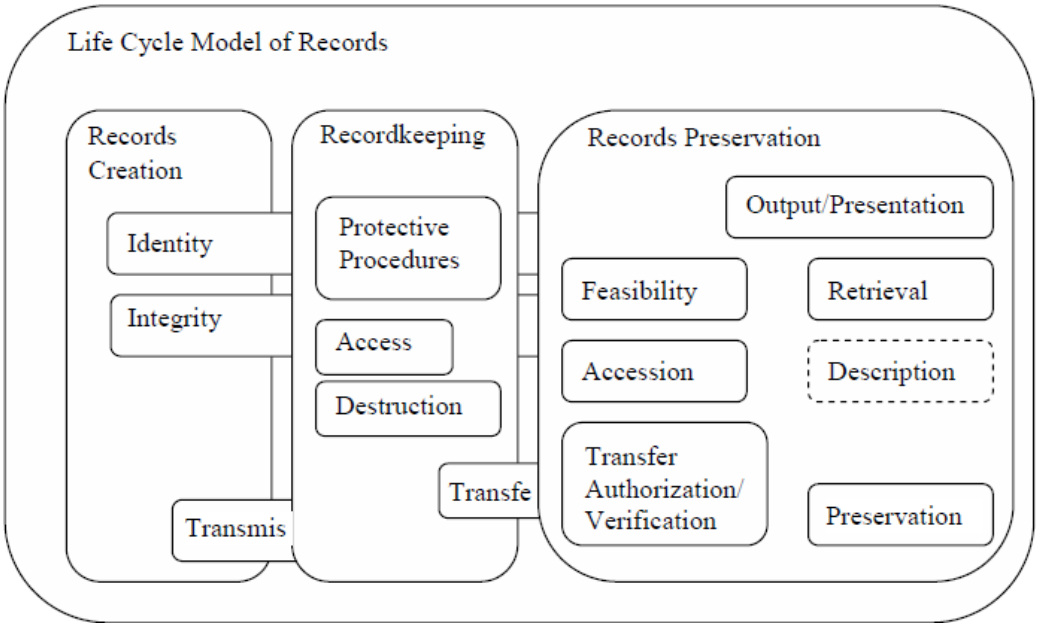
The concept of digital chain of preservation was created and developed by InterPARES (TENNIS, 2008) as a necessary mechanism for archival repositories. The chain of custody was elaborated in the creation and maintenance stage of records. However, difficulties exist with the preservation processes over the long-time, and this tool was developed with the intention to overcome these issues. Currently, chain of preservation is barely researched in the academic literature; nevertheless, it is necessary to deep in its attributes and support to address born-digital records and their respective metadata.

Chain of preservation is thus explained by InterPARES as,

> […] a system of controls that extends over the entire life cycle of records and ensures their identity and integrity in any action that affects the way the records are represented in storage or presented for use. The benchmark requirements for assessing the authenticity of the creator's electronic records define evidence that demonstrates how the records creator established and maintained the chain of preservation while the records remained in its custody. The baseline requirements supporting the production of authentic copies of electronic records articulate what the preserver must do to ensure that the chain remains unbroken from the moment the records are transferred to the archives.

The identity and integrity concepts must continue from the creation through the preservation process. Daniel Flores and Charlley Luz (2017, p.368) explain that the chain of custody and chain of preservation must be kept uninterrupted to guarantee the authenticity of records in any phase of the record's lifecycle. Thus, in the preservation stage, these two requirements must be maintained over time and space to guarantee the trustworthiness of digital records. Figure 2 presents the importance of identity and integrity traversing the three phases in the lifecycle of a record.

Figure 2 – LIFECYCLE MODEL OF RECORDS



SOURCE: Tennis (2008, p. 8).

Figure 2 identifies in addition to the identity and integrity that runs through all the three stages of the lifecycle, the transmission of digital records

and then their possible transference to preservation systems in situations when the records can be permanent. Furthermore, in the recordkeeping systems, protective procedures must be applied with metadata “[…] This requires the recordkeeping system not only to backup records, but also to account for such action indicating that a backup was made, who effected the backup, the date and time of backup, and the location of the backup copy”. Destruction metadata refers to when the digital records were eliminated. Access metadata enables the use of digital records in active or semi-active time. Transfer metadata establishes all the identification about transfer of these records (TENNIS, 2008, p.12-13).

The preservation stage model of figure 2 identifies the output/presentation, which allows identification of which records were presented and package for output. Retrieval is related with the user’s ability to recover the records and use them. Feasibility deals with the decision made by the preserver to store the records over the time. Accession means the capacity to access records after feasibility. Description is the creation of describing metadata that verifies the presumption of authenticity of each record. Preservation deals with the state of records before and after they undergo any preservation action. Transfer authorization/verification deals with how the records are transferred to the preserver systems and that the transfer was authorized and verified (TENNIS, 2008, p.15-18).

The relevance of figure 2 is found in the condensed form to realize the ideal mechanism to deal with born-digital records. If in the traditional paper records, the recordkeeping system as a whole could be analyzed, for born-digital records, this framework is difficult due to the granularity of digital components and partitions into the logic and physical layers (record storage). When these components are reproduced, their parts are reconstituted to create the digital component in the conceptual layer (record manifested). Therefore, the interoperability of born-digital records should be considered and their metadata be preserved over the time (FLORES; LUZ, 2017, p. 89).

2.4 TRUSTED REPOSITORIES AS EVIDENCE OF AUTHENTICITY

To deepen and develop this research in an international academic experience to provide better understanding about the connection of digital Forensics to Archival Science, a specific project was submitted in 2018 to several Brazilian fellowships to obtain financial resources. The initial project was sent to the three main grant research entities, namely: the National Council for Scientific and Technological Development (*Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq*), the Coordination of Superior Level Staff Improvement (*Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES*), and the São Paulo Research Foundation (*Fundação de Amparo à Pesquisa do Estado de São Paulo – FAPESP*), which ultimately funded the fellowship. As referenced throughout this research, the international academic experience with the significant economic resources was obtained from *FAPESP*. The project was finally accepted at the end of 2018 to develop the international academic experience.

Although the project was not accepted by the *CNPq* or *CAPES* in 2018, because of bureaucratic matters, before obtaining the positive *FAPESP* international grant result[44], an interesting insight was received from a CNPq peer review related to the issue of trusted archival repositories in the Brazilian reality:

> Criteria: The project goals are well defined? There is sound scientific grounding, and the performed methods are adequate?
>
> Response by the CNPq peer review: Yes, the goals are clearly and well formulated. The project has a solid and comprehensive grounding; however, that theoretical grounding is missing the *issue of trust digital repositories,* which can provide important support […] (CNPq, 2018, p. 3, our translation)[45].

Although trusted archival repositories are necessary to create, maintain, and preserve born-digital records, we had not delved into the close relationship

[44] The name of the international fellowship is Research Internships Abroad (BEPE). In: https://fapesp.br/en/bepe

[45] *Critério: Os objetivos do projeto estão bem definidos? Há solida fundamentação científica e os métodos empregados estão adequados?*

Sim, os objetivos estão claros e bem formulados. O projeto tem uma fundamentação teórica e sólida e abrangente; falta nessa fundamentação teórica a questão dos repositórios digitais confiáveis, que pode fornecer subsídios importantes [...] *(CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO – CNPq, 2018, p.3).* In*:* http://www.carloschagas.cnpq.br/

between records and trusted repositories with suitable requirement to maintain the authenticity of records over the time. Hence, this section is justified due to the urgency to establish reliable records in any stage of the lifecycle and to guarantee their permanence in reliable and trusted archival repositories. The same way that the paper records must be keep in adequate physical facilities, born-digital records must depend on suitable and archival digital repositories.

The lines mentioned above are related with another part of the peer review assessment, when the reviewer highlighted the current situation in the country related with the legal subject of the born-digital records and the repositories, along with their suitable archival requirements:

> [...] It is an important subject to Archival Science, necessary and quite urgent considering the current Brazilian situation of legal insecurity of digital records when they lack strong benchmarks from the Digital Archival Forensics Diplomatics – DAFD, for the maintenance of authenticity, reliability, and preservation for the long-term in a systemic way in Archival Repositories […] (CNPq, 2018, p. 2, our translation)[46].

Along with the situation of the national legal insecurity, there is other issues related with precarious Legal and Archival practices. With a mismatch between the theory and practices of Diplomatics, lack of infrastructure, technology, models of literacy in our profession, among other situations. This sort of issues creates a rupture between the state and the citizen because no have integrity in the data asked.

The miracle of technology is often noted; however, the necessity of professionals to intervene in these important issues cannot be forgotten. The legal issues in the digital contexts are a problem that needs to be solved in the current reality. Thus, the foundation of the research tries to discuss how sciences such as Diplomatics, Forensics, Archival Science, History, and Law provide elements to address this legal situation. Many professionals are working to create and enhancing systems with archival features by maintaining and perpetuating worthy born-digital records defined by records schedules and other records management instruments.

[46] [...] *É um tema caro ao campo da Arquivística, necessário e muito urgente considerando o atual cenário brasileiro de insegurança jurídica dos documentos arquivísticos digitais quando carecem de referenciais robustos da ciência forense digital arquivística para a manutenção da autenticidade e da confiabilidade e preservação a longo prazo de forma sistêmica em Repositórios Arquivísticos* [...] *(CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECHNOLÓGICO – CNPq, 2018, p.3). In*: http://www.carloschagas.cnpq.br/

In Archival practices, research developed by Brazilian authorities in the topic is interesting, such as the National Council of Archive – *CONARQ*[47], which establishes a model to maintain accurate, reliable, and authentic born-digital records throughout their lifecycle. This model obeys the international guidelines related with archival requirements and with the lifecycle model: the first stage (creation and transactions of born-digital records) entails the Records Management Computerized System - *SIGAD*[48] model. The *SIGAD* model was thought to solve the core archival problems such as, archival bond, organicity, reliability, authenticity, and digital evidence, as well as working with hybrid records.

In a second digital records stage related with the long-term preservation, the *CONARQ* policies establish the *RDC-Arq* Trusted Digital Archival Repository[49] based in the Open Archival Information System – OAIS model, as is also explained in the digital Forensics chapter. This model is applied in digital technological platforms, such as *Archivematica* and *Atom*, both software developed by the Artefactual Company[50].

On the one hand, *Archivematica*[51] is an open-source application to preserve born-digital records in a trustable, authentic, and reliable manner. On the other hand, *Atom*[52] (Access to Memory) is also an open-source "application for standards-based archival description and access in a multilingual, multirepository environment" (ATOM, 2021). Currently, these two digital platforms do not work in an interoperable way, although they are the most used by cultural heritage institutions.

Both Archivematica and Atom platforms are widely used in Brazil due to their records management and archival features. Recently, the research of several national research centers has explored these two platforms and held workshops intended to prepare both records management and archival professionals to deal with digital difficulties.

[47] *Conselho Nacional de Arquivos – CONARQ.*

[48] *Sistema Informatizado de gestão arquivística de documentos – SIGAD*

[49] *Repositório Arquivístico Digital – RDC-Arq.*

[50] In: https://www.artefactual.com/

[51] Archivematica features: https://www.archivematica.org/en/

[52] Atom features: https://www.accesstomemory.org/en/

In the 2000s, some organizations emerged concerned with digital preservation matter, including the Online Computer Library Center – OCLC and the Research Library Group – RLG, where a report was complied with standard specifications to preserve the records[53], in which the *CONARQ* analyzed the report to apply in the Brazilian context. Thus, the OCLC/RLG report highlighted interesting mechanisms to assure trusted digital repositories, namely:

> ✓ accept responsibility for the long-term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users;
> ✓ have an organizational system that supports not only long-term viability of the repository, but also the digital information for which it has responsibility;
> ✓ demonstrate fiscal responsibility and sustainability;
> ✓ design its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access, and security of materials deposited within it;
> ✓ establish methodologies for system evaluation that meet community expectations of trustworthiness;
> ✓ be depended upon to carry out its long-term responsibilities to depositors and users openly and explicitly;
>
> ✓ have policies, practices, and performance that can be audited and measured; […] (RLG-OCLC, 2002, p.5).

Even though the report was written 20 years ago, some interesting elements continue to be used. As a consequence, the archival policies to implement a trusted digital repository emerge as the cornerstone to technological and administrative matters. The international research for this dissertation was performing at the UBC in 2019 included attendance of the 11th Annual International Symposium, Policy Matters[54], which related to the relevance of the policies in records management and archival activities. This event clarified the importance of records policies as a crucial rule to be considered among organizational people, systems, procedures, operational production, transactions of digital records, and others. The international symposium presentation highlighted that:

> Our guest speakers are internationally renowned academics, researchers, and professionals from institutions around the world here to address the multifaceted role of policy in the history, present and future of the records and archives professions. Together we will explore how policies work in

[53] https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

[54] https://acasymposium2019.sites.olt.ubc.ca

> practice and how professionals can make use of them, how policies help to contend with matters of privacy and freedom of information, trust in new technologies, digitization, and authenticity and how policies can guide records, archives and information practices in reconciliation or decolonisation. We will hear about the role that policy matters can play in ensuring that the records and archives profession remains responsive and relevant to stakeholders outside of the field, building trust in our users, as well as in our profession, and confidence in our ability to deal with new challenges (ACA/UBC, 2019).

To implement trusted repositories in any institution, the two vital elements are: first, the policies must be applied to the entire framework of the institutions; and second, the legal aspect is another foremost characteristic for the well-functioning of trusted repositories. Both policies and the legal issue are mandatory as referenced by the OCLC/RLLG (2002). Some policies that might be considered in trusted digital repositories are listed below:

> - Policies for collections development (e.g., selection and retention) that link to technical procedures about how and at what level materials are preserved and how access is provided both short and long term.
> - Policies for access control to ensure all parties are protected, including authentication of users and disseminated materials.
> - Policies for storage of materials, including service-level agreements with external suppliers.
> - Policies that define the repository's designated community and describe its knowledge base.
> - A rigorous system for updating policies and procedures in accordance with changes in technology and in the repository's designated community.
> - Explicit links between these policies and procedures, allowing for easy application across heterogeneous collections (RLG-OCLC, 2002, p.29).

On the other hand, the legal matters, as was written at the beginning of this section, are a key element and an issue that continues to generate difficulties in several repositories. This is seen, for example, in cases of open-access scientific journals where in a preprint article made by Mikael Laakso, Lisa Matthias, and Jahn Najko (2021, p.2), pinpointed how 176 open access journals were deleted from the web between 2000–2019. For that reason, it is constantly necessity to establish trusted digital repositories to avoid legal issues:

> Digital preservation has even wider legal implications. How preservation infringes on copyright remains unclear. For example, the content creator does not usually own the rights to

> the software and systems used to create the digital file. This raises legal issues when access or changes to those systems are necessary. In such cases, at best, a repository will need to arrange separate rights clearance for long-term maintenance; at worst, preservation will be compromised because rights clearances for access cannot be obtained. Some work has been done on the establishment of repositories for software to help address these concerns, however the research repository community will need to make an appeal to have this conflict taken into consideration in the creation or renewal of national deposit legislation (RLG-OCLC, 2002, p.19).

Ultimately, the core of the word “trust” in this context deals with the supreme attribute of digital repositories to perpetuate reliable born-digital records. The OCLC/RLG (2002, p.37) defines how these sorts of trusted repositories would be established:

> The framework is broad enough to accommodate different situations, architectures, and institutional responsibilities while providing a basis for the expectations of a trusted repository. A trusted digital repository is more than just an organization responsible for storing and managing digital files. A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future. Some institutions may choose to address all functional and informational responsibilities in a complete local system. Others may choose to manage the logical and intellectual aspects of a repository while contracting with a third-party provider for digital file storage and maintenance. A critical component is the overall infrastructure supporting the reliability and sustainability of digital repositories so that organizations and their designated communities can trust that digital resources will be preserved for the long-term.

Trusted digital repositories are a concept with real weight in the digital realm and deal with the commitment to perpetuate reliable information to future generations. To achieve this goal, Margaret Hedstrom (1998) explained that it must combine policy, standards systems design, and implementation to guarantee reliable and authentic born-digital records. These subjects are analyzed in current research related to information governance which is a “[…] strategic framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use and dispose of information in ways that align with and contribute to the organization’s goals” (IRON MOUNTAIN, 2021). This kind of information governance is allied with the records management process.

3 DIPLOMATICS

> […] if I did not understand how people got where they did, I would not understand what they were doing now, what they might do in the future, and why (POLLITT, 2010, p.4).

Based on the academic literature, Diplomatics is a science that analyzes the authenticity of records through their external and internal characteristics, or in diplomatic words, their extrinsic and intrinsic elements. The external/extrinsic elements are those elements that support and cover the intellectual message, including the medium, script, language, special signs, seals, and annotations (DURANTI, 1991, p.7). The internal/intrinsic elements are "[…] considered to be the integral components of its intellectual articulation […]" (DURANTI, 1991, p.11).[55]

Thus, this chapter intends to analyze the foundation of Diplomatics. This re-examination is necessary to understand the elements of the science and why it is currently important. Historicizing Diplomatics provides an epistemological perspective of its functionality within the digital context.

Throughout history, a series of professionals have used Diplomatics for diverse purposes, for instance: diplomatists verifying the authenticity of documents; Historians applying historical criticism methods to documents, as a research source; Legal professionals analyzing legal frameworks; Records professionals (archivists and records managers) verifying the authenticity of records in Archival contexts. As a result, a close dialogue should persist between archivists and historians (CAMARGO, 2018).

3.1 HISTORY OF DIPLOMATICS, DIPLOMATICS AS SUPPORT TO HISTORY

Diplomatics was created and subsequently applied in 1681 by the Benedictine monk, Dom Jean Mabillon, also known as, Johannis Mabillon, Johannes Mabillon, or merely as Jean Mabillon (MABILLON, 1681). His objective was to demonstrate the authenticity of Merovingian's diplomas

[55] Or, "The diplomatic speech" to Bellotto (*o discurso Diplomático*) (BELLOTTO, 2008, p.35, our translation).

questioned by the Jesuits Order. This situation caused some problems for the Benedictine Order, which is why they had to appoint a scholar from their religious community to try to solve this issue.

Was the Benedictine monk Dom Jean Mabillon a historian, a diplomatist, a paleographer, a librarian, or an archivist? It is possible to state that he supported all these works. He was a historian looking to achieve the historical truth (or “love of truth” as pointed out by Randolph Starn), (2002, p.398). He was a diplomatist because he was its founder, and he developed the principles of Diplomatic studies. He was paleographer because he dedicated the last part of the treatise to developing knowledge about ancient and historical handwriting: “[…] the medieval scripts done by handwriting, the forms the curves, the ink, the style […]” (JOHN, 1992).

He was also a librarian, because he came to the *Abbey of Saint-Germain-des-Prés* in France with the initial objective of organizing its library (BARRET-KRIEGEL, 1988). Finally, he was an empirical archivist because his research was the result of an investigation of solemn records preserved in the archives that he had organized. This dissertation emphasizes the character of Mabillon as an archivist, wherein Blandine Barret-Kriegel (1988, p.26) outlines his contribution in this scenario:

> […] He was not quite a Benedictine like the others either if the others were precisely defined by Georges Tessier: << The young people who applied for admission to the Congregation of Saint-Maur were not from candidates for the School of Charters. They did not envisage a career of archivist or librarian; they did not seek to introduce themselves into the disciplines of scholarship. Their primary vocation was not that of Léopold Delisle or Maurice Prou. The school of which they intended to become the pupils was that of the evangelical counsels and the perfect life. The instruction offered to them was the Rule of St. Benedict and the Constitutions of the Congregation. The perspectives offered to them were the recitation of the long canonical hours, the meditations, retreats, and recollections honored by the spirituals of the sixteenth century, silence, abstinence, macerations, the cell without comfort and fire. >> Mabillon seriously imagined being an archivist, he had already been appointed as a library assistant and he was already initiated into the disciplines of scholarship. Nevertheless, it was in the austere atmosphere of the abbey, in the regularity of the conventual exercises, in the difficulty of Benedictine asceticism that he was going to find a framework,

> superiors, companions, to produce a work (BARRET-KRIEGEL1988, p.26, our translation) [56].

In some studies, Jean Mabillon is not considered to be an archivist. This is understandable because he probably did not use the same techniques, concepts, and practices as other scholars including Jacob von Rammingen (1510-1583) or Baldassarre Bonifacio (1585-1659). The latter created a short treatise in 1632, which was […] one of the first exclusively dedicated to archives […] (DURANTI, FRANKS, 2019, p.58).[57] It was probably not his main objective either, since his work only occurred thanks to religious convulsion of the times.

The contribution of Mabillon to Archival Science started to make sense, three centuries later when was subject of Diplomatics elements addressed in the research of various archival scholars of the twentieth century, first and foremost in the studies of Hilary Jenkinson (1957), Robert Henri-Bautier (1961), Luciana Duranti (1989), Antonia Heredia-Herrera (1991), Manuel Romero-Tallafigo (1994), Bruno Delmas (2010), among others.

The relevance of archival heritage was embodied in Mabillon's study. The cover photo of *De re diplomatica libri VI* (MABILLON, 1681) has a drawing of a building wall with the heading "*ARCHIVA*", as seen in image 1, hinting at the importance of the archive as a source of knowledge for the Benedictine community. Manuel Romero-Tallafigo (2004, p.141) described this picture in detail:

> The legend appears complemented by a large stage in the background of which a forum full of Roman temples is

[56] *[…] Il n'était pas non plus tout à fait un bénédictin comme les autres, si les autres ont été justement définis par Georges Tessier :<<Les jeunes qui sollicitaient leur admission dans la Congrégation de Saint-Maur n'étaient pas de candidats à l'école des Chartes. Ils n'envisageaient pas une carrière d'archiviste ou de bibliothécaire, ils ne cherchaient pas à s'initier aux disciplines de l'érudition. Leur vocation première n'était pas celle d'un Léopold Delisle ou d'un Maurice Prou. L'école dont ils entendaient devenir les élèves était celle des conseils évangéliques et de la vie parfaite. L'instruction qu'on leur proposait était la Règle de Saint-Benoît et les constitutions de la Congrégation. Les perspectives qu'on leur offrait étaient la récitation des longues heures canoniales, les méditations, retraites et recollections mises à l'honneur par les spirituels du XVI siècle, le silence, l'abstinence, les macérations, la cellule sans confort et sans feu>> Mabillon, lui, imaginait sérieusement d'être archiviste, il avait déjà été désigné comme aide-bibliothécaire et il était déjà initié aux disciplines de l'érudition.Néanmoins, c'est dans l'atmosphère austère de l'abbaye, dans la régularité des exercices conventuels, dans la difficulté de l'ascèse bénédictine qu'il allait trouver un cadre, des supérieurs, des compagnons, produire une œuvre* (BARRET-KRIEGEL,1988, p.26).

[57] It is noticed this idea with the publication of Luciana Duranti and Patricia C. Franks, Encyclopedia of Archival Writers, 1505-2015 (DURANTI; FRANKS, 2019). However, reading this study, is understandable that the focus of the work was to emphasize the significant concepts of Archival studies.

represented. Between two classic buildings, an Archive and a Library, two beautiful ladies or matrons appear seated, occupying the central place: Justice and Truth. The crowned Justice manifests itself with a large open eye in the chest and carrying a scale in the right hand. The matron of Truth is displayed without a crown, her hair gathered with a tiara, one breast naked, with the unbreakable palm of triumph in her right hand and the radiant sun of truth raised by her left hand. The truth was born out of skepticism about inherited ideas. The Enlightenment and the Lights of modernity began. At the feet of both ladies, Diplomatics Science is represented as another lady: prostrated before them on her knees, covered with the petasos or winged helmet of Hermes, the insightful god of Hermeneutics, mentor of paths and crossroads towards progress. Diplomatics holds in her hands a parchment wherein classical capital script the text *"De re diplomatica libri sex*" appears. Under this parchment, as tools of Diplomatics, the precise tools of truth, measurement, and objectivity: a sphere, a triangle, and a mirror (ROMERO-TALLAFIGO, 2004, p.141, our translation).[58]

[58] *La leyenda aparece complementada por un gran escenario en cuyo fondo se representa un foro repleto de templos romanos. Entre dos edificios clásicos, un Archivo y una Biblioteca, aparecen sentadas, ocupando el lugar central, dos hermosas damas o matronas: La Justicia y la Verdad. La Justicia coronada se manifiesta con un gran ojo abierto en el pecho y portando una balanza en la mano derecha. La matrona de la Verdad se exhibe sin corona, el cabello recogido con una tenia, desnuda de un pecho, con la inquebrantable palma del triunfo en su mano derecha y el sol radiante de la verdad elevado por su mano izquierda. La verdad nacía del escepticismo ante las ideas heredadas. Se iniciaban la Ilustración y las Luces de la modernidad. A los pies de ambas damas se representa la ciencia Diplomática como otra dama: Postrada ante aquéllas de rodillas, cubierta con el pétasos o casco alado del Hermes, el dios perspicaz de la Hermenéutica, mentor de caminos y encrucijadas hacia el progreso. La Diplomática porta en sus manos un pergamino donde en escritura capital clásica aparece el texto "De re diplomatica libri sex". Bajo este pergamino, como herramientas de la Diplomática, las herramientas precisas de la verdad, la medida y la objetividad: una esfera, un triángulo y un espejo* (ROMERO-TALLAFIGO, 2004, p.141).

Image 1 – THE WORD “ARCHIVA” ON THE RIGHT SUPERIOR SIDE

SOURCE: Mabillon (1681)

In the same way that Jean Mabillon was recognized for his treatise, he was also noted for his work as an antiquarian (BARRET-KRIEGEL, 1988; ROMERO-TALLAFIGO, 1994, p.18). The collection of ancient objects was seen

as a respectable craft[59]. Mabillon's ability to function as a diplomatist, archivist, and antiquarian resulted in the achievement of records being used as materials to be studied. He dedicated part of his life to organizing and classifying records for his projects and "[…] in the years (1667-1703) Mabillon journeyed in France, Germany, Switzerland, Austria, and Italy […]" (BRUUN, 2010, p. 429), intending to visit the archives and libraries and to establish debates and discussions with other religious orders (BARRET-KRIEGEL, 1988, p.83-86). In parts of Blandine Barret-Kriegel's (1998) text, she highlights the role of Mabillon as an archivist:

> [...] The archives are not yet established, the libraries are not yet organized, the sources are not yet listed, the diplomas, the books or the manuscripts even if they do not belong to Antiquity, emerging that they are from an almost entire past bent under the night, the gleaming eyes of the darkness seem. This is why, when it comes to enumerating his findings, presenting them, exhibiting them, the scientist calls his works, albums, analects, museum […] (BARRET-KRIEGEL, 1988, p.78- 79).
>
> [...] Mabilloniens travels move and reclassify the traces by the groping constitution of museums, of treasures, but soon of directories and catalogs, they contribute to this movement of a general census of the sources of "Antiquity" by what was constituted, before, well before, the formation of contemporary Archival Science, the technology of learned History [...] (BARRET-KRIEGEL, 1988, p.81-83, our translation)[60].

Thus, Jean Mabillon approached the issue of archives, libraries, and museums of the 17th century, as places to preserve mankind's knowledge. Albeit little was known of some of the abuses performed with the intent to provide authenticity to the records, as Luciana Duranti (1989, p.12) points out:

[59] […] *Antiquaire, le bénédictin l'est en effet, dans la mesure où il applique aux pièces et aux documents qu'il examine, l'attachement obsessionnel et émerveillé dont l'archéologue fait plus souvent montre que l'historien moderniste […]* (BARRET-KRIEGEL, 1988, p. 78-79).
(Translation): […] *Antiquarian, the Benedictine is indeed, insofar as he applies to the pieces and documents that he examines, the obsessive and amazed attachment which the archaeologist more often shows than the modernist historian* […] (BARRET-KRIEGEL, 1988, p. 78-79).

[60] [...] *Les archives ne sont pas encore établies, les bibliothèques ne sont pas encore organisées, les sources ne sont pas encore répertoriées, les diplômes, les livres ou les manuscrits même s'ils n'appartiennent pas à l'Antiquité, sortis qu'ils sont d'un passé presque entier ployé sous la nuit, semblent les yeux luisants de l'obscurité. C'est pourquoi, lorsqu'il s'agit d'énumérer ses trouvailles, de les présenter, de les exposer, le savant intitule ses ouvrages, spicilège, analectes, musée* […] *(*BARRET-KRIEGEL, 1988, p.78-79).
[...] *Les voyages mabilloniens déplacent et reclassent les traces par la constitution tâtonnante de musées, de trésors, mais bientôt de répertoires et de catalogues, ils contribuent à ce mouvement de recensement général des sources de << l'Antiquité >> par quoi s'est constituée, avant, bien avant, la formation de l'archivistique contemporaine, la technologie de l'histoire savante*[...] (BARRET-KRIEGEL, 1988, p.81-83).

> Diplomatics and paleography were born as sciences arising from the need to analyze critically documents considered to be forgeries. The problem of distinguishing genuine documents from forgeries was present in the earliest periods of documentation, but until the sixth century no attempt was made to devise criteria for the identification of forgeries. Even legislators did not demonstrate interest in the issue, basically because of the legal principle commonly accepted in the ancient world that authenticity is not an intrinsic character of documents but is accorded to them by the fact of their preservation in a designated place, a temple, public office, treasury, or archives. This principle was open to abuse. Eventually, people began to present forgeries to designated records offices to lend them authenticity. Therefore, practical rules to recognize them were introduced in Justinian's civil code *(Corpus iuris civilis)* and later in a number of Papal *Decretales.* These rules referred only to the external forms of documents created by imperial and papal chanceries, that is, to documents contemporary to the laws, not documents of previous centuries which were often used by authorities to support political or religious claims.

Making a current comparison with the digital context, the importance is known of maintaining both digital records and digital environments could to guarantee authenticity.

Before the *De re Diplomatica* study, other cases of document forgeries had been studied in previous centuries. From the Middle Ages, humanists, popes, bishops, and jurists were concerned about the authenticity of records, "[…] Innocent III (1198-1216) issued a celebrated, if far from watertight, decretal on the detection of false bullae *(Boyle 1967) […]"* (BOYLE, 1992, p.82). In 1358, the Italian humanist Francesco Petrarch (1304-1374) identified one forged record called *"*The *Privilegium Maius"* (The greater privilege), which "[…] proved privileges granted to Austria by Caesar Augustus and Nero in the first century [..]" (DURANTI, 1989, p.12).

In 1440, Lorenzo Valla confirmed the falsehood of the donation made by Constantine to Pope Silvester in the fourth century (DURANTI, 1989, p.12; BOYLE, 1992, p.82; GINZBURG, 2002, p.64; WILLIAMS, 2007, p.3; DOSSE, 2012, p.21). At times, this is shown to be normal behavior during the Middle Ages, in which there was "[…] a notion of 'false' and 'falsification' very different from our own […]" (MERTON,1993, p.XVII).

Following the chronology, during the Middle Ages, a series of violent events occurred within the European territory that was reorganizing itself. In this reorganization, huge amounts of records were tampered with to gain political,

economic, and social recognition (ROGERS, 2015, p.21; MONTOYA-MOGOLLON; TROITIÑO, 2019, p.49-50). With the arrival of the 16th century, the protagonists of the Reformers and Counter-Reformers started to write critical studies about these historical documents, due to the lack of analysis in this context, as is outlined by Leonard Boyle (1992, p.82):

> […] The Protestants, for example, with the *Ecclesiastica Historia of Magdeburg Centuriators* (13 vols., Basle, 1559-1607*).* These were followed in the next century by such critical or semi-critical enterprises as the *Gallia Christiana* of C. Robert (Paris, 1626; later expanded form one volume to four by C. Scevóle and L. de Sainte-Marthe in 1656), the *Italia sacra* of the Cistercian F. Uguelli (9 vols., Rome, 1644-62), and the *Sacrosanta concilia* of Jesuits F. Labbe and G. Cossart (17 vols., Paris, 1671-73).

At this period of cultural and intellectual revolution, the Catholic Church decided to take advantage of the scientific progress of the 17th century, when the figure of Jean Mabillon arises. The intellectual inheritance of previous centuries of authenticity issues provided elements of research for the Benedictine monk to perform his studies. In this context, the *De re diplomatica libri VI* arises as a result of a dispute between two religious orders, the Jesuits and the Benedictines. In a moment of historic convulsion, this dispute was known as the *Bella Diplomatica:* “diplomatics war” (DURANTI, 1989, p.13) or, in words of Randolph C. Head (2012, p.2), “wars over charters”. On the one side, the Jesuit position with Daniel Papenbroeck, who at the time was making recompilation research on all the saints (*Acta Sanctorum)* in 1675:

> In 1643 the Jesuits of the learned society founded in Antwerp by Jean Bolland began publishing the first volumes of their immense series of *Acta Sanctorum*. The Bollandist project was not only to collect testimonies on the lives of the saints but also to evaluate them so as to distinguish facts from legends. In the second tome, appearing in 1675, the Jesuit scholar Daniel Papenbroeck claimed to have demonstrated that a parchment concerning the life of the Merovingian king Dagobert I was a forgery—and other early documents tainted by implication—because, as our critical jargon would put it, they could be deconstructed against their own claims of transparency and immediacy to the transactions they reported (STARN, 2002, p. 397).

The *Acta Sanctorum* was a project that started in 1603 by the monk Heribert Rosweyde. In this process, Daniel Papenbroeck affirmed that several Merovingians diplomas (5th–8th century) maintained in the monasteries were

spurious. Afterwards, the same Papenbroeck recognized that all this controversy served to inspire Mabillon to write his excellent work (SMEDT, 2008; JOHNSON, 1965, p.102; BOYLE, 1992, p.83).

The historian Carlo Ginzburg (2002, p.40) states that without the study of Lorenzo Valla, the work of Mabillon would not have existed. The Mabillon's work began, according to an article by Mette B. Bruun (2010, p.430), when:

> […] he traversed monastic archives, collected information about the history of the monasteries, and copied charters. The use of charters as a source for monastic history was a novelty, and it soon became evident that many of them were unreliable and had been forged either in the Middle Ages or later in order to acquire land or prestige. It was his work with these documents that led to Mabillon's identification of sets of criteria which might be used in assessing the authenticity of historical texts. These criteria were presented in his main work *De re diplomatica* (1681) […]

The success of Mabillon's investigation, unlike previous works produced from the 11th century was due to his method: first, its neutrality, […] in stark contrast to Valla's polemical rhetoric […] (BRUUN, 2010, p.430). Second, *De re diplomatica* (along with the foundation of Paleography outlined in this treatise), had a meticulous and systematic methodology where each record was described and analyzed in the almost 900 pages of the book.

His friend and fellow Benedictine, Bernard de Mountfaucon, continued with the legacy of Paleography study, and he "[…] published his study of Greek scripts and entitled it *Palaeographia Graeca"* (JOHN, 1992, p. 5*).* Both Jean Mabillon and Bernard Mountfaucon have historical recognition in the pantheon at the Abbey *of Saint-Germain-des-Prés* in France, alongside René Descartes. This fact is both highlighted and criticized by some medievalists and church historians (STARN, 2002, p.397).

With this analysis of Mabillon's influence, the object of study among historians, diplomatists, and even the archivists becomes clearer. The author François Dosse (2012, p.25-28) outlined this idea when he said that different from the ancient archives, it was mainly the ecclesiastical archives which were considered to be natural sources of authenticity, a notion that had started with the criticism of Valla and was reaffirmed with the research of Mabillon:

> This new discipline constituted by diplomatics theme has a function to contribute to formulating the rules that allow differentiating and classifying old documents, to judge the old

> titles. The erudite study deals with a document in its content, but it is also attentive to the material supports used: the type of ink, the parchments, the letters, the stamps, the formulas, etc. Thanks to diplomatics, Mabillon registered the History in the series of disciplines of knowledge and accentuates the distance in relation to the literature, from where the historical genre comes from, in the name of the strict rules for compliance in the approach to archival material. With diplomatics, what disappears are the arrangements of medieval historians, which juxtapose military and diplomatic narratives with narratives of divine prodigies. With Mabillon, History is based on proven documents and opens the way for an enormous archival effort, to extract from them authenticated letters that will become our heritage as the community of scientific historian. As Marc Bloch believed: "In that year -1681- on criticism of documents and archives was founded". Although diplomatics makes a decisive contribution to forming the foundations of historical scholarship, it also has its limits, both philosophically and epistemologically (DOSSE, 2012, p.25-28, our translation)[61].

3.2 DIPLOMATICS: AN AUTONOMOUS OR AUXILIARY SCIENCE?

Why is this science called Diplomatics? Many of the documents preserved in archives from de Middle Ages until the 18th century were known as diplomas due to their solemnity and/or their legal value. Therefore, Diplomatics became the science that addressed the authenticity of diplomas, which today are called documents or records.

The etymology of “Diplomatics” or “Diplomatic” has its roots in the Greek: *διπλωματικός*, that means “diploma” (*δίπλωμα)* with the prefix *“di” (δι),* meaning “two”, because, in classic antiquity, the documents were built in two parts, folded in on themselves and closed (DURANTI, 1989, p.12; PIQUERAS, 1999,

[61] *Essa nova disciplina constituída pela diplomática tem como função contribuir para formular com clareza as regras que permitem distinguir e classificar os documentos antigos, julgar os velhos títulos. O estudo erudito trata do documento em seu conteúdo, mas também está atento aos suportes materiais utilizados: o tipo de tinta, as folhas dos pergaminhos, a figura das letras, os selos, as fórmulas etc. Graças à diplomática, Mabillon inscreve a história na série das disciplinas de conhecimentos e acentua a distância em relação à literatura, de onde vem o gênero histórico, em nome das regras estritas de conformidade na abordagem da massa arquivística. Com a diplomática, o que desaparece são os arranjos dos historiadores medievais, que justaponham narrativas militares e diplomáticas a narrativas de prodígios divinos. Com Mabillon, a história fundamenta-se em documentos comprovados e abre caminho para um enorme esforço arquivístico, para extrair deles as cartas autenticadas que se tornarão o patrimônio comum da comunidade historiadora científica. Como escreve Marc Bloch: “naquele ano -1681- foi definitivamente fundada a crítica dos documentos dos arquivos”. Embora a diplomática contribua de maneira decisiva para constituir os fundamentos da erudição histórica, ela também tem seus limites, tanto de ordem filosófica como epistemológica* (DOSSE, 2012, p.25-28).

p.192). This sort of format was called diptychs, which were the heirs of the waxed tablets that remained closed (*πλωμα)* after being used, intending to preserve the written information within. If the information was relevant, it was then transcribed onto paper, and the tablets were scraped and waxed again to be reused another time (ROMERO-TALLAFIGO, 1994, p.14-15).

The wax tablets were also used to educate children at the beginning of the Roman Empire due to their capability of reuse. Other written supports included the clay used by the Sumerian civilization or the papyrus used by the Egyptians. In medieval times, another kind of support appeared made from the skin of goat or sheep called parchment, and although it was a more rigid support, it could also be reused. The wax tablets and the parchment were called “palimpsests”, which means, “scraping again”. This is interesting because according to the hypothesis of Jason Bengtson (2012), we are currently living in a similar time of digital palimpsest, due to the ease of writing, rewriting, and erasing digital information.

Diplomatics arose in the 17th century as a methodology to provide solutions to the concerns of authenticity being challenged at the time. In the 18th century, Diplomatics strengthened its *corpus* with forensics arts and legal matters (ROMERO-TALLAFIGO, 1994, p.22). In the 19th century, it was included as a discipline in various faculties of law in Europe. In the late 19th and early 20th centuries, it became a historical approach and identified as an “auxiliary science”. The crisis came in the mid-20th century, due to the exhaustion and the difficulty of providing analysis elements to other knowledge fields. Therefore, Diplomatics had to re-examine its core philosophy and look for new horizons of research.

From being the auxiliary science of history in the 19th century, Diplomatics became the transcendental and the “little history” of documentation (ROMERO-TALLAFIGO, 2004, p.140, our translation). It is considered by some historians and archivists as an auxiliary science, because it contributed as a methodology to historical science in the 19th century (BAUTIER, 1961; BOYLE, 1992; JOHN, 1992; BLOCH, 2002; ROMERO-TALLAFIGO, 2004), along with other auxiliary sciences such as Paleography, Sigillography, Philology, Heraldry, and Numismatics. With the creation of Diplomatics as a knowledge

area, historical science established a methodology and a scientific character, moving away from both philosophy and rhetoric:

> An art or a science does not formulate the rules of its technique until it becomes independent and self-conscious. So long as History was regarded as a branch of philosophy or rhetoric or oratory, no one felt the need of observing any special rules of technique apart from grammar or formal logic. Only when the circumstances gave History an acknowledged role apart from other sciences or arts, were any attempts made to formulate rules of historical method; and these circumstances did not occur until the seventeenth century[62]; They were of many kinds. the study of classical antiquity had revived interest in the forgotten Greek and Roman histories. Men began to acquire a certain historical sense- a feeling of continuity between the ancient world and their own. The religious revolt of the sixteenth century led to a zealous searching of ecclesiastical records, of the writings of the church fathers, and of the lives of the saints rather, it must be admitted, to find arguments to opponents than to establish the truths of History. Yet the outcome was a measurable increase of interest in historical study (JOHNSON, 1965, p.103).

Heather MacNeil (2000, p.29), highlights this evolution of Diplomatics and its role as an auxiliary science to historical concerns:

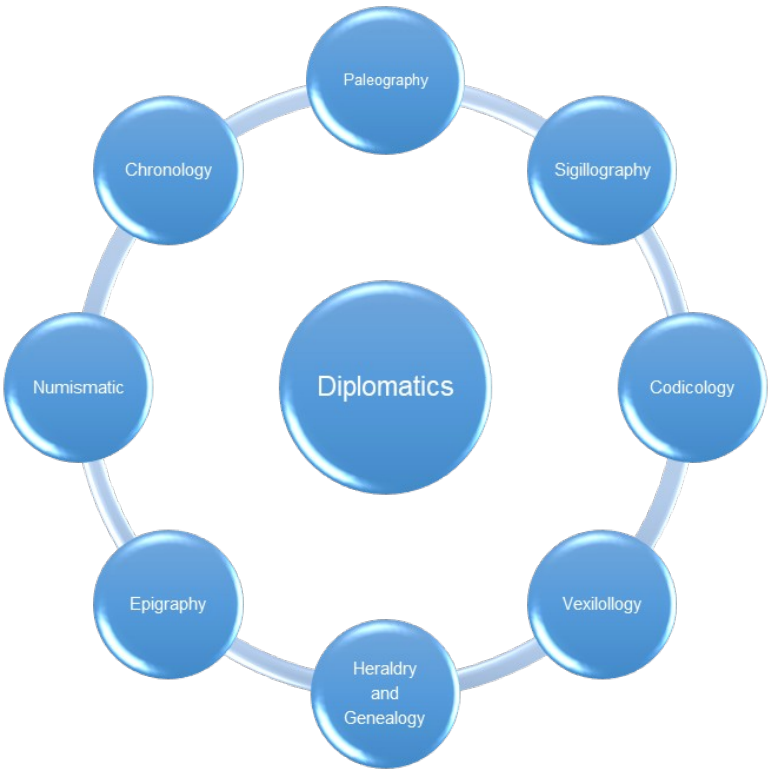
> For medieval documents, external criticism included the application of concepts and principles of diplomatics. The original purpose of diplomatics had been to determine a record ´s authenticity for legal purposes and that purpose continued into the eighteenth century when its concepts and principles were incorporated into the curriculum of many European faculties of law. By the end of the nineteenth century, however, under the influence of classical philology and the scientific school of historiography, diplomatics had emerged as an auxiliary science of History and a discipline in its own right. The emergence of diplomatics as an academic discipline was helped along by the founding of the *École des chartes* in France in 1821 and the Austrian Institute of Historical Research in Vienna in 1854. Both institutions aimed to promote the study of the auxiliary sciences of history and, particularly, paleography and diplomatics.

As Manuel Romero-Tallafigo (2004) points out, today Diplomatics focusses on guaranteeing the authenticity of records. Diplomatics has left behind its role as just an auxiliary science that was consolidating analysis elements from other disciplines, to becoming a “real” science. The relationship

[62] (Explanatory note by the author): Several writers in the early seventeenth century anticipated this differentiation of history from other subjects, but C.J. Voss is the first, in his *Ars historica* (1623), to state effectively the claims of history as an independent subject of study. These early works contribute little or nothing to the methodology, so far as problems of evidence are concerned.

with Archival Science in the 20th century forced Diplomatics to renew and revise its framework.

Figure 3 – DIPLOMATICS AND THE RELATIONSHIP WITH OTHER SCIENCES



SOURCE: Elaborated by the author

Figure 3 establishes the relationship between Diplomatics and the "auxiliary sciences" to shape its core of record analysis. However, it will be reductionist to try to argue that Diplomatics is a science just because of its relationship with other sciences. Diplomatics is a science because of its established theory and the practice that survived and evolved through time. Its core as Caroline Williams (WILLIAMS, 2007, p.5) notes:

> […] is that all records can be analyzed, understood and evaluated in terms of a system of formal elements that are universal in their application and decontextualized in nature. Or, as Brooke put it, 'the need to study it [diplomatic]as a coherent science and not simply to apply its practical uses within one's own specialism' […]

This discussion was approached in the early of 20th century by Charles-Victor Langlois & Charles Seignobos (2009, p.28), who were reluctant to consider Diplomatics as an “auxiliary science” or an “auxiliary science of History”, because of two main reasons:

> We are now in a position to examine to some purpose the hazy notion expressed by the phrase, "the sciences auxiliary to history." We also read of "ancillary sciences," and, in French, "*sciences satellites*." None of these expressions is really satisfactory. First of all, the so-called "auxiliary sciences" are not all of them *sciences*. Diplomatic, for example, and the History of Literature are only systematised accumulations of facts, acquired by criticism, which are of a nature to facilitate the application of critical methods to documents hitherto untouched. On the other hand, Philology is an organized science, and has its own laws.
>
> In the second place, among the branches of knowledge auxiliary—properly speaking, not to history, but to historical research—we must distinguish between those which every worker in the field ought to master, and those in respect of which he needs only to know where to look when he has occasion to make use of them; between knowledge which ought to become part of a man's self, and information which he may be content to possess only in potentiality. A mediævalist should know how to read and understand mediæval texts; he would gain no advantage by accumulating in his memory the mass of particular facts pertaining to the History of Literature and Diplomatic which are to be found, in their proper place, in well-constructed works of reference.

The vision of Langlois & Seignobos in the above quotation, seems appropriate because the science must be called either a science or not a science.

“Auxiliary science” is an approach with a difficult scientific character. Moreover, Langlois & Seignobos who do not consider Diplomatics to be a science do so for two reasons: first, because they underpin their scientific study from the standpoint of historians with the consolidation of the history as a science. Second, because the aforementioned study was released in 1867, in a historical period where the practice of positivism remained as the only paradigm to define science. Ultimately, the study undertaken by Langlois & Seignobos was important because, besides analyzing the function of Diplomatics in the course of History, it started a fruitful academic discussion. This scientific legacy was addressed and extended upon by the historian Marc Bloch in his research, “The Historian’s Craft” (1949).

3.3 FROM DIPLOMATICS TO ARCHIVAL SCIENCE

By analyzing how Diplomatics became an effective discipline for archival purposes, several significant elements and authors emerged from the 17th century up to the 20th century. This process carries on from Mabillon's treatise with the study performed by the Monks Dom Charles-François Toustain (1700-1754) and Dom René-Prosper Tassin (1697-1777), who belonged to the same Benedictine Congregation of Saint-Maur, in their "*Nouveau traité de diplomatique"* developed in 1750, where they analyzed other kinds of records, such as juridical or solemn documents. Their work was rooted in the notion that the records belonged to an archival fond and it was not an isolated element (BAUTIER,1961, p.201-202; RONDINELLI, 2011, p.108). In addition, the Monks drew in their work a sort of especial Diplomatics "[…] for records of the same provenance […]" (DURANTI, 2009, p.1).

In 1809, the Italian Angelo Fumagalli (1773-1809) wrote "*Delle istituzioni diplomatiche",* where he suggests some instructions to maintain and preserve the diplomas. Natália Tognoli explains in this regard that "Although timidly, Fumagalli is the first to make use of the expression "Archival Science", and the first to address its principles of formation, distribution, and organization" (TOGNOLI, 2013, p.43).

The 19th century started with a new breath of democracy, and archives were, foremost, to research and rescue the national spirit. In this century, a complementary work is evident between Archival and Diplomatics. The legal processes were vanishing slowly to give rises to another field of knowledge.

The historian Theodor Von Sickel (1826-1908), considered as the "father" of the modern Diplomatics and Especial Diplomatics, wrote the "*Beiträge zur Diplomatik*", between 1861 and 1882, and the *"Acta regum et imperatorum Karolinorum digesta et ennarata"*, in 1867, which are the most representative academic production. In those studies, Sickel divided the intrinsic elements into "text and protocol" Diplomatics (TOGNOLI, 2013, p. 53). Elements that are still currently used.

Julius Ficker (1826-1902) contributed in the late 19th century, with the time between the action (*action)* and the moment of the record-creation

(*conscription)*. These two moments are relevant for business contexts to understand the transaction of the documentary production, along with the people that participate during the process.

The archival view must acknowledge Robert-Henry Bautier for his study, "*Leçon d'ouveture du cours de diplomatique à l'Ecole des Chartes",* in 1961, which contained pioneering research to analyze the possibility of employing the Diplomatics elements to Archival Science. The study was considered the third

> *"*turning point", as the expansion of the chronological and territorial limits of its problematic, a decision proposed by Bautier to face the crisis of exhaustion that Diplomatics experienced in the 1950s, when there was stagnation across Europe, compared to the golden period experienced by art critical in the days of Sickel and Ficker. (TOGNOLI, 2014, p.92, our translation)[63].

María Belén Piqueras García (1999, p.197, our translation) describes the contribution made by Teodore Sickel and Julius Ficker:

> In the 19th century, the work of Teodore Sickel was relevant in which his most representative works of modern Diplomatics were: *Beiträge Zur Diplomatik* e *Actra regum et imperatorum Karolinorum*. In the same century, Julius Ficker wrote *Beiträge Urkundenlehre*, a work where he established the two stages of the record: *actio & conscriptio*[64].

These two stages of the record outlined by Julius Ficker – *actio* and *conscription* – were the key to understanding the bond between Diplomatics and Archival Science. The record production in the administrative routines starts with an action stage and then its documental materialization. Duranti (1990-91, p.11) calls these the moment of action and the moment of documentation. Comparison can be made with the study of Michael Buckland (1991), "Information as Thing", where the author divides the information process into three moments or stages: as a process, as knowledge, and as a thing: data and documents.

[63] *O terceiro momento decisivo nos estudos diplomáticos, que pode ser considerado também um turning point, é a expansão dos limites cronológicos e territoriais de sua problemática, decisão proposta por Bautier para enfrentar a crise de esgotamento que a Diplomática vivenciava na década de 1950, quando se observou uma estagnação em toda a Europa, em comparação ao período de ouro vivido pela arte crítica na época de Sickel e Ficker*. (TOGNOLI, 2014, p.92).

[64] *En el siglo XIX, fue importante el trabajo del autor Teodore Sickel, representativo de la Diplomática Moderna: Beiträge zur Diplomatik y Actra regum et imperatorum Karolinorum. En ese mismo siglo, Julio Ficker escribió Beiträge Urkundenlehre, el cual estableció la distinción entre las dos fases del documento: actio e conscriptio. (*PIQUERAS-GARCÍA, 1999, p.197).

Bautier's contribution establishes a historic work to show how the idea to bond Diplomatics and Archival Science germinated in the beginning of the 20th century. In his study, the author made a classification of academics that were maturing to join Diplomatics with Archival Science. In this regard, Bautier (1961, p.206) wrote:

> Drawing the conclusion from the premises developed by M. Tessier, M. Dumas came to assert that Diplomatics is not necessarily linked to medieval history: «It would be necessary for the drafting of acts to be studied for the contemporary era with as much scientific spirit as they were for the Middle Ages... There would be a contemporary Diplomatics which would be the counterpart of historical Diplomatics, the only one until now constituted in science"[65]». A revolutionary suggestion which for a long time was not echoing, although Alain de Boüard also insisted on including, in the Album of his Diplomatics Manual, modern documents and even minutes of imperial decrees apostilles by Napoleon I. On the other hand, the eminent professor and archivist of Berlin, Dr. Heinrich-Otto Meisner, had reached the same conclusions, and as early as 1935, he published a small work entitled Aktenkunde 3, where between classical Diplomatics, Urkundenkunde, and the Archivist, Archivwissenschaft, he introduced a new discipline devoted to the forms of administrative papers (Akten) of the 17th and 18th centuries (BAUTIER, 1961, p.206, our translation)[66].

[65] (Explanatory note by the author)*: A. Dumas, dans Le Moyen Age, 1932, p. 29. 2. A. de Boüard, Album, Paris, 1929 : minutes de lettres royaux, 1675 et 1777 (pi. XII et XIII), originaux-minutes d'arrêté et de décrets, 1793-1812 (pi. XV- XVII). 3. Heinrich- Otto Meisner, Aktenkunde. Ein Handbuch für Archivbenutzer, Berlin, 1935. A la base de la nouvelle conception du Dr. Meisner était sa propre expérience d'archiviste et spécialement ses travaux sur les papiers du cabinet royal de Prusse (cf. Zur neueren Geschichte des preussischen Kabinetts, dans Forschungen zur brandenburgischen und preussischen Geschichte, t. 36, 1924)* (BAUTIER, 1961, p.206).
(Translation)*: A. Dumas, in Le Moyen Age, 1932, p. 29. 2. A. de Boüard, Album, Paris, 1929: minutes of royal letters, 1675 and 1777 (pi. XII and XIII), originals - minutes of decrees and decrees, 1793-1812 (pi. XV- XVII). 3. Heinrich- Otto Meisner, Aktenkunde. Ein Handbuch für Archivbenutzer, Berlin, 1935. Dr. Meisner's new conception was based on his own experience as an archivist and especially his work on the papers of the Royal Prussian cabinet (cf. Zur neueren Geschichte des preussischen Kabinetts, in Forschungen zur brandenburgischen und preussischen Geschichte, t. 36, 1924)* (BAUTIER, 1961, p.206).

[66] (Explanatory note by the author)*: Tirant la conclusion de ces prémisses, ainsi mises au point par M. Tessier, M. Dumas en vint à affirmer que la diplomatique n'est pas nécessairement liée à l'histoire médiévale : « Il serait nécessaire que la rédaction des actes fût étudiée pour l'époque contemporaine avec autant d'esprit scientifique qu'elle l'est pour le Moyen Age... Il y aurait une diplomatique contemporaine qui serait le pendant de la diplomatique historique, seule jusqu'à présent constituée en science 1. » Suggestion révolutionnaire qui longtemps n'allait pas rencontrer d'écho, bien qu'Alain de Boüard lui aussi eût tenu à faire figurer dans Y Album de son Manuel de diplomatique des documents modernes et même des minutes de décrets impériaux apostilles par Napoléon 1er 2. De son côté l'éminent professeur et archiviste de Berlin, le Dr. Heinrich-Otto Meisner était parvenu aux mêmes conclusions et, dès 1935, il publiait un petit ouvrage intitulé Aktenkunde 3, où entre la diplomatique classique, l'Urkundenkunde, et l'Archivistique, Archivwissenschaft, il introduisait une discipline nouvelle consacrée aux formes des papiers administratifs (Akten) des XVIIe et XVIIIe siècles* (BAUTIER,

However, four years before the pioneering study of Bautier in 1961, a study by Hilary Jenkinson proposed the idea of applying Diplomatics to Archival Science. In 1957, he wrote “Archives and the Science and Study of Diplomatics” (1980, p.345), which address the Diplomatics can benefits the archival practices:

> […] This brings me - after, I fear, a rather long exordium - to the problem to which I thought I might venture to call your attention on the present occasion: the problem of Selection; of securing (an important, even an urgent, matter of view of those difficulties of labour and expense to which I have referred) the best possible use of our resources for Record Publication. As a whole the question is, of course, too wide to be discussed here. Indeed, its solution involves, if I am not wrong, an interchange of views between publishing bodies, and an organization of co-operative work between them, on a large scale. But there is one criterion for publication, one interest which (as it seems to me) ought to have a strong claim of attention of all publishing bodies; and one aspect of it that I think might be of special concern to Archivist. That interest is in one word *Diplomatic* or, to give it the spelling under which it first made its bow to English scholars, *Diplomatique.* This title was given a few years ago by a member of this Society[67] to the study of documentary form in one particular category of English Archives, those of Quarters Sessions; which was a considerable extension of the original narrow sense of the term[68]. I wish to extend it yet further and to suggest that in that extend sense the study might offer an opportunity for active publishing work of a kind particularly suited to professional archivist.

Both Hilary Jenkinson (1957) and Robert-Henri Bautier (1961), each with their studies and approach, tried to establish the match between Archival and Diplomatics research. Bautier systematized the possible benefits of the Diplomatics studies within Archival Science and focused his ideas on the most relevant diplomatists, such as Julius Ficker (1877), Arthur Giry (1901), George Tessier (1930), and Auguste Dumas (1932). In its turn, the writing of Jenkinson has an interesting view from the Anglo-Saxon societies, about an embryonic idea realized by an archivist for Archival science.

1961, p.206).

[67] (Explanatory note by the author): Mr. J.H. Hodson in a paper published in 1951 in No. 8 of the Bulletin of the Society of Local Archivist.

[68] (Explanatory note by the author): As used by its early exponents, it applied only to the original diplomata issued by authority.

The 20th century started with the authors described at the beginning of this section and the importance of Hilary Jenkinson and Robert-Henry Bautier in the middle of the century to approach the Diplomatics and Archival Science as complementary disciplines. This idea was consolidated later, and a new science was created with various names, such as, “Contemporary Diplomatics”, “Archival Diplomatics”, and “Documentary Typology”[69] (TOGNOLI and RODRIGUES, 2018, p. 46). In table 2, Natália Tognoli (2013, p.146) presents the evolution of the Diplomatics, from the individual concept of documents or diplomas to the archival concept of archival unit.

These two mentioned academic views helped provide the opportunity to unite Archival to Diplomatics. This union has two paramount gains: First, the opportunity to redeem Diplomatics in the 20th century from being focused only on studies and records of Middle Age, which was a constant striving by various diplomatists for years. Second, it is a golden opportunity for archivists to apply the Diplomatics elements and enhance the processes of authenticity of the archival activities.

Table 2 – OBJECT OF STUDY FOR DIPLOMATICS ACCORDING TO SCIENTIFIC STUDIES

AUTHORS	OBJECT OF STUDY OF DIPLOMATICS
PAPEBROCH, 1675	Diploma: solemn and authentic documents Synonymous for: *Instrumentum/Charta/Diploma*.
MABILLON, 1681	Authentic instruments and solemn acts: *Chartes eclésiatiques* (ecclesiastical documents) *Diplomes royaux* (royal diplomas) *Actes publics* (public documents) *Cédules privée* (private documents).
MAFFEI, 1727	Diploma: most noble documents from supreme authority.
TASSIN; TOUSTAIN, 1750-1765	Authentic diplomas endowed with authority. Synonymous with: Letters/Instruments/Memoirs/Papers/Scriptures/ Bulls/Parts/*Cédules*/Rolls/Wills/Privileges/Cartulary/TreatiesTitles.
FUMAGALLI, 1802	Synonym for: Diploma/Instrument/Act/Testament/Contract/Letter/Epistle/Monument.
SICKEL, 1867	*Urkunde*: Written testimony, written in a specific way – variable concerning place, time, person, business, on facts of a legal nature.

[69] Each one with their specific approaches as was described in the introduction chapter.

BRESSLAU, 1889	Written declarations in specific ways, even if they vary concerning the person, the time, or the objective, intended to serve as a testimony of facts of a legal nature.
GIRY, 1893	*Acte*: written testimony, written in a specific way - variable about the place, time, person, business, about facts of a legal nature.
PAOLI, 1898	Written testimony of a fact of a legal nature, compiled according to the observation of certain specific forms, which are intended to provide faith and strength of evidence.
BOÜARD, 1929	*Acte*: written testimony, written in a specific way - a variable with the place, time, person, business, on facts of a legal nature.
TESSIER, 1956	*Actes instrumentaires:* Authentic writings or under private authentication, intended for the knowledge of the accomplishment of a legal act.
BAUTIER, 1962	All archival documents.
CARUCCI, 1987	Elementary archival unit of a juridical nature or not.
DURANTI, 1989	Elementary archival unit of a juridical nature or not.

SOURCE: Tognoli, (2013, our translation)

In the early the 20th century, Hillary Jenkinson and Robert-Henry Bautier proposed the possibility of applying Diplomatics elements to Archival Science. Therefore, in the second half of the 20th century, the work of the Italians Paola Carucci (1987) and Luciana Duranti (1989) complemented the archival contexts with the Diplomatics concepts. This project reached until the digital context, where academic contributions from digital Diplomatics are increasingly necessary to establish the trustworthiness of the born-digital records.

3.4 DIGITAL DIPLOMATICS

From the end of the 20th century onwards, the digital world has changed the way reality is conceived. With this new reality, the scientific community had to adapt and provide new forms of thought and practices to try to solve these challenges. Diplomatics and Archival Science, as was written in the previous section, unified the core concepts when approaching the issues of born-digital records.

This section will explore Diplomatics and Archival studies for further understanding about how these concepts are dealt with in the digital realm.

Additionally, how these concepts work to guarantee the accuracy, reliability, and authenticity of born-digital records shall be discussed. Later chapters will explore how Diplomatics can establish a relationship with digital Forensics, and how these sciences can work together to establish the trustworthiness within digital contexts.

InterPARES (2000) analyses four concepts that provide possible solutions documentary form, annotations, medium, and context. It is noted how these conceptual elements have worked within traditional Diplomatics itself. The connection with Archival Science helped to enhance the issues of authenticity in bureaucratic routines.

The concept of the documentary form deals with “the rules of representation according to which the content of a record, its administrative and documentary context, and its authority are communicated” (INTERPARES, 2000, p. 1). That is, the composition of the record, the form that the record is managed in its diverse contexts, and the objective of its communication. The extrinsic and intrinsic elements belong to the documentary form.

The extrinsic elements are defined as “the elements of a record that constitute its external appearance” (INTERPARES, 2000, p. 1), meaning the way that we understand the record through our eyes. The concepts of the InterPARES Project as an analytical template are outline here because it presents an accurate approach to the characteristics of born-digital records. Thus, the extrinsic elements in the digital contexts are described in table 3:

Table 3 – EXTRINSIC ELEMENTS OF THE DOCUMENTARY FORM

1. Documentary Form
1.1 Presentation Features *Definition:* A set of perceivable features (graphic, aural, visual), generated by means of encoding and program instructions, and capable, when used individually or in combination, to present a message to our senses.
1.1.1. An Overall Presentation *Definition:* The record’s overall information configuration, i.e., the manner in which the content is presented to the senses.
1.1.1.A.i Text *Definition:* Words, numbers, or symbols. (***Authors Note***): The InterPARES 2 (2008, p.47) Glossary definition clarifies this point further for a better understanding.

n., A collection of words, numbers, or symbols that conveys meaning as language.
n., [documentary form] The central section of a document, which contains the action, including the considerations and circumstances which gave origin to it, and the conditions related to its accomplishment.

1.1.1.A.ii Graphic
Definition: A representation of an object or outline of a figure, plan, or sketch by means of lines. A representation of an object formed by drawing.

1.1.1.A.iii. Image
Definition: An artificial imitation or representation of the external form of any object, or an optical appearance or counterpart of an object, such as is produced by rays of light, refracted as through a lens, or falling on a surface after passing through a small aperture. A subset of image is moving images, which are visual images, with or without sound that, when viewed, present the illusion of motion.

1.1.1.A.iv Sound
Definition: Aural representation of words, music, or any other manifestation of sound.

Combination of More Than One of the Above.

1.1.1.B. Specific Presentation Features
Definition: specific aspects of the record's formal presentation that are necessary for it to achieve the purpose for which it was created.
Examples: Specific presentation features might include but are not limited to the following:
• Special layouts
• Deliberately employed type fonts
• Deliberately employed colors
• hyperlinks
• graphic indication of attachments
• sample rate of sound files
• resolution of image files
• scales of maps

1.1.2 Electronic Signature
Definition: a digital mark having the function of a signature in, attached to, or logically associated with a record, which is used by a signatory to take responsibility or give consent to the content of that record, and which may be used to verify its authenticity.

1.1.2. An Electronic Seal
Definition: specific electronic means of authenticating a record or ensuring that it is only opened by the intended addressee. It is distinct type of electronic signature.
Example: An electronic seal might include but is not limited to the following:
• digital signature, i.e., an electronic signature based on public key cryptography.

1.1.2.A.i Authentication Certificate of Trusted Third Party (T.T.P.)
Definition: an attestation issued by a T.T.P. for the purpose of authenticating the ownership and characteristics of a public key. Such attestation appears in conjunction with the digital signature of the author of a record and is itself digitally signed by the T.T.P.

1.1.3 Digital time-stamp Issued by a Trusted Third Party (T.T.P.) Digital time-

stamp Issued by a Trusted Third Party (T.T.P.) *Definition:* an attestation by a T.T.P. that a record was received at a particular point in time. **1.1.4 Special Signs** *Definition:* Symbols which identify one or more of the persons involved in the compilation, receipt, or execution of the record. *Examples:* Special signs might include but are not limited to the following: • digital watermarks • organization crest • personal logo • originator identifier

SOURCE: Quoted from INTERPARES (2000)

The attributes of the extrinsic elements presented in table 3, correspond to the external appearance of digital records. Depending the complexity and necessity, digital records can have all these attributes or just some elements. The model presented by InterPARES, attempts to approach the general elements. In addition, the late elements such as, electronic signature, electronic seal, authentication certificate by a trusted third party – T.T.P., and special signs, to reinforce the authentication of records to be admissible as evidence in several contexts.

The intrinsic elements are defined as “the elements of a record that convey the action in which the record participates and its immediate context” (INTERPARES, 2000, p. 3). That is, an intellectual message fixed in support. In the analogical support, this element traditionally always remains together with the message and cannot be separated. However, in the digital environment, both the message and the support can work separately. An example would be a Word file record, which can be migrated to other software, such as a Portable Document Format (PDF), and its content can remain unaltered. The intrinsic elements in digital contexts are described in table 4:

Table 4 – INTRINSIC ELEMENTS OF THE DOCUMENTARY FORM

1.2 Intrinsic Elements of Documentary Form *Definition*: The elements of a record that convey the action in which the record participates and its immediate context.
1.2.1 Name of Author *Definition:* Name of the physical or juridical person having the authority and capacity to issue the record or in whose name or by whose command the record has been issued. *Note:* In traditional records, the name of the author typically appears as the name

expressed in the letterhead (*entitling*), in the initial wording of the record (*superscription*), and/or at the bottom of the record (*subscription*). It may be the same name as that of the writer, and, with records that are electronically transmitted, may correspond to the name of the originator. However, the name of the author only validates the record when it has the function of an attestation.
1.2.2 Name of Originator *Definition:* Name of the person assigned the electronic address in which the record has been generated and/or sent. *Note:* When the name of the originator is different from the name of the author of the record, the law usually considers the originator's name as the indication of the person responsible for issuing the record.
1.2.3 Chronological Date *Definition:* The chronological date is the date, and possibly the time, of the record included in the record by the author or the electronic system on the author's behalf in the course of its compilation.
1.2.4 Name of Place of Origin of Record *Definition:* The name of the geographic place where the record was generated, included in the content of the record by the author or the electronic system on the author's behalf.
1.2.5 Name of Addressee(s) *Definition:* The name of the person(s) to whom the record is directed or for whom the record is intended. *Note:* In traditional records, this element corresponds to the *inscription* and usually occurs at the top of the record. With electronic mail records, the name of the addressee(s) continues to appear in the top portion of the record (i.e., in a header).
1.2.6 Name of Receiver(s) *Definition:* The name of the person(s) to whom the record is copied for information purposes.
1.2.7 Indication of Action or Matter *Definition:* The *subject* line(s) and/or the *title* at the top of the record.
1.2.8 Description of Action or Matter *Definition:* Presentation of the ideal motivation (*preamble*) and the concrete reason (*exposition*) for the action as well as the action or matter itself (*disposition*).
1.2.9 Name of Writer *Definition:* The name of the *person* having the authority and capacity to articulate the content of the record. *Note*: In traditional records, the name of the writer usually appears at the bottom of the record and is typically constituted by the *subscription*. The name of the writer may be the same as the name of the author (and perhaps of the originator).
1.2.10 Corroboration *Definition:* Explicit mention of the means used to validate the record. *Note*: "to validate" means to make legally valid; to grant official sanction to by marking; to support or corroborate on a sound or authoritative basis.
1.2.11 Attestation *Definition*: The written validation of a record by those who took part in the issuing of it (author, writer, countersigner) and by witnesses to the action or to the signing of the record. *Note:* In traditional records, the attestations usually appear as *signatures* at the bottom of the record (the eschatocol). However, some records have the attestation in the protocol. For example, memoranda may be signed or initialled beside the *superscription*. With electronic records, such as electronic mail messages, the attestation appears in the header of the message.
1.2.12 Qualification of Signature *Definition:* The mention of the title, capacity and/or address of the persons signing a

record. *Note:* Qualification of signature may follow either a *subscription* or a *superscription*.

SOURCE: Quoted from INTERPARES (2000)

These internal elements increase their importance due to the new forms of digital records. However, it is possible to recognize that the written structure remains the same in digital records. The mean difference with analog records is the form as the records are transmitted to recipients. To date, the use of emails reinforced the administrative forms of communications and constitute an important subgroup of born-digital records: "[…] is the modern day equivalent of paper-based correspondence […]" (BYERS, 2020, p.3).

Another concept that functions in Diplomatics is the annotations, which take place in the life cycle of the records, described by the InterPARES (2000) as "additions made to a record after it has been created". Table 5 lists the types of the possible annotations of a record in its business processes:

Table 5 – THE ANNOTATIONS MADE TO A RECORD

2. Annotations
2.1 Annotations Made in the Course of Executing the Record *Definition:* Additions made to a record after it has been created as part of the formal execution phase of an administrative procedure. *Note:* Normally this sort of annotation is used only for the authentication and registration of legal records whose form is required by law, e.g., the registration number added to a land deed by the land registry office, or the statement of the authenticity of the signatures in a will. *Examples*: Such additions might include, but are not limited to the following: • **Priority of Transmission** *Definition:* Indication of the priority in which a record is to be transmitted. • **Transmission Date, Time and/or Place**. *Definition*: The *date*, *time*, and/or *place* when the record leaves the space in which it was generated. *Note*: Transmission date, time and/or place is usually added by the electronic system. • **Indication of Attachments** *Definition*: Mention of autonomous items that have been linked inextricably to the record before transmission (i.e., added during its execution) in order for it to accomplish its purpose.
2.2 Annotations Made in the Course of Handling the Business Matter to which the Record Relates *Definition:* Additions made to the record in the course of handling the business matter in which the record participates and reflecting actions taken subsequent to the creation of the record for the purpose of handling the action or matter in which the record participates. Such additions might include, but are not limited to the following: • Received Date and Time

• Name of Handling Office • Action taken • Dates and Times of Further Action or Transmission
2.3 Annotations Made in the Course of Managing the Record for Records Management Purposes *Definition*: Additions made to a record for the purpose of handling the record itself and reflecting actions taken subsequent to the creation of the record for the purpose of managing it as part of the agency's records. Such additions might include, but are not limited to the following: • **Archival Date** *Definition*: The date on which a record is officially incorporated into the creator's records. • **Draft or Version Number** *Definition:* The unique identifier assigned to sequential drafts or versions of the same record, added to the record when it is saved. • **Record Item Identifier** *Definition*: The progressive number of the record within the dossier or, in the absence of dossiers, within the specific class. • **Dossier Identifier** *Definition*: The identifier for the dossier in which the record belongs. *Note*: It may be constituted by the name of a person or organization, a symbol, a progressive number, a date, or a specific topic within the class's general subject. • **Class Code** *Definition*: The code of the class to which the record belongs, as it appears in the classification scheme, thus connecting it to other records in the same class. • **Registration Number** *Definition*: The consecutive number added to each incoming or outgoing record in the protocol register, which connects it to previous and subsequent records made or received by the creator. • **Name of Creator** *Definition*: The name of the *person* in whose archival fonds the record exists.

SOURCE: Quoted from INTERPARES (2000)

Even though the annotations continue being used as an aid in the three moments presented above, in digital records, these annotations are being surrogated by automated systems. Same way that in the intrinsic elements, annotations are automatically configured in digital technological systems such as emails, so that the difficulties increase to try to identify them. To face these problems, are developing some scientific projects, such as the Review, Appraisal, and Triage of Mail – RATOM[70], centered on managing and preserving emails and the information embedded in these sorts of digital objects.

The medium is another element addressed in Diplomatics and is "the physical carrier of the message" (INTERPARES, 2000, p.6). This definition was extended in 2008, making a both generic and Diplomatics definition:

[70] In: https://ratom.web.unc.edu/

> medium n., The physical material or substance upon which information can be or is recorded or stored […]
> n., [diplomatics] An extrinsic element of documentary form that comprises the material carrying the message of a document (INTERPARES, 2008, p.30).

Thus, the medium is defined as the support where the message is fixed, which can be in the analogical context, a paper format, stone, clay, wax, parchment, wood, etc. In a digital context, as already explained, the support can be separated from the content or intellectual message and can be described as optical support, such a CD-ROM, or magnetic support, such as a hard drive, or a USB (Universal Serial Bus). According to InterPARES (2008), the medium is divided into “analogue medium” and “digital medium”:

> Analogue medium n., Physical material, such as a paper, parchment, stone, clay, film, or certain types of magnetic audio- and videotape, used for storage of analogue data […] (p.4).
>
> Digital medium n., Physical material, such as a CD, DVD, DAT or hard disk, used for storage of digital data (p.16).

Finally, the context is where the record has been created or produced. In the definition of InterPARES (2000, p.6), context is “The framework of action in which the record participates”. These sorts of contexts, following the examples of InterPARES, are defined in table 6:

Table 6 – THE CONTEXTS OF THE RECORDS

3. Context
3.1 Juridical-Administrative Context *Definition*: The legal and organizational system in which the creating body belongs. *Note*: Indicators of juridical-administrative context are laws, regulations, etc.
3.2 Provenancial Context *Definition*: The creating body, its mandate, structure, and functions. *Note*: Indicators of provenancial context are organizational charts, annual reports, the classification scheme, etc.
3.3 Procedural Context *Definition*: The business procedure in the course of which the record is created. *Note*: In some organizations, the business procedures are integrated with documentary procedures. Indicators of procedural context are workflow rules, codes of administrative procedure, classification schemes, etc.
3.4 Documentary Context *Definition*: The fonds to which the record belongs and its internal structure. *Note:* Indicators of documentary context are classification schemes, record inventories, indexes, registers, etc.
3.5 Technological Context *Definition*: The characteristics of the technical components of the electronic system in which the record is created. **3.5.A. Hardware**

3.5.A.i. Storage
Definition: The medium that stores data in the system.

3.5.A.i.a. Main Memory (a.k.a. primary memory)
Note: This type of storage is fast, different parts of it can be accessed randomly (rather than sequentially) and directly by the CPU/Microprocessor. Thus, for a process to run or a file to be accessed, it must be loaded, at least partially, into the main memory. The main memory is provided via integrated circuit chips and does not involve mechanical movements. It is "volatile" in that its contents will be lost when a computer system is shut down.
Example: Random Access Memory (RAM), cache memory

3.5.A.i.b. Secondary Storage (a.k.a. secondary memory)
Note: This type of storage is slower than main memory and is cheaper. It involves mechanical parts and movements that contribute to its low speed of access. It is non-volatile in that shutting down the system will not result in loss of data on the secondary storage. Compared to magnetic tapes, secondary storage devices are randomly accessible.
Examples: hard disks, magnetic or optical disks, CD
ROM's, DVD's.

3.5.A.i.c. Tertiary Storage
Note: This type of storage is sequentially accessible only and is used for long-term file preservation.
Examples: magnetic and digital tapes.

3.5.A.i.d. Storage for Security/Recovery Purposes
Note: This type of storage is used as a protective measure against the possibility of catastrophic loss. It tends to be overwritten at regular intervals and is not intended to serve the purpose of long-term file preservation.
Examples: magnetic and digital tapes.

3.5.A. ii. CPU/Microprocessor
Definition: The primary resource for job/instruction execution.
Note: This resource can be broken down further into its own subsystems (e.g., registers and logic units). Its speed of executing instructions is considerably higher than the speed of accessing main memory. It interfaces directly with main memory, so a record must be loaded into main memory from secondary or tertiary storage before it can be readable.

3.5.A.iii. Network
Definition: The primary source of communication between systems or components thereof.
Note: Network encompasses its own types of hardware, software, and architectures.

3.5.A. iv. Peripheral Devices
Examples: Mouse, monitor, keyboard, printer.

3.5.A.v. Architecture
Definition: The configuration of hardware components and their interfaces.
Examples: CPU architecture, mother board architecture, system architecture (i.e., serial, pipelined, parallel, distributed, client-server), Network architecture.

3.5.B. Software

3.5.B.i. Operating System

Definition: The system which manages, controls, protects, and facilitates the use of hardware resources in the electronic system.
Note The following can be identified as functions and main modules of an operating system: process management (scheduling, switching, deadlock management, memory management, secondary storage management, storage scheme (data mapping), disk scheduling, virtual memory, management, file system (distributed, file format, directories), interrupt handling, user interface, device, and network interface. The way an operating system is configured (parameterized) may affect certain aspects of data and files in the system. For example, there may be a limit imposed on the size of a data file.

3.5.B. ii. System Software

Definition: Software that creates an environment for application programs to be created, executed, and maintained, typically through system calls to the operating system.
Note: System software is sometimes referred to as system utilities or system tools.
Examples: languages (machine language, high-level languages), compilers, interpreters and translators, coding (compression, encryption), system utilities (i.e., hard disk defragmentation tools, virus detectors, etc.)

3.5.B.iii. Network Software

Definition: network software manages networks and their resources in order to meet the communication requirements of one or more applications.
Examples: protocols, routing, and switching software.

3.5.B. iv. Application Software

Definition: Software that constitutes any type of program that is tailored to satisfy real-world needs and requirements.
Note: Application software varies widely in nature and complexity, as the range of applications using this type of software is quite diverse. Application software may be developed in-house by the organization that uses it, custom-made by another company or contractor for the organization that uses it, or purchased as an off the-shelf package. It is important to know whether the software includes source code, documentation, and other components, in addition to the executables. As in the operating system, a set of parameters or characteristics may be associated with the application software whose values affect the number, format and size of the records that are handled.
Examples: Microsoft Word, Lotus 1-2-3, Netscape Communicator, Database Management (DBMS) software, Computer Aided Design (CAD) software.

3.5.C. Data

Definition: numbers, characters, images, or other methods of recording which represent values that can be stored, processed, and transmitted by electronic systems.

3.5.C.i. File Structure

Definition: The relationship and organization of files within a system.
Note: File structure includes the directory structure of a file system. The physical structure and organization of files in a file system may also constitute an aspect of the file structure and data format. This can include the mapping of files onto disk blocks of each disk plate, and among a set of disks.

3.5.C.ii. Data Format/File Format
Definition: The organization of data within files. These are organizations that are usually designed to facilitate the storage, retrieval, processing, presentation and/or transmission of the data by software.
Note: Data format is concerned with the representation of each piece of data and the relationship between pieces of data. Within a file, it includes standardized data formats such as ASCII text, as well as proprietary file formats such as Microsoft's WORD97 and Adobe's PDF file formats. It also includes structures such as the tabular format of data files in a database management system, and the format (using tags) of data files used by mark-up languages.
Examples: Portable Document Format (PDF), Rich Text Format (RTF), ASCII text

3.5.D. System Models
Definition: System models are abstractions that represent the entities, activities and/or concepts in the system as well as their attributes, characteristics, and the functional relationship between them.
Note: "Functional relationship" refers to a relationship involving two or more entities/objects that is important to represent explicitly in order for the application to function correctly. System models contrast with data format and file structure in that they represent behavioural, procedural, and/or functional aspects of a system or software application. They may, however, affect directly or indirectly the way files are conceived in an application and the way data are organized within the files in an application. A model is usually represented graphically (e.g., as in entity relationship, object-hierarchy, data-flow, control-flow, and state-transition diagrams). Modelling languages (e.g., IDEF, UML) and their associated software tools serve as aides in creating model specifications. The model usually becomes part of an application's requirements, specifications, and/or design document. Parts of the model can also be represented and used in an application's data dictionary.
Examples: entity-relationship models, object domain diagrams, IDEF (0) process models, UML use-case models, data-flow diagrams.

3.5.E. System Administration
Definition: System administration is a set of procedures that ensure correct, secure, reliable, and persistent operation of the system.
Examples: Providing access privileges, ensuring security, availability, reliability, and integrity of the system over time, configuring the system, backing up files, system maintenance and upgrading hardware, software, and storage systems.

SOURCE: Quoted from INTERPARES (2000)

Therefore, with the template created by InterPARES (2001), broken down into tables, indicates the line that separates Diplomatics (documentary form and medium) and Archival Science (annotations and context). In this sense, the concepts outlined in the template of analysis complement traditional Archival elements, such as, archival bond, which is the organic relationship of the records with other records, and the provenance and original order principles, which, as already explained earlier, is to avoid the records being incorrectly mixed with other records.

The purpose of the InterPARES research was to show that the concepts of two different knowledge fields could interact with each other for the benefit of digital records. Herein, this science shall be called Archival Diplomatics.

The elements listed and described in the template analysis above can be determined as characteristics of metadata for the management and preservation of born-digital records. Hence, it would be reductionist to consider it just an instrumentalist or a technician tool. Therefore, Diplomatics can be interpreted in two ways: First, as a science that addresses documents to ascertain their authenticity, and alongside Archival Science, we are able to analyze the records as societal products through the acts and facts established by respected institutions. Second, the application of diplomatics characteristics to the record itself assures its trustworthiness as a concept, which surpasses the concept of authenticity to be preserved over time.

As explained by Caroline Williams (2007, p.4), the Diplomatics of the 20th and 21st century has been widely utilized by academics in the field to expand the threshold of the document and to turn it into a process of "*recordness"*:

> […] However, developments in record-keeping by the end of the 20th century meant that, to continue to be useful, diplomatic had to become more broadly applied and its traditional definition reconsidered. The purpose of diplomatic analysis was required to be much wider than Mabillon's because of the need to:
>
> - include informal documents as well as formal;
> - encompass aggregations of documents as well as individual ones;
> - consider the organisations and systems producing documents as well as the documents themselves;
> - enable prospective as well as retrospective analysis;
> - encompass electronic as well as paper-based systems.

William's aforementioned quotation can be justified by stating that Diplomatics addressed the documents in a raw and individual way. Meanwhile, Archival Science addressed the records name as a process that binds one document to another to create a *corpus* when the elements remained together and make up part of all a whole process. The authenticity concept changed the vision with the Archival processes in respect to Diplomatics, which is one of the reasons of the strength of authenticity in the archival sense is beyond the support.

Another Diplomatics element to be considered is the documentary classification in respect to the context where the record is created. In this sense, according to Duranti (1989), records can be dispositive, probatory, supporting and narrative records. This meaning of Diplomatics has not changed in Archival contexts. The dispositive records are defined as those related with an order or disposition accomplished and constituting "[…] a written evidence of a juridical fact […]" (INTERPARES, 2008, p.5).

The probatory records are those that prove some juridical act "[…] of an action that came into existence and was complete before being manifested in writing […] (INTERPARES, 2008, p.5). Supporting records are those records used to support the bureaucratic activities that do not result in a juridical act. Narrative records are also usually juridical irrelevant records (INTERPARES, 2008, p.5).

The fourth sorts of records still remain in the digital era. In this case, only the alteration of the support occurred because most change took place between the Middle Ages and modern bureaucratic processes. Duranti explains (1990) that the moment of the action and the moment of the documentation were integrated into one procedure:

> Gérard and Christiane Naud have pointed to the most obvious fact which differentiates the genesis of medieval documents from that of modern documents. Each medieval document contained the whole transaction generating it, and its creation, as the apex of the transaction, was either sequential to it (probative documents), or parallel (dispositive documents), that is, perfectly distinguishable from the transaction as an expression of will. On the contrary, each modern document incorporates only one phase of the transaction, or even less, and its creation, as a means of carrying out the transaction, is integrated in each of the phases through which the transaction develops, and is not distinguishable from the action of the will. This fact invalidates the definition of the moment of the action and the moment of documentation as two separate sets of routines, or two distinct procedures. They are still two *conceptually distinct moments,* nevertheless, even if they are considered integral parts of one procedure. This can be demonstrated by analysing the ideal structure of the integrated procedure which generates documents.

The integrated procedure highlighted by Duranti is expanded in her Diplomatics' article (1990), where she explains that two or more phases existed in administrative contexts in the creation of records: "Introductory phase or

initiative; Preliminary phase or *inquiry;* Consultative phase or *consultation*: Deliberative phase or *deliberation*; Controlling phase or *deliberation control*; and Executive phase or *execution* (DURANTI, 1990, p. 14-15).

Diplomatics concepts when applied to Archival Science modify the initial structure to adapt in a “better” way. The isolated concept of a document gains importance as a record and the relationship with other records. The concept of authenticity differs between Diplomatics and Archival Science. It is no longer applied to the individual document but to the records of the same provenance. The link or archival bond among the records establishes a concept of authenticity stronger than Diplomatics. In countries such as Canada, the admissibility of the records is easy to determine due to them being within a correctly administrative system.

For this reason, importance of each of the steps to organize the records charges no matter their support. As is explained by Terry Cook (2013, p.98-99):

> […] Archivists are not archivists because they do the same things in different places (appraise, acquire, process, describe, preserve, make available), or because they or others find what they do to be ‘‘valuable,’’ but because what they do has its own societal significance and impact, its own community of meaning, its own transcendence beyond the mundane to the ideal, the individual to the communal.

Cook’s quotation explains how Archival Diplomatics addressed the records as a whole without forget the social character. The archival processes, with maybe some slight changes, has been adapted in many cultures as demonstrated in several conferences and other scientific experiences. The studies of Theodore Roosevelt Schellenberg in the United States and Hilary Jenkinson in England, developed in the 20th century, continue to have relevance today, especially in digital contexts.

Redeeming Diplomatics in the 20th and 21st century is justified because this approach is again necessary for the digital record individually, but without avoiding its archival bond and provenance. This can be perceived by analyzing the abstraction of the records as shown in the aforementioned tables 4, 5, and 6.

To conclude this chapter, Diplomatics is an important science that supports the Archival thought and practice and due to the complexities of the composition of born-digital records as well as the need of other knowledge

areas such as Forensics. The same way that Diplomatics, Forensics, specifically digital Forensics, has a long history, and the process of adapting its mechanisms to archival practices is beginning to show some interesting outcomes.

4 FORENSICS

> Unlike the document written on paper, we can say that documents on computers work more or less as a metaphor for our memory. When we remember, we do not recover the moments as they happened. We represent those memories and modify them when we bring them permanently to our present. When we write on the computer, it represents our thoughts in format of bits, artificially, but exactly[71] (Written by the author).

While Jean Mabillon can clearly be identified as the creator of Diplomatics, it is a little difficult to identify a figure like Mabillon for Forensics. Perhaps the most recognized author in Forensics during the 20th century was the scientist Edmond Locard (1877-1966), who established the famous Locard's exchange principle. This principle states that "when a person or object comes in contact with another person or object, a cross-transfer of materials occurs" (ÅRNES, 2018, p.2). The principle allowed Forensics to become an area of scientific knowledge.

Although both Diplomatics and Forensics have their own historical context of foundation and evolution, they also have some characteristics in common: first, the positivist environment (PALMER, 2001), wherein the concept of scientificity is paramount to prove the truth; second, their close relationship with the Legal concepts. Even though Diplomatics was born in legal environments, the junction with Archival Science changed its core to fit to records activities.

In addition, some authors called Diplomatics between the 17th-19th centuries "*Forensics-Diplomatics",* due to the relationship with the legal elements (ROMERO-TALLAFIGO, 1994; BELLOTTO, 2008; TOGNOLI, 2014). Manuel Romero-Tallafigo (1994, p.17, our translation) notes that the record dictates rights and obligations: "[…] Besides being a historic and administrative

[71] *Diferente del documento en papel, podríamos decir que los documentos generados en computadores funcionan más o menos como una metáfora de nuestra memoria. Cuando recordamos no recuperamos los momentos como realmente acontecieron. Representamos esos recuerdos y los modificamos cuando los traemos a nuestro presente. Cuando escribimos en el computador, este representa nuestros pensamientos en formato de bits. De forma artificial, pero exacta* (Escrito pelo autor).

science, it is a science that works for the legal and forensics world that dictates the Law (*iuris dictio*)"[72].

In this regard, the core of Forensics is its strong bond with the legal area and its main function is to provide support to legal issues (GOLDBERG, 1994, ARONSON, 2007; ADAM, 2015). Thus, "forensic science in its broadest definition is the application of science to law" (ÅRNES, 2018, p.1). The versatility of this science is perceived when it has been historically applied to other disciplines, such as Biology, Medicine, Physics, Geology, Computer Science, Electric Engineering (ÅRNES, 2018, p.2). Currently, its theoretical and practical corpus is being applied in other sciences, in this case to support Archival Diplomatics.

In the last 20 years, Forensics has managed to adapt to the digital context. Some authors (BOGEN; DAMPIER, 2004; ZATYKO, 2007; DURANTI; ENDICOTT-POPOVSKY, 2010; TOGNOLI, 2014; ROGERS, 2015; ÅRNES, 2018) have highlighted the standard definition of digital Forensics, addressed by the digital Forensic Research Workshop - DFRW (PALMER, 2001, p.15):

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

However, Forensics needs to overcome some difficulties before it can be applied to archival practices. One of them is the interaction of professionals with each other, when it reaches the purposes in a certain investigation scenario. This difficulty could be analyzed with the dynamic participation of each individual involved. The point described above is outlined by Christopher Lawless (2016, p.5), when he explains that:

> Given the number of people and practices involved in the transition from crime scene to court, it is difficult for any individual actor (be they forensic practitioners, police, lawyers, suspects, etc.) to be well positioned to observe all that goes on. Indeed, these participants may not be aware of the totality of practices and interactions needed to ensure the continuity of the process through which forensic evidence is translated across a range of spaces. Lynch et al. (2008) have observed

[72] […] *Además de ciencia histórica y administrativa, es ciencia que sirve al mundo judicial y forense que dicta el derecho (iuris dictio)* (ROMERO-TALLAFIGO, 1994, p.17)

> that bureaucratic practices may play an important role in maintaining the integrity and objectivity of forensic evidence as it comes into being. They describe ‘administrative objectivity’ as involving a combination of technical, legal and Bureaucratic elements. Lynch et al. assert that, rather than being a purely scientific or legal achievement, the credibility of forensic evidence also relies on administrative procedures, including logbooks, checklists, forms and archives, which together constitute a ‘paper trail’, or chain of custody, to transform crime scene traces into legal evidence. The observations of Lynch et al. indicate how the administration of modern forensic science embodies complex assemblages of diverse forces, practices and devices. Such assemblages appear to play a key role in stabilizing the relationship between science and the state.

The belief that Forensics is applied just by a certain kind of technical professional working in a laboratory is constantly changing. The previous quote emphasizes Forensics in other domains, mainly in administrative process, in which born-digital records need to maintain their authenticity and reliability all the time.

Thus, this chapter intends to explore the possibilities brought by digital Forensics to Archival Diplomatics. For this reason, discussion about the underpinnings and development of Forensics are necessary to understand its contribution to the digital process, especially when it comes to the creation, maintenance, preservation, and use. Likewise, the core concepts of this science and its narrow relationship with the Law will be explored. The end of this chapter will address how the contribution of the Forensics to Archival Diplomatics activities is established, and how records professionals can exploit this knowledge to improve their practices.

4.1 HISTORY OF FORENSICS

The word “forensics” is usually related to medicine, laboratories, crimes, death, and so on. Furthermore, it is often related to books, movies, and TV shows like Sherlock Holmes (2010) and Crime Scene Investigation – CSI (2000). The reality is that Forensics has been applied since the Ancient World (SILVA, 2010), albeit with elements that were quite hard to define it as science at that time.

The evolution of practices appeared in antiquity and have developed throughout the course of the history. The research of Alexandre Silva (2010) maps the initial purposes, the people involved in the processes, and the instruments used to address the cases. The author starts with the explanation of two key concepts: expert and forensics. The term “expert” comes from the Latin “*perita”*, meaning expertise, experimental science, perfect knowledge, capacity, intelligence. The term “forensics” comes from the Latin “*Forensis”*, belonging to the legal forum, being performed by a *peritus,* an adjective related with expert, learned, wise, experienced, intelligent (SILVA, 2010, p.13, our translation). The meaning of the word “forensics” is also described by Collier and Spaul (1992, p.204), thus:

> The word forensic is defined in the Oxford English Dictionary as an adjective meaning "... used in, or connected with a court of law." and the term forensic science as "a science that deals with the relation and application of scientific facts to legal problems." Traditionally forensic science has centred on the physical and applied sciences such as medicine, engineering, chemistry, ballistics, etc. However, more recently social sciences, such as psychology and accounting, have been added to the forensic science armoury. These social science extensions of forensic science have a dominant requirement for interpretive and judgemental skills, rather than the detection of physical evidence.

Following the study of Alexandre Silva, the author explores the seemingly first case of “modern” Forensics, in the medical area: an analysis of Abbot papyrus dated from 130 After Christ, where a doctor called C. Menicius Valerianus, a borough of Karanis, carried out a report related with wounds sustained by a man called Mystharion. The report contains feature of a current forensic analysis: “[…] the request from an authority, the commitment of the participants, actions of the professional, the presence of witnesses, a detailed description of the wound, as well as the type of object that caused it, and the writing of the document by the scrivener” (SILVA, 2010, p.15, our translation)[73].

Nevertheless, some steps and procedures had not yet been defined and/or clarified. The judge itself performed the gathering of evidence and analysis because, at that time, the function of what today we know as forensics

[73] [...] *requisição da autoridade, compromisso dos participantes, atuação do profissional, presença de testemunhas, descrição minuciosa da lesão, assim como o tipo de objeto que a inferiu e redação do documento pelo escrivão* (SILVA, 2010, p.15).

expert did not exist. Years later, the role of judge and specialist was mixed because the function of each was not yet known. The Legal Power was a priestly assignment, and the Supreme Court was responsible for prosecuting serious crimes. The oral debate, likewise, did not exist, but all the acts were written and published (SILVA, 2010).

Another relevant historic period is when Forensics begins to be applied in the western world, in the Roman Civil process, and three significant points are identified: the actions of the law (*legis actiones*), the forms (*per formulas*), and the extraordinary *(cognitio extraordinaria).* The highlights of this period were the lack of knowledge of some expert examinations in Forensics, as is currently known, and the use of surveyors as experts, in cases about the delimitation of lands. In the Middle Age, when the only truth came from God, the technical and/or scientific discussions were left out. However, since the 11th century, some changes revived scientific knowledge. Thus, the Roman and the Canonical Law was commonly accepted over the systematization of legal evidence (SILVA, 2010).

In the 15th century, the transformation of society and rise of an apparent era of progress began. This change gradually started three centuries before. The main facts to establish the modern thinking was the inclusion of Hindu-Arabic numerals, which were easier to use than the Roman numbers, and the sea navigation expeditions that allow development of a series of technologies to discover and trade with the new territories. In the end, engineering, which had been abandoned in the Middle Age, became important (SILVA, 2010).

The 16th and 17th century are characterized by the technological revolution and the use of nature as the source of scientific and technical knowledge. Two ways of thinking permeated the mentioned period: the investigation from experience of Francis Bacon (1561-1626) and the thinking of René Descartes (1596-1650), who stated that the knowledge was founded in the abstract rational thinking of mathematics (SILVA, 2010).

With the above picture, it is possible to examine how the theories and hypotheses affected Forensics. Apart from this analysis, elements and/or procedures suffered modifications. In 1572, the analysis of evidence started to be done not just by the witnesses but also by forensics experts. With this

reform, a corporation of official experts was constituted to work with judges, as auxiliaries in technical issues (SILVA, 2010).

In the 18th and 19th centuries, the scientific revolution prioritized rationality and put aside the religious character. In this context, the function of the judge and the forensics experts was becoming clearer and more consolidated. With the publication of the treatise, *"Dei Delitti e Delle Pene*" (1764), Cesare Beccaria (1738-1794) expressed the idea that "[…] the judge's objectivity in a social environment was tainted with bias" (SILVA, 2010, p.47, our translation)[74].

In the 19th century, the Industrial Revolution process also made substantial changes. Countries like France and the United States modified and implanted new models of democratic states, which allowed these countries to create new institutions, to begin an era of progress based in new scientific areas including several agencies of criminal investigation. "France created the "*Brigade de La Sûreté"* lead by François Eugéne Vidoq (1775-1857), who had been persecuted by the justice and escape from prison, then later founded this pioneering criminal agency" (SILVA, 2010, p.59, our translation)[75].

The importance of this agency, according to Silva, was its use for the first time of several unedited techniques, such as fingerprint, ballistic projectile, graphology analysis, and blood test. Other concepts improved in the science were the division of regular inspections, made by Forensics experts, and legal inspections, conducted by judges. The differentiation between the forensics inspection and the judicial inspection clarified the functions of the forensic expert and judge, and lead to accurate value judgment by judges (SILVA, 2010, p.59)[76].

[74] *Importante não só para a perícia nesse período foi a obra "Dos Delitos e das Penas", de Cesare Bonesana Beccaria, escrito em 1763 e publicado em 1764, onde tratava da objetividade do juiz dentro de um contexto social dominado pelo preconceito* (SILVA, 2010, p.47).

[75] *Na França, a Brigade de La Sûreté utilizava técnicas avançadas para a época na investigação de crimes. Françõis Eugéne Vidocq (1775-1857), personagem lendário, passou de condenado, procurado pela justiça por fugir da cadeia, a fundador e diretor da Sûreté* (SILVA, 2010, p.59).

[76] MITTERMAYER *(1909), trouxe em sua obra, intitulada Tratado da Prova Criminal, importante contribuição à perícia, tratando de questões como a diferenciação entre a "vistoria", ato realizado pelo perito, e a "inspeção judicial", ato realizado pelo juiz, que pessoalmente inspeciona corpo do delito* (SILVA, 2010, p.59).

The above information outlined by Silva was taken from the scientific study of the German jurist, Carl Joseph Anton Mittermaier (1787-1867) in his research, “The German criminal procedure in advanced training through court use and particular codes of law: and in exact comparison with the English and French criminal trials; in two divisions” (1832)[77]. Mittermaier in this sense, was considered the most influential critic of the death penalty (EVANS, 1996, p.255). Along with Mittermaier, scientific studies appeared in the Austrian criminal jurist, and criminologist, Hans Gustav Adolf Groß (1847-1915), who was the first crime investigator to use the word “criminalistics” (ANDREW, 2007).

Groß reinforced in his “*Handbook for Examining Magistrates as a Criminalistics System*” (1908)[78] the necessity of a close relationship between the forensic expert and the judge for better determination in cases. In addition, Groß dealt with forensics expert techniques, as for example, the conservation of cadavers and parts of cadavers as well as the use of Forensics Psychology to learn about mental issues and their symptomology. Moreover, “he worked various types of expertise, such as graphology, odontology, microscopy on stains and trace elements, hairs, and forgeries techniques […]” (SILVA, 2010, p.66, our translation)[79].

With this outlook of scientific knowledge, the 20th century achieved a series of significant technological advances. One of these remarkable advances in Forensics is the prolific scientific study made by the French criminologist Edmond Locard (1877–1966). This author developed the Principle of Exchange in his treatise “*L'enquête criminelle et les méthodes scientifiques”,* published in 1920. This principle used concepts and elements from Mittermaier and Groß, but Locard systematized them and presented them with better intelligence and detail. The two main principles of Forensics, applied first by Locard and then by Paul Kirk (1902–1970), were first the exchange principle, which states that with contact between two items, there will be an exchange. Individualization principle

[77] Original name of the study: *“Das deutsche Strafverfahren in der Fortbildung durch Gerichts-Gebrauch und Partikular-Gesetzbücher: und in genauer Vergleichung mit dem englischen und französischen Straf-Prozesse; in zwei Abtheilungen”* (1832).

[78] Original name of the study: *Handbuch für Untersuchungsrichter als System der Kriminalistik* (1908).

[79] *Tratou de vários tipos de perícias, como grafotécnicas, odontológicas, microscópicas em manchas e vestígios, pelos, falsificações* [...] (SILVA, 2010, p.66).

advanced by Kirk, “[…] states that an action can be tied to a unique individual by identifying items that are discovered both at the scene and the perpetrator’s environment, such as threads, hair and fibers” (ANDREWS, 2007, p.19).

All this knowledge created new spaces for investigations, as for instance, Forensics being applied in documents, in a similar manner as Diplomatics to ascertain the authenticity. This is described by Matthew G. Kirschenbaum (2008, p.47–48):

> The most relevant forensic science precedent for computer forensics is the field of questioned document examination, which dates back to the end of the nineteenth century. It concerns itself with the physical evidence related to written and printed documents, especially handwriting attribution and the identification of forgeries. Questioned document examination also bears some resemblance to the academic pursuits of analytical and descriptive bibliography (which emerged in an organized fashion during roughly the same years), but the forensics enterprise subjects the myriad implements of writing and inscription to a degree of scrutiny that might give even a hardened bibliographic pause. (Handwriting identification as it is practice by a forensic expert is not to be confused with graphology, the more dubious practice of deriving personality traits from the appearance of an individual's handwriting; this approach was explicitly rejected by the earliest text on document examination, including Persifor Frazer's *Bibliotics, or the Study of Documents* {1894, itself now largely discredited} and Willian Hagan's *Disputed Handwriting* {also 1894}.[80]). The questioned document examiner is almost always concerned with a document in its physical entirety. To quote Ordway Hilton, a contemporary authority:
>
> Not only must these examiners be able to identify handwriting, typewriting, and printed matter, but they must be able to distinguish forgery from genuineness, to analyze inks, papers, and other substances that are combined into documents, to reveal additions and substations in a document, and to restore or decipher erased or obliterated writing. When records produced by complex modern business machines are suspected of having been manipulated document examiners may be among the first to be consulted (p. 47-48).

The above Kirschenbaum quote includes some elements that had been studied by Diplomatics since the 17th century. Most of them were about the extrinsic and intrinsic elements. The scope of Forensics is broader than

[80] (Explanatory note by the author): Even Sherlock Holmes, author of a "little monograph" on the dating of documents, was not above the temptation of graphology: '"look at his long letters,' he said. 'They hardly rise above the common herd. That d might be an a, and that l an e. Men of character always differentiate their long letters, however illegibly they may write. There is vacillation in his k's and self-esteem in his capitals'" (Sir Arthur Conan Doyle, The Sign of Four).

Diplomatics, but in some aspects both sciences share some similarities when it comes to analyze records.

The technological impulse of the 20th century was accelerated during the two World Wars (1914–1918 and 1939–1945) by the scientific community, as mechanism for the powerful nations to show their weapons capacity. Albeit, after World War II, the technology initially created for the war was transferred to benefit society in the middle of the 20th century.

The internet was originally created by researchers from the United States during the Cold War, as a military program to create a bombing defense system, linking several computers and allowing the exchange and sharing of data between them. In 1957, the Advanced Research Projects Agency – ARPA was created to coordinate military issues. The ARPA project established an interaction among military and university researchers to create a communication network in the informatics systems to the benefit of the military (SILVA, 2010).

In 1968, the United States Secretary of Defense ordered a project to develop communication protocol for the codes used in informatics systems communication in case of a nuclear war. In 1969, the same organization created the Advanced Research Projects Agency Network – ARPANET, to guarantee the normal operation of the systems. In the 1980s, the project was shared with universities and divided into in two sections: Military Operations Network – MILNET, restricted to the U.S. Armed Forces, and the ARPANET, for academic purposes.

In the late 1980s, the same organizations from the United States formalized and standardized information protocols called “Transmission Control Protocol/InterNet Protocol” – TCP/IP. The Transmission Control Protocol function – TCP, was used to transmit data, and if this data was not transferred in a complete form, they had to be rebroadcasted. The InterNet Protocol – IP function established a communication protocol between different local computer networks (SILVA, 2010). This was interesting because it became the underpinning to the democratized internet.

As a result, the internet evolution was the turning point of the epoch and is presently considered one of the most considerable technological advancements around the world. This phenomenon, popularized and

democratized by Tim Berners-Lee, resulted in the creation of the World Wide Web in 1989, which allowed anyone to connect to the internet.

The internet phenomenon has created the mass distribution of computers throughout the entire world. Along with this, came the need for law enforcement to analyzed new crimes related with digital environments. The main physical object seized by the investigators has been the hard drive which contains the information stored on the computer.

Kirschenbaum (2008) explores how the hard drive became the key to the functioning of computers and how computer storage developed from the punched cards into these complex devices. In his second chapter, “A Book That Can Be Read Without Be Opened and a Day of Solid Achievement”, Kirschenbaum performs an exhaustive analysis of the nature and framework of the hard drive. The author explains the functioning of the first computer disk storage system called RAMAC (Random Access Method of Accounting and Control), developed by IBM:

> When RAMAC was first announced in 1956, Thomas J. Watson, Jr., president of IBM, opined that it was “the greatest product day in the history of IBM”. The remark was arguably not an overstatement. The RAMAC, which stood for Random Access Memory and Control, was, as its name implies, a random access storage device. This was fundamentally different from the punched paper or magnetic tape that then dominated the storage industry. As Paul E. Ceruzzi notes, “In time, the interactive style of computing made possible by random access disk memory would force IBM, as well as the rest of the computer industry, to redefine itself”. This is a powerful insight, and not often grasped by students of new media, who tend to ascribe “interactivity” to the advent of the screen display, the graphical user interface (GUI), and the mouse in a genealogy that runs from the SAGE air defense network through Ivan Sutherland’s Sketchpad to Douglas Engelbart’s 1968 “mother of all demos”. Yet the advent of random access disk storage goes to the heart of the contemporary critical assumptions about new media. For Lev Manovich, for example, new media is characterized by a “database paradigm”, manifested in the modular nature of a digital production’s constituent objects and the lack of an essential narrative or sequential structure for how those objects are accessed and manipulated: “In general, creating a work in new media can be understood as the construction of interface to a database”. While Manovich is reluctant to associate database and narrative with specific storage technologies in any deterministic sense – the codex book, he notes, is the random access devices par excellence, yet it is a haven for some of our most powerful narrative forms (233) – computers

> could not have expanded from their role as wartime calculators to new media databases without the introduction of a nonvolatile, large-volume, inexpensive technology affording operators near-instantaneous and simultaneous access to all stored records. Magnetic disk media – more specifically the hard disk drive – was to become that technology and, as much as bitmapped-GUIs and the mouse, usher in a new era of interactive, real-time computing (p.77-78).

This quote by Kirschenbaum presents the information about the process of a method transformation from the storage of one device to another. With that technology, the other interactive elements started to appear and the computing world started to change in the late 20th century. The digital Forensics section will address new research in the 21st century and the evolution of Forensics in the last 20 years.

4.2 DIGITAL FORENSICS AND THE LAW

The historical context at the beginning of this chapter illustrated the close relationship between Forensics and the Law. The previous section described how Forensics and Law have walk together through time and how both sciences have been connected throughout their history. It will explore how Diplomatics had its underpinning with Forensics and legal character, and how these elements slowly vanished through time until almost disappearing in the late 19th century.

This section discusses the influence of the legal subject for two purposes: on the one hand, the mentioned relationship between digital Forensics and Law; on the other hand, the likelihood of identifying born-digital records as evidence for determined purposes, and the support of DAFD – to guarantee trustworthiness and long-term preservation options.

In this study, the aim of DAFD is to guarantee the accuracy, reliability, and authenticity (trustworthiness) of born-digital records and their systems in the lifecycle and to develop mechanisms and tools to assure the integrity all the time and as evidence admissible in legal situations. Furthermore, digital Forensics can use a series of mechanisms adopted by the Law to support born-digital records. These elements make up the core of digital Forensics and their use in Archival Diplomatics.

The relevant concepts performed in Law and used in digital Forensics activities are chain of custody, a concept addressed in the born-digital records and digital Forensics chapters, as well as audit trails used in business processes, non-repudiation, and admissibility. These concepts are essential attributes of born-digital records and are mandatory to enable better born-digital records in any scenario where are required. At the same time, the digital context requires other support besides that traditional used in Archival Diplomatics, and this is the main value and justification of digital Forensics as a science that depends on the Law.

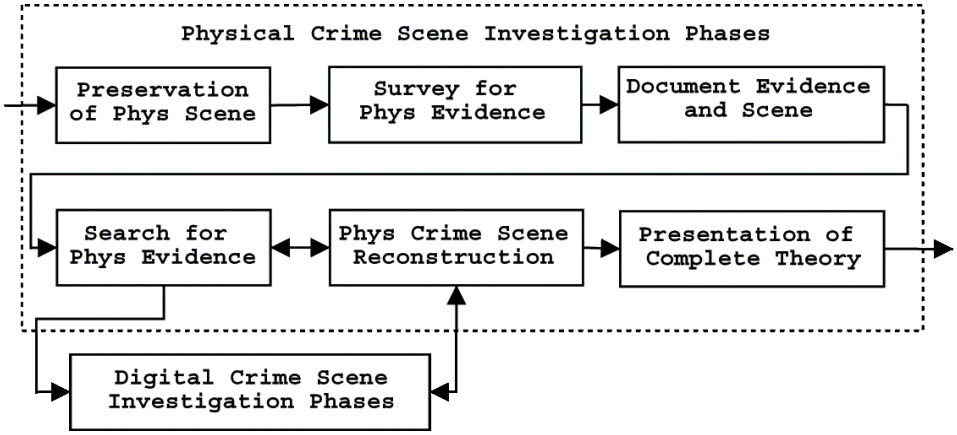
Chain of custody arises as a foremost principle with the objective to protect the integrity of data in diverse systems. The technological tools developed in digital Forensics allow that the chain of custody is applied in an uninterrupted manner to avoid data modification. Thus, the chain of custody should be applied mainly in three objectives:

> […] This element is essential to maintaining the integrity of the bitstreams, and although some challenges exist to ensure such integrity, its use is increasingly common. Its issues are related to 1) The volatility of digital evidence in resources such as register, memory, table, processor, temporary filesystem, disk, remote logging and data monitoring, physical configuration, and network topology, as well as archived data (Prayudi & Azhari, 2015, p.3); 2) with medium failure/bit rot; and 3) the obsolescence of both software and hardware […] (MONTOYA-MOGOLLÓN; TROITIÑO, 2020, p.9).

Archivists have developed apart from chain of custody, chain of preservation to preserve the bitstreams managed in the systems and archival repositories. Thus, chain of custody and chain of preservation should work as unbroken custody in the records-making and records-keeping process.

Traditionally, chain of custody in the Law was considered as an interesting element in the physical world as a method to follow the proper pathway of an investigation. For Daniel Flores (2017, p.370), “Chain of custody (CoC) is a concept shared among areas like law and archival science, related to those that store and apply management and security principles to a certain asset or heritage collection stored.” While this is true, CoC works differently when used in the Law with the intent of solving legal cases. To understand a little bit about the chain of custody element in the traditional legal system, figure 4 presents the steps of a suitable investigation.

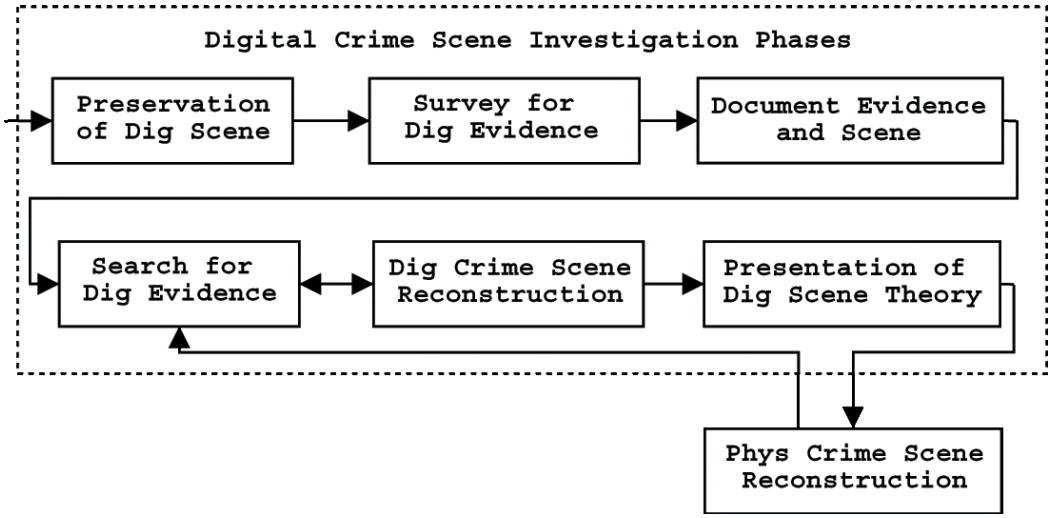
Figure 4 – THE SIX PHASES IN THE PHYSICAL CRIME SCENE INVESTIGATION AND THE INTERACTION WITH THE DIGITAL CRIME SCENE INVESTIGATION.



SOURCE: Carrier & Spafford (2003, p.8)

Figure 4 provides an example of chain of custody in a physical crime scene. The relevant point in figure 4 is to understand how these steps are followed at the time to seize any kind of information intended to protect its integrity. Figure 4 also presents the relationship between admissible physical and digital evidence, with the awareness of the difference in physical and digital context, which are analyzed in a separate way. In this regard, Carrier and Spafford (2003, p.10) state that the digital chain of custody begins when the physical process is finished. Hence, the digital chain of custody is described in figure 5:

Figure 5 –THE SIX PHASES IN THE DIGITAL CRIME SCENE INVESTIGATION. THE RESULTS ARE FED BACK TO THE PHYSICAL CRIME SCENE INVESTIGATION.



SOURCE: Carrier & Spafford (2003, p.10)

Along with the chain of custody, the audit trail is another mechanism to verify the authenticity of born-digital records. Although this last element is not related directly to Law, its application impacts the legal system. The term “audit” normally is related with a person or system with the competence to review and examine records and activities to test for compliance with established policies and standards (PEARCE-MOSES, 2005, p.40). The term “trail” works as a function to map out activities, in this case, activities of born-digital records.

Consequently, the audit trail is used in business activities as a manner to avoid the information from being compromised and as a mechanism necessary to present in the context when required. Therefore, the definition of audit trail is: “[...] an information in records that track a transaction form beginning to end, making it possible to review whether it was done according to relevant policies and standards” (PEARCE-MOSES, 2005, p.40). To reach the admissibility, evidence must have accuracy, reliability and authenticity of records, and an audit trail (business), along with chain of custody (legal) to support these issues,

> […] at a minimum, with the next statements:
> - the results of the who used the system,
> - when they used it or instigated a transaction,
> - what they did while using the system, and,
> - transaction (COHASSET ASSOCIATES, 2001).

The elements listed above allows tracing of both digital records and the context where they were created. Thus, the advantages of an audit trail are relevant because it includes “[…] the time of transaction, the parties involved, and actions taken” (PEARCE-MOSES, 2005, p.40). However, it was necessary to complement the audit trails with the chain of custody due to the easiness to modify sensible information.

The implementation of chain of custody and audit trail, as well as guarantee of the accuracy, reliability, and authenticity of born-digital records, enables the examination of the technological system where they are stored. This allows the non-repudiation of information in both technical and legal scenarios. Non-repudiation deals with the acceptance of information after to make a digital transaction in reliable systems.

In legal contexts, the non-repudiation is defined as sufficient evidence to persuade the legal authority to respect “the source, submission, delivery, and

integrity […]" (SANTIAGO, 2018, our translation[81]). In technical context, the non-repudiation allows both verification of the authorship of the record and establishment of content with "logic immutability". Any change made in the record invalidates the digital signature (SANTIAGO, 2018[82]).

Even though digital signatures are accepted as an admissible method in a country like Brazil, this technology does not assure the authenticity of born-digital records, only its authentication. Authentication in this sense is "[…] a declaration of authenticity made by a competent officer, and consists of a statement or an element, such as a seal, a stamp, or a symbol, added to the record after its completion […]" (DURANTI, 2009, p.54). As a result, authenticity does not mean the same thing as authentication.

In addition, the admissibility of born-digital records depends on the type of legal system (Common Law or Civil Law). The international experience at the University of British Columbia – UBC, illustrated relevant specificities of the Common Law[83] as well as how the Common Law system act in relation with records, specifically, born-digital records.

A deeper discussion of the Canadian Rules of Admissibility is relevant because that legal reality, which requires support from the scientific community, could improve the contemporary Law system. Even though Civil Law has its own delimited functions and norms, this section is justified to learn how other systems deal with the diverse difficulties in digital context. Therefore, it is relevant to note how the Common Law provides elements to accept digital records in trials.

The traditional legal practices in Common Law recognize norms related with the admissibility of records, specifically, the Hearsay Rule and the Best

[81] *O não repúdio deve ser visto sob a ótica legal e técnica. Sob uma perspectiva legal, o não repúdio é definido como suficiente evidência para persuadir a autoridade legal (juiz, jurado ou árbitro) a respeito de sua origem, submissão, entrega e integridade, apesar da tentativa de negação pelo suposto responsável pelo envio.* In: https://solutiresponde.com.br/voce-sabe-o-que-significa-nao-repudio-descubra-neste-post/

[82] *Desse modo, a técnica permite não apenas verificar a autoria do documento, como também estabelecer uma forma de "imutabilidade lógica" de seu conteúdo, pois qualquer alteração do documento, por menor que seja, como a inserção de mais um espaço entre duas palavras, por exemplo, invalida a assinatura.* In: https://solutiresponde.com.br/voce-sabe-o-que-significa-nao-repudio-descubra-neste-post/

[83] Only the Canadian Common Law is taken as reference. An interesting difference between the United States and Canada for instance is the application of Capital Punishment. This kind of state-sanctioned is practiced in some states of United States and not in Canada.

Evidence Rule, which recognize the vantages of paper-based records for admissibility in trials. With born-digital records, the process is different. To be admissible in legal contexts a third-party expert, such as a digital forensics expert and/or an archivist, must prove the trustworthiness of these records. This is a hard assignment because, although the rules are constantly improving, the Law normally moves in slow pace, unlike the rapid pace of digital technology.

The Hearsay Rule is considered inadmissible in most courts because it supposes witness's lack of objectivity to state a determined case, and recognizes some influential bias in its statement. However, this rule has some exceptions, and records, as products of business transactions, are one of them. This is explained as follows:

> Digital forensic experts have been concerned with the different types of records that can be found in digital systems, although only in relation to their ability to be admissible evidence. In fact, the courts have generally admitted digital records under the business records exception to the hearsay rule. This rule, which is shared by common law countries, considers all written evidence hearsay because it contains statements made by humans who cannot be cross-examined on the stated matter. However, written documents which 1) are produced in the usual and ordinary course of business, 2) at or near the time of the facts or acts of which they are offered as evidence, 3) by someone who is under a duty to create them for the purposes of the business and is familiar with the procedure for doing so, are considered "business records" and admissible under an exception to the hearsay rule. The term "business" is used in a general sense and includes, in addition to business proper, the work conducted by any institution, association, profession, occupation, and calling of every kind, whether or not carried out for profit. The identification of what constitutes a business record according to the criteria listed above has never been problematic with traditional records, but, with computer records, experts are beginning to make distinctions (DURANTI, 2009, p.49–50)

Following the point written above, physical records normally are accepted in courts. In the digital realm, support is necessary of forensics and/or archivist to act as a trusted third part. This professional can guarantee the trustworthiness of records, along with the system where they are management. To consider the exception of the Hearsay Rule, the records must be recognized with the principled approach, the business records rule, and the statuary records rule to meet their admissibility (ROGERS, 2019, s.25).

Thus, the Hearsay Rule establishes two points to be admissible: first, the necessity that the evidence is crucial to the case and "[…] reasonably necessary in the sense of the direct evidence not being available […]". Second, "[…] If a statement sought to be adduced by way of hearsay evidence is made under circumstances which substantially negate the possibility that the declarant was untruthful or mistaken, the hearsay evidence may be said to be 'reliable', i.e., a circumstantial guarantee of trustworthiness is established" (ROGERS, 2019, s.29).

The Hearsay Rule should be strongly connected with the Best Evidence Rule to increase the admissibility. Best Evidence Rule arises from the possibility to maintain the "original" record. However, this is a little problematic in digital contexts, when the notion of original is hard to consider in a diplomatics sense, "[…] because when we close a digital record for the first time, we destroy the original and every time we open it, we create a copy […]" (DURANTI, 2009, p.58).

Traditionally, the Best Evidence Rule usually requires "original" records, insomuch that:

> […] (1) a copy is always liable to errors; (2) an original may contain subtle details that may be missing from the copy and that may be significant in terms of the record's meaning; and (3) it is very difficult for oral testimony to reproduce the terms of a document accurately. The "best evidence" rule is intended to increase the probability of the record's trustworthiness by decreasing opportunities for deliberate or inadvertent falsification (MACNEIL, 2000, p.49).

Thus, the Best Evidence Rule considers relevant mechanism that must be fulfill following the Canadian Evidence Act (2000), which contains these core statements:

> • 31.2 (1) The best evidence rule in respect of an electronic document is satisfied
> – (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
> – (b) if an evidentiary presumption established under section 31.4 applies[84].
> • (2) Despite subsection (1), in the absence of evidence to the contrary, an electronic document in the form of a printout

[84] This point is related with the Presumptions regarding secure electronic signatures. Available in: https://laws-lois.justice.gc.ca/eng/acts/c-5/fulltext.html

> satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout (ROGERS, 2019, s.38).

Ultimately, the Hearsay Rule (exception) and the Best Evidence Rule are, following the international scholar experience, norms that can help to improve the trustworthiness of born-digital records, not only to be admissible as evidence in trails, as also to be used as daily practices in Archival Diplomatics activities. For this reason, these sorts of legal rules can be complemented with other legal cases used to improve the difficulties of digital contexts.

Some legal disputes related with the admissibility of evidence in different contexts were identified in countries like United States and Canada. The inclusion of the scientific community is necessary to furnish some support. The following examples of historic legal cases provided interesting outcomes for the Common Law:

- USA
– *Frye v. United States* (1923)
– *Daubert v. Merrell Dow Pharmaceuticals* (1993)
– *Kumho Tire Co. v. Carmichael* (1999)
- Canada
– *R. v. Mohan* (1994) (ROGERS, 2019).

The scholar elements from the disputes described above are currently still considered, because they help to pinpoint how these experiences could provide interesting insights and solutions. First, Frye v. United States (1923)[85] was a legal case, where a defendant was convicted of second-degree murder and the court ruled that scientific theory needs to be generally accepted in the scientific community to be admissible. Second, the Daubert v. Merrell Dow Pharmaceuticals (1993)[86] case is about a prenatal ingestion by women of antinausea drug, *Bendectin*, which caused birth defects. The court of that case rejected the testimony of plaintiff's expert, because the analyses had not been published or subjected to peer-review and the analyses was not sufficiently established to be generally accepted. In the latter dispute, it was necessary to elaborate a series of standards by the Law for evidence to be admissible:

> Set out criteria for the admissibility (and thus, reliability) of expert scientific testimony:

[85] To further information see:https://law.justia.com/cases/federal/district-courts/FSupp/72/405/2238888/

[86] To further information see: https://supreme.justia.com/cases/federal/us/509/579/

> • Has the scientific theory or technique been empirically tested; or, is it falsifiable?
> • Has the theory or technique been subjected to peer-review and publication?
> • What is the known or potential error rate?
> • Do standards exist and are they maintained that control its operation?
> • Is the theory or technique generally accepted within the relevant scientific community? (ROGERS, 2019, s.53).

Third, the Kumho Tire Co. v. Carmichael (1999)[87] case is related with a car accident resulting from tire failure. Finally, the legal case in Canada is the R. v. Mohan (1994)[88], where the defendant was a pediatrician accused of sexual assault. In this process the admission of expert evidence was considered, which must satisfy four criteria: relevance, necessity in assisting the trier of fact, absence of any exclusionary rule, and properly qualified expert (ROGERS, 2019, s.56). The importance of each one of the mentioned cases is the identification of the relevance of an expert to validate the evidence and use of scientific and the proven technical data to be accepted in legal scenarios.

Brazilian Law also includes norms related with the admissibility of evidence. One example of this is the Brazilian Code of Civil Procedure, ACT No. 13,105, of March 16th, 2015[89] (As amended by Law 13.256/2016). This norm describes in articles 405 up to 480 the importance of records as evidence as well as the key role of an expert to assess the trustworthiness of records.

Ultimately, even though the legal systems in theory are different, some similarities can be identified for addressing born-digital records and their admissibility in legal contexts. The main characteristics between Common and Civil Law was identified in the term “evidence”. This concept makes sense when it is used in Common Law or science. In the Civil Law, a series of scientific articles and academic studies that used the term “*evidência”* (proof) with the same weight as “*prova”* (evidence) in legal contexts. This is interesting because currently to identify this concept, we found similar problems in Anglo-Saxon countries, including:

[87] To further information see: https://supreme.justia.com/cases/federal/us/526/137/
[88] To further information see: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1131/index.do

[89] *Lei No. 13.105, de 16 de março de 2015:* http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm

Proof vs. Evidence

Another word that is commonly misused (sadly, sometimes even by scientists, who should know better) is "proof". What "proof" means in everyday speech: In casual conversations, most people use the word "proof" when they mean that there is indisputable evidence that supports an idea.

Scientists should be wary of using the term "proof". Science does not "prove" things. Science can and does provide evidence in favor of, or against, a particular idea. In science, proofs are possible only in the highly abstract world of mathematics.

What should scientists say instead of "proof"?

Scientists should use the term "evidence" instead of the word "proof". When we test our hypotheses, we obtain evidence that supports or rejects the hypotheses. We do not "prove" our hypotheses.

While this may seem like a subtle difference, the words we use can subconsciously color our thinking. "Proof" suggests that a matter is completely settled, that we have had the last word on something.

In science, we are constantly adding to and refining our knowledge. When we have a sufficiently large body of evidence supporting an idea, we accept that idea. In the words of Stephen Jay Gould, "In science, 'fact' can only mean "confirmed to such a degree that it would be perverse to withhold provisional assent."

For example, we accept that DNA is copied into mRNA which directs the synthesis of protein, because many studies have provided evidence that this is the case, and no studies have shown this idea to be wrong. So, we have a very high degree of confidence that this idea is correct. However, we remain open to the possibility that we may (and probably will) find, at some point, that there is more to the story than we understand at this moment […] (OREGONSTATE.EDU).

In this regard, Michael W. Andrew (2007) elaborated figure 6 to differentiate the impacts and use of the concept "evidence" and "proof" in Forensics.

Figure 6 – LEVELS OF PROOF

Proof	Intuition	Probable Cause	Preponder-ance of Evi-dence	Clear and Convincing	Reasonable Doubt	Scientific Certainty
Evidence	Hunch, guess	Reasonable-ness of facts	Corroborated facts, eyewitness testimony, physical evidence, evidence interpreted by an expert			Precise facts, known accuracy

SOURCE: Michael W. Andrew (2007)

In Brazilian Civil Law, this concept has an ambiguous definition due to issues of a cognate translation of the word "*evidência"* as "evidence". In this case, the more appropriate use of the word would be "*prova"*[90].

As a consequence, both legal systems have the same issues of "proof" and "evidence" in each social reality. The term "evidence" in Portuguese reality has several meanings depending on its use[91].

Finally, the Law constitutes a key science to Diplomatics and Forensics. The concepts used in the legal system are foremost to address the digital context. Born-digital records are evidence in any context and in legal systems both Law and the scientific community must understand the benefits of the Law to fill the digital gaps.

4.3 COMPUTER OR DIGITAL FORENSICS?

Evolution began with the concept of "Computer Forensics", passing through "Cybercrimes", until the current use of "digital Forensics". In some contexts, Computer Forensics was often also related to Computer Security. Alastair Irons (2006, p.103) clarified this distinction to establish the boundaries:

[90] As explained by Braguittoni in Portuguese, the terms "*prova*" and "*evidência*" bears diferents uses and meanings in the Brazilian context: ***Evidência (ou prova?)****: Prova e evidência não são sinônimos, ao contrário do que muita gente pensa. Por conta de traduções mal feitas do inglês, é comum ouvir-se 'não há evidências de que ele seja culpado...', 'as evidências mostram que...' Típico caso de inglês mal traduzido, que gera expressões totalmente erradas. A tradução de 'evidence' não é 'evidência', mas sim prova. 'Evidência', em português, significa aquilo que é claro, inequívoco, muito visível, incontestável. Prova, muito diferentemente, é um meio de demonstrar que um fato é verdadeiro. Ou seja, se existem muitas provas de um fato, pode-se dizer que esse fato é 'evidente' (muito claro, muito visível). Mas, em português, não se pode nunca dizer que há 'evidências' de um fato. São costumeiras, em seriados policiais, e infelizmente na imprensa também, construções como 'foram encontradas evidências', 'não há evidências de que ele seja culpado' etc. Em português, essas construções são mais do que erradas, são verdadeiros absurdos. O correto é: 'foram encontradas provas', 'não há provas de que ele seja culpado' [...]* (BRAGUITTONI, 2006). In: https://migalhas.uol.com.br/coluna/gramatigalhas/31108/evidencia--ou-prova

[91] According to the *Dicionário Jurídico da Academia Brasileira de Letras Jurídicas (*1994, p.631-632, our translation), exists several forms to apply the evidence depending the context: "Artificial Evidence", "Enough Evidence", "Casual Evidence", Circumstantial Evidence", "Complete Evidence", "Documentary Evidence", Exclusively Witness Evidence", "Extrajudicial Evidence", "Founded Evidence", "Indictment Evidence", "Indirect Evidence", "Instrumental Evidence", "Judiciary Evidence", "Judicial Evidence", "Literal Evidence", "Material Evidence", "Oblique Evidence", "Oral Evidence", "Expert Evidence", "Full Evidence", "Pre-constituted Evidence". This is important in order to recognize in which category, born-digital records fit better.

> Computer forensics is often associated with computer security and whilst there are synergies it is most appropriate to think of computer forensics and computer security being opposite sides of the same coin. Computer forensics differs from computer security, the issue of securing computers against malicious attacks […] […] Computer security is a defence against unauthorised and malicious intrusion and computer forensics allows for identification of incidents, gathering of evidence, analysis of evidence and potentially recovery of records.
> Although computer forensics is a subject in its own right it derives principles from forensic science and computer science in establishing an area of study which is unique. Computer forensics has a strong inter-disciplinary background drawing on forensic science, criminology, law, mathematics, audit and business as well as from computer science.

In accordance with Forensics, some researchers still consider this science to be “computational or computer Forensics” (COLLIER; SPAUL, 1992, p.215; BOGEN; DAMPIER, 2004; WHITCOMB, 2002; IRONS, 2006; SHEETZ, 2007; KIRSCHENBAUM, 2008). Meanwhile, other scholars call it “digital Forensics”. There seems to be no distinctions between the two definitions. However, the concept of “digital Forensics” will be used here (similar to the term “digital” record instead of “electronic” record), to distance from the word “computer” and to be aware that digital Forensics encompasses further elements than Computer Forensics. Furthermore, digital Forensics has expanded its object of study not only to the study of computing, but also to the digital environment that surrounds computer mechanisms. This is explained by Chow and Shenoi (2010, p.XVII):

> Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every type of crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in information assurance – investigations of security breaches yield valuable information that can be used to design more secure and resilient systems.

Each category or subcategory that exists within the digital context is divided, as explained by Bogen and Damper (2004, p.141-142):

> - Computer Forensics: Collecting, analyzing, and preserving evidence from digital storage media;

> - Network Forensics: Collecting, analyzing, and preserving evidence that is spread throughout a network of computers;
> - Software Forensics: Determining the identity of the original author of a piece of software, malware, virus, malicious code, etc.;
> - Digital Forensics: The general, emerging discipline that governs the three topics above […].

The aforementioned Computer Forensics, Network Forensics, and Software Forensics definitions are branches or pieces that belong to digital Forensics as a whole. Each branch in the digital world is fragmented, granular, modularized, subjective, and should be analyzed with these same principles and tools.

Thus, the area of digital Forensics is not a novel study as has been previously thought. With the emergence of the Era of Computing in 1948 (POLLITT, 2010, p.4) and its rapid development in the late 20th century, digital Forensics reflected this progress in trying to address several technological issues. Mark Pollitt (2010) presents digital Forensics as a historic evolution separated into “epochs”. He defines digital Forensics as an evolution categorized into pre-history to 1985, infancy 1985–1995, childhood 1995–2005, adolescence 2005–2010, and future 2010 & beyond. Ian Charters (2009, p.5) takes a similar temporal approach, albeit he divides it into “ad hoc, structured, and enterprise phase”. Simson L. Garfinkel (2010) divides this history into the early days (1980–1999); golden days (1999–2007); and the coming digital Forensics crisis (2010– and beyond).

In table 7, Rogers (2019) outlines an adaption of Pollitt’s article (2010) encompassing the foremost points of the history of digital Forensics:

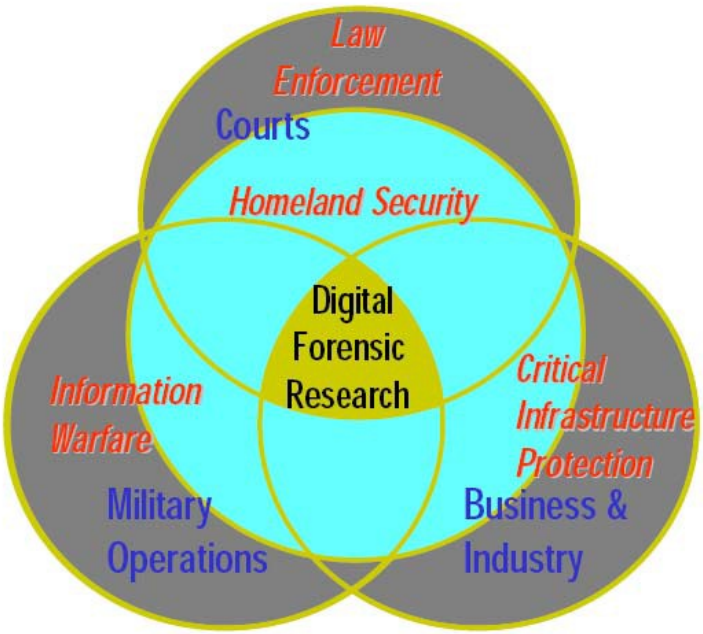
Table 7 – HISTORY OF DIGITAL FORENSICS

Epoch	People	Targets	Tools	Organizations/ Community
Pre-history to 1985	System admin	Mainframe	System audits	Ad hoc, individual
Infancy 1985-1995	Law enforcement; operating outside lab-based forensic practice	PCs, stand-alone, dial-up internet	Command-line, adapted commercial products	IACIS; FBI, IOCE
Childhood 1995-2005	Law enforcement; intelligence; military	Explosion of technology; broadband	GUI commercial and open source forensic tools; standards	Professionali-zation; SWGDE DFRWS; IFIP Working Group 11.9
Adolescence 2005-2010	Investigators, consultants, prosecutors	Virtually any device using electricity	Virtualization	Increase in number/quality of conferences
Future 2010 & beyond			Automation; evidence-based knowledge management process	Education, certification

SOURCE: Quoted from Rogers (2019)

In addition to the epochs, table 7 lists the people involved, the targets, the tools, and the organizations/community. Each of the row headings indicates the evolution and the foremost changes throughout the course of recent history. Moreover, the table allows an explanation of a field that, in the beginning, was directly related to military and legal issues (the business and industrial fields are included later) and how its use expanded from the epoch of “childhood” (1995-2005) to further areas. Currently, Diplomatics is nourished by the theories and practices that are used to address these digital complexities. It is necessary to delve into these changes to analyze how Forensics can be adapted to Diplomatics activities.

Figure 7 – NUCLEUS OF DIGITAL FORENSIC RESEARCH



SOURCE: Palmer (2001, p.4)

Just as Diplomatics, History, Law, Engineering, Mathematics, and other knowledge areas have been important to the strengthening of Archival Science throughout its history, digital Forensics is contributing with practices and elements to try to overcome the difficulties of born-digital records. Conversely, digital Forensics is seen as an important area used to explore the benefits of Archival Science; however, Archival Science is also an area that can offer elements to enhance the processes of digital Forensics. Alastair Irons (2006, p.110) highlights how Archival Science, specifically Records Management can be analyzed and used as aids in digital Forensics:

> The relationship between records management and computer forensics is, however, not all one way. There are many records management techniques and skills, such as metadata expertise, functional requirements for electronic records management, digital preservation, retention management, knowledge of digital libraries and archives, skills in data analysis, managing the electronic knowledge of an organisation and the understanding of intellectual property regulations which could contribute to the analysis and audit activities associated

> with computer forensics. In addition, in the area of recordkeeping systems design and implementation, methodologies such as DIRKS (State Records New South Wales, 2003) and others (Johnston, 2005), records managers have valuable knowledge and expertise to bring to the table and share with their computer forensics colleagues.

As a consequence, the relationship between digital Forensics and Records Management explained by Irons should be analyzed with care. To date, the same concepts are used in both sciences, but with a different meaning and application. An attempt will be made to differentiate the concepts of both areas to understand how these concepts can be applied in the digital contexts.

In the aforementioned idea expressed by Irons, the role of the archivists in the records management processes, business continuity, archival practices, legal supports, etc. is paramount. Their knowledge within any institution concerned with the maintenance, preservation, and constant use of records, especially born-digital materials, determines their importance.

For this knowledge to be effective, there must be a clear communication and division of responsibilities, mainly between Information Technology IT and Digital Forensics (if exists), to determine for instance: what kind of records are important within the institution to be preserved over time; what are the policies of maintenance, preservation, and constant use; what digital archival repositories are used for storage; if policies of migration to other digital repositories exists; how to maintain integrity, and so forth.

With this overview, digital Forensics in the first decade of the 2000s achieved some prevalence as its own field, and as a support to other disciplines. This was valued by archival researchers who used its processes to further explore the field of forensics as a support to issues of Diplomatics practices. An idea that had already began with the concern of the archivist Elizabeth Diamond (1994), as stated in her scientific paper, “The archivist as forensic scientist: seeing ourselves in a different way”.

Thus, we notice how digital Forensics is becoming an inseparable area of Diplomatics issues. This relationship was utilized in the projects and the research of the InterPARES 3 (2007–2012) and Digital Records Forensics Project DRFP (2008–2011), led by Duranti and Rogers, respectively. However, the existence of further relevant projects, courses, and research related to

digital Forensics and records management[92] will also be explored in this work. Albeit, priority has been given to the InterPARES and DRFP experiences at the University of British Columbia – UBC in Vancouver, Canada, because their contribution fundamentally enhanced this study.

Duranti (2010, p.109) tried to bring together Diplomatics and Forensics knowledge in an attempt to deal with the challenges of the digital context:

> Two of the most challenging issues presented by digital technology to the law enforcement, records management, archival and legal professions, researchers, business, government and the public are the identification of "records" among all the digital objects produced by complex dynamic and interactive systems, and the determination of their "authenticity." The first issue—the identification of digital records—is addressed by Digital Diplomatics, a contemporary development of a centuries-old discipline that studies the nature, genesis, formal characteristics, structure, transmission and legal consequences of records (Duranti, 1996, 1998). The second issue—the assessment of the authenticity of digital records—is only indirectly addressed by Digital Forensics, which is defined by Ken Zatyko as "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation" […].

Duranti highlights that Diplomatics and Digital Forensics studies from their perspective to try to assure the authenticity of the born-digital records. Therefore, many contemporary works are related to Diplomatics projects, concepts, and practices that have been incorporated from Forensics that provide vital contribution to the field.

The research has its challenges when two sciences come together, in this case, digital Diplomatics and digital Forensics, which have their own boundaries to approach born-digital records. These boundaries are relevant to observe how these elements perform and how they work in each area. Rogers (2013, p.7) describes some issues to consider in both sciences:

> One barrier to the integration of archival and digital forensic principles has arisen from the definitions and terminology specific to each discipline. Carrier and Spafford define "digital object" as "a discrete collection of digital data, such as a file, a hard disk sector, a network packet, a memory page, or a

[92] Formal forensics education is performed in 16 Certificate Programs, 5 Associate Level Programs, 16 Bachelor Level Programs, 14 Master Degree Programs, and 3 Doctoral programs. In: http://www.digitalforensicsassociation.org/formal-education/

> process” [16]. The state of the digital object is an expression (or value) of its characteristics (unique features) that derive from how and why the objects are created. A digital event is any occurrence that changes the state of the object, and every object is evidence of at least one event. This view of digital objects is event- and state-based, a machine behavior model grounded in a technological point of view. The creator of digital evidence in this model is a theoretical Finite State Machine (FSM), with a finite set of inputs that act on a state (a set of bits) and produce a new state and output values. The activity of the FSM produces traces, or evidence of events, which may be investigated and interpreted by the digital forensics examiner [6].
>
> Contrast this with the view of digital evidence held by archivists. Digital evidence exists in the form of data (smallest meaningful unit of information), documents (recorded information), and records (documents made or received in the course of some practical activity and set aside for further action or reference) generated and/or maintained in digital form. The creator (i.e., author or recipient) of digital evidence is a juridical actor (human or otherwise.) This juridical actor creates data, documents and records whose rich contextual information (administrative, provenancial, procedural, documentary, and technological), revealed through archival and diplomatic processes, support its evidentiary capacity.

What Rogers sees as a barrier is a clear and objective definition of concepts in each field of study. As was written in the first chapter, a similar discussion was held when Diplomatics began to be adapted to Archival Science. Diplomatics analyzes the authenticity of each record, differently than Archival Science, which analyzes the set of records through of archival bond. With the application of Diplomatics to Archival Science, the authenticity of the records is addressed organically in an archival sense.

Digital Forensics works with digital objects and digital events as evidence. Archival Science on the other side, works with data, documents, and records within contextual information. This differentiation can be used to address the born-digital records as evidence in an archival, legal, and historic sense, and this is important to recognize the different meanings of concepts in each studied area.

To summarize, historically the field called Forensics was built with the rules of the Law and used to solve the complexities of a number of disciplines. In the late 20th century, Forensics gave birth to Computer or Computation Forensics, which was initially developed to control cybernetics crimes, defined in figure 7 by Law Enforcement, Military, and Industry domains. Finally, digital

Forensics, which is a junction between Forensics and Computer, also helps to control digital crimes and provides archivists support for archival and/or administrative business activities.

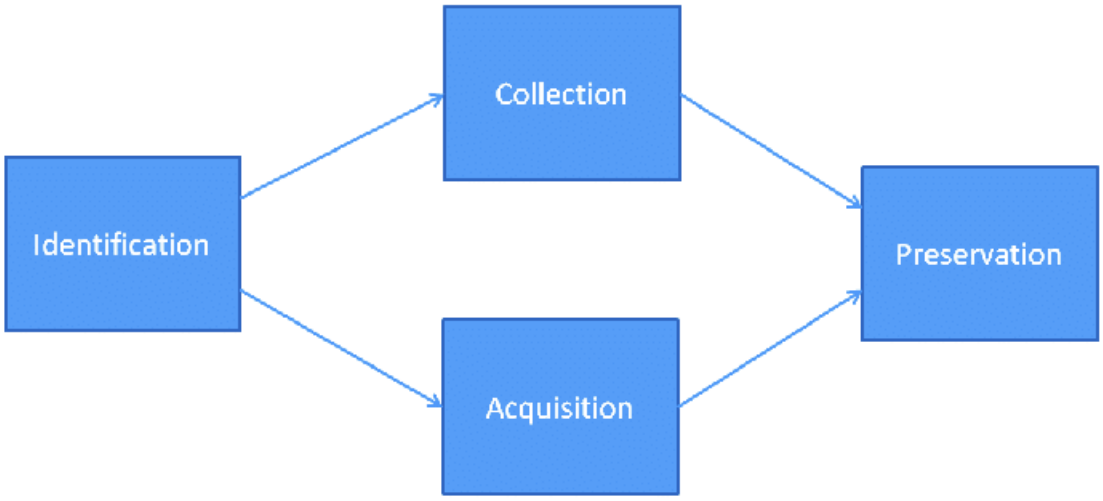
4.4 DIGITAL FORENSICS AS FOUNDATION TO DIGITAL DIPLOMATICS

For a better understanding of how digital Forensics supports to digital Diplomatics practices, its main concepts and terminology must be analyzed. An extensive and complex list of terminology related to digital Forensics research is not needed; however, it is necessary to analyze how these elements and concepts deal with born-digital records in archival contexts. How these elements can improve their trustworthiness during creation, maintenance, and preservation over time will be also explored.

The necessity to delve into Forensics concepts will explore how they work within their own area and then, how these elements contribute to digital Diplomatics. Similar terms for concepts describe different functionalities in Forensics and Diplomatics. Thus, the terms must be adapted and incorporated to reach the desired DAFD, in digital contexts, that allows an improved process to verify authenticity.

As outlined at the beginning of this chapter, Forensics experts might follow a series of steps determined by this science, which is summarized mainly in the ISO 27037 (2013), as shown in figure 8. The phases most used in this process follow the definitions by Brian Carrier and Eugene H. Spafford (2003), and André Årnes (2018) – identification, collection, preservation, examination, analysis, and presentation – are explored in table 8. In addition, existence of other phases such as validation, interpretation, and documentation presented by Gary Palmer (2001, p.16), could be incorporated in the previously mentioned named phases.

Figure 8 – EVIDENCE-HANDLING PROCESSES ACCORDING TO ISO 27037



SOURCE: Cloud Security Alliance (2013, p.11)

Table 8 – COMPARISON OF DIGITAL FORENSICS PROCESS

ANDRÉ ÅRNES	BRIAN CARRIER & EUGENE H. SPAFFORD
Identification:	
The task of detecting, recognizing, and determining the incident or crime to investigate.	Detect the incident or crime.
Collection:	
Collection of data from digital devices to make a digital copy using forensically sound methods and techniques.	Search for and collect electronic evidence. **Secure and Evaluate the Scene**: Secure the scene to ensure the safety of people and the integrity of evidence. Potential evidence should be identified in this phase. **Document the Scene**: Document the physical attributes of the scene including photos of the computer. **Evidence Collection**: Collect the physical system or make a copy of the data on the system.
Preservation:	
The processing of potential evidence normally starts during the identification phase, and it is crucial to preserve the chain of custody and evidence integrity from the very start. This includes activities to isolate, secure, and document the physical and digital devices at hand. Evidence preservation may require the assessment of technologies for subsequent copying of the original media, establishing time synchronization, and any other tasks that facilitate additional forensic activities.	Isolate and secure the physical and digital evidence.
Examination:	
Preparation and extraction of potential digital evidence from collected data sources.	A technical review of the system for evidence.
Analysis:	
The processing of information that addresses the objective of the investigation with the purpose of determining the facts about an event, the significance of the evidence, and the person(s) responsible.	Determine significance and draw conclusions based on the evidence found. Repeat examination until a theory has been supported.
Presentation:	
The process by which the examiner shares results from the analysis phase in the form of reports to the interested party or parties.	Summarize and provide an explanation of the final conclusions and theory.

SOURCE: Quoted from Carrier; Spafford (2003) and Årnes (2018)

The processes presented in table 8 contains some points that must be considered. First, preservation was defined by Årnes (2018, p.22) as a “sub-activity” within the identification process intended to protect the integrity and chain of custody of the evidence and not as a phase in and of itself. Second, for Carrier and Spafford (2003, p.10), preservation is a phase of the forensics process, which deals with the protection of data integrity during the investigations processes:

> The **Preservation Phase** of the digital crime scene involves securing the entrances and exits to the digital scene and preserving the digital evidence that could change. In the physical world, this involves reducing foot traffic and collecting physical evidence that could be lost because of weather. In the digital world, this includes isolating the system from the network, collecting the volatile data that would be lost when the system is turned off, and identifying any suspicious processes that are running on the system. Suspect users that are logged

> into the system should be noted and possibly investigated. Log files can be considered an eyewitness to the crime and should be secured if there is a threat that they will be lost before the system is copied. Note that other models use "preservation" to refer to preserving digital evidence. In this model, the entire digital environment is being preserved. In fact, no digital evidence has been identified yet when this phase occurs (CARRIER; SPAFFORD, 2003, p.10).

Third, the concept of preservation for digital Diplomatics works differently than for digital Forensics. Preservation in the digital Diplomatics sense is related to the maintenance of the records over the long-term to “preserve perpetual memory” (DURANTI,1996, p.243). Thus, InterPARES 2 (p.41) defines records preservation as:

> **records preservation** n., The whole of the principles, policies, rules and strategies that controls the physical and technological stabilization and protection of the intellectual form of acquired records intended for their continuing, enduring, stable, lasting, uninterrupted and unbroken chain of preservation, without a foreseeable end. Syn.: archival preservation; permanent preservation. See also: digital preservation; persistent object preservation; preservation.

The preservation process for digital Forensics is concerned with the care of data integrity of digital evidence so it is not corrupted or tainted during the investigation. For digital Diplomatics, preservation mechanism is concerned with the care of data integrity in the same way as digital Forensics, but in addition it is concerned with the assurance of data integrity over time. These clarifications are relevant because these three sciences have similar concepts to the same object studied, but with different applications and with the aim to achieve DAFD.

This research defined accuracy, reliability, and authenticity as the cornerstone of digital Diplomatics to obtain the supreme trustworthiness. Digital Forensics has also its own “trustworthiness” concern related with digital evidence. The trustworthiness in a digital Forensics manner is defined in concepts of integrity, authentication, reproducibility, non-interference, and minimalization.

Integrity appears as the foremost element to achieve the trustworthiness in digital Forensics and one of the elements that provides technological knowledge to Archival practices. The relevance of integrity relies on its use in the data integrity, bitwise integrity, and computer and system integrity. When the bitwise integrity is assured, in that the original bits are in a complete and

unaltered state from the time of capture, the data integrity is assured. Computer integrity means that the computer process produces accurate results when used and operated properly and it was so employed when the evidence was generated. System integrity means, a system could perform its intended function in an unimpaired manner, free from unauthorized manipulation whether intentional or accidental (MOCAS, 2004; ROGERS, 2019, s.34-37).

The relevance of integrity to digital Forensics and digital Diplomatics, arises in the versatility to analyze born-digital records as well as the software and hardware. For this reason, Forensics practitioners establish their practices under this process. One of the main labors that they perform when working on an investigation is duplication integrity to not modify the original data.

Authentication, as was referenced in the digital Forensics and the Law section, is a declaration of authenticity. This part shows that the apparent author is the true author through security mechanisms, such as biometrics, cryptographic validation, and corroborating evidence from non-digital sources (ROGERS, 2019).

Reproducibility relies on the guarantee that all the actions taken to examine and extract data can be replicated. This process is also relevant because it can be extended to the archival preservation process, where it is necessary to assure the availability of information in any moment.

Non-interference is the manner to guarantee that the methods and tools used to gather information or digital evidence do not produce changes and, if changes occur, they can be identified. Ultimately, minimalization is the search of essential data to determine purpose. In this case, the targeted search is considered, separating “known good” from “known bad”, and optimizing searches.

Each one of the digital elements of trustworthy digital Forensics (integrity, authentication, reproducibility, non-interference, and minimalization) are considered for Archival purposes. The same way these are be elements that can guarantee archival trustworthiness. To apply the mentioned concepts, standards, policies, rules, and other norms are necessary to guide the proper use that assures the integrity of procedures in determined context.

As digital Forensics is in constant evolution, its rules, policies, and standards are still founded a process of enhancement. Although some

Forensics standards exist, these are defined by different scientific sources. However, this is a normal part of a science that is continuing to be constructed. Michael W. Andrew (2007) explains that digital forensics was still in its relative infancy and mentioned some interesting standards that contribute to improve the science, which can also be useful to digital Diplomatics.

The standards described by Andrew (2007) are based upon some legal cases listed here in the digital Forensics and Law section, such as: *Frye and Daubert,* Rule 702 in the Federal Rules of Evidence*,* and *Kumho Tire v. Carmichael*. These rules helped Andrew to develop seven standards: The Principle of Consistent Result, The Principle of Static Storage, The Law of Association, The Law of Context, The Law of Access, The Law of Intent, and The Law of Validation (ANDREW, 2007, p.23)

The principle of Consistent Result implies that the use of “A well designed system will produce consistent results from any given action unless corrupted by an outside force” (ANDREW, 2007, p.23). This principle can be applied to trustworthiness of repositories. If the repositories have trusted archival features to preserve the records, better records will always be obtained.

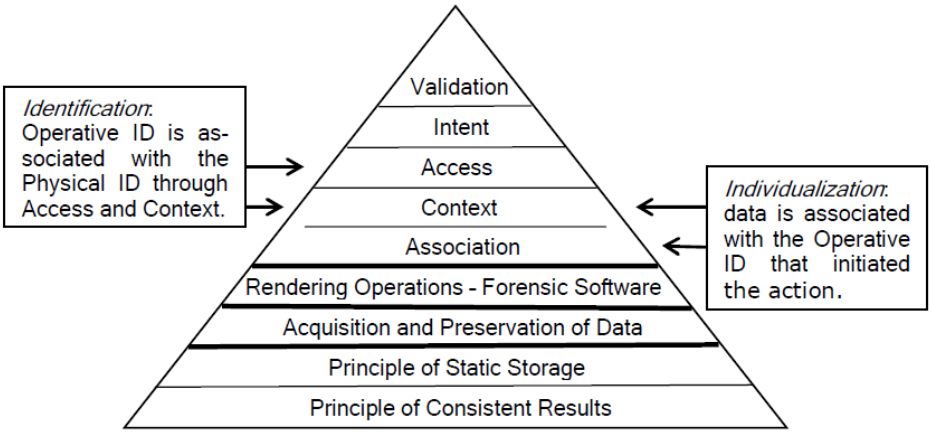
The principle of Static Storage means with although the digital data is latent, the practitioner must identify the possible changes when they occur: “Data at rest will remain at rest unless accessed for a directed purpose” (ANDREW, 2007, p.24). This principle has a relationship with the Non-interference (or identifiable interference) pointed to by Sarah Mocas (2004, p.63).

The Law of Association states that the “Data must be correctly associated with both the processes that created it and the source that initiated those processes” (ANDREW, 2007, p.24). This law redeems the exchange principle created by Locard in the digital environments, which is another law that highlights the trust of born-digital records and systems.

The Law of Context points to the necessity to contextualize the internal (systems) and external (peripheric of computers) elements to understand that “Data can only be interpreted correctly in context” (ANDREW, 2007, p.26). For digital Diplomatics, the context appears as a relevant concept.

The Law of Access, “It must be demonstrated that the individual had access to the device at the time the data was created” (ANDREW, 2007, p.27).

This law establishes the recognized authorship of records. One of the



cornerstones of digital Diplomatics are the persons involved with records, the author of born-digital records must be identified.

The Law of Intent is the accountability of data and records: “It must be demonstrated that the data was created as the result of an intentional action taken by the user. Conversely, the analyst must be able to refute any claims that the system was corrupted and controlled by an unknown agent” (ANDREW, 2007, p.28). For, digital Diplomatics the accountability starts with the data-creator and then passes to the record/archivist.

Ultimately, The Law of Validity, means that: “The integrity, authenticity, and accuracy of the data must be validated before it can be presented as evidence in support of conclusions and opinions” (ANDREW, 2007, p.29). Another relevant and traditional knowledge from digital Forensics experts that must be applied in Diplomatics Archival activities.

All these listed principles and laws are described in figure 9 for a better understanding of how they should be used in DAFD.

Figure 9 – DIGITAL FORENSICS PROCESS MODEL

SOURCE: Andrew (2007)

With the Forensics phases and trustworthiness elements described, the examiners can analyze the digital evidence structured in layers as is explained by Kenneth Thibodeau (2002), such as physical objects: signs inscribed on a medium; logical objects: processable units, and; conceptual objects: what we deal with in the real world. The definitions are similar to Rogers (2015, p.11), who writes that a conceptual layer is an object as it is recognized and

understood by a person; a logical layer is an object that is recognized and processed by hardware and software; and a physical layer is an inscription of signs a physical medium. Additionally, Rogers (2015, p.11) goes deeper to explain that several layers of abstraction into the logic layer exist, for example: “application software: word processing, spreadsheets, multimedia, databases, etc.; system software: operating system, utilities, compilers, etc.; hardware: hard drive, optical disk, tape, solid state, etc.”

Christopher Lee perceives the above-mentioned layers of abstraction in levels of representation. He defines them as “levels at a degree of granularity” with important implications for digital curation (LEE, 2012, p.516). These layers are represented in table 9. A column was added on the right side of the table to indicate how each layer works with the above explanation by Thibodeau and Rogers:

Table 9 – LEVELS OF REPRESENTATION

Level	Label	Explanation	Interaction examples	Layer
7	Aggregation of objects	Set of objects that form an aggregation that is meaningful encountered as an entity	Browsing the contents of an archival collection using a finding aid	Conceptual
6	Object or package	Object composed of multiple files, each of which could also be encountered as individual files	Viewing a web page that contains several files, including HTML, a style sheet and several images	Conceptual
5	In-application rendering	As rendered and encountered within a specific application	Using Microsoft Excel to view an .xls file, watching an online video by using a Flash viewer	Conceptual
4	File through a filesystem	Files encountered as a discrete set of items with associate paths and file names	Viewing contents of a folder using Windows Explorer, typing "ls" at the Unix command prompt to show the contents of a directory	Conceptual
3	File as “raw” bitstream	Bitstream encountered as a continuous series of binary values	Opening an individual file in a hex editor	Logic
2	Sub-file data structure	Discrete “chunk” of data that is part of a larger file	Extracting a tagged data element in an XML document (see Stiihrenberg 2012 in this volume) or value of a field in a relational database	Logic
1	Bitstream through I/O equipment	Series of 1s and 0s as accessed from the storage media using input/output hardware and software (e.g. controllers, drivers, ports, connectors)	Mounting a hard drive and then generating a sector-by-sector image of the disk using Unix dd command	Logic
0	Bitstream on a physical medium	Physical properties of the storage medium that are interpreted as bitstreams at Level 1	Using a high-power micro-scope and camera to take a picture of the patterns of magnetic charges on the surface of a hard drive or pits and lands on an optical disk	Physical

SOURCE: Quoted from Lee (2012)

The digital curator Doug Reside (2011) demonstrates the importance of depth in the layers and abstraction of records that are represented in table 9. In 2008, he began to work with the digital files in the Jonathan Larson collection at the Library of Congress. Jonathan Larson was an American composer who died of an aortic aneurysm caused by Marfan Syndrome (VAN GELDER, 1996)[93]. The curator Reside analyzed specifically a Larson's final draft written in an early version of Microsoft Word 5.1 for the Macintosh. When he opened the file with an editor called "Text Wrangler", he noticed a slight modification in the content of the information because of:

> "[…] a setting called "fast save" to speed up the frequent action of writing to a file (a slow process in those days of floppy disks and computers that ran only about 2% as fast as today's iPhones). "Fast save" worked by appending revisions to the end of a file rather than completely overwriting the existing the text. […]".

This "fast save" modified the content without realizing the changes. In this process, the digital curator used a tool called "hex editor" to try to solve the problem because this tool is able to open the texts as it finds it (RESIDE, 2011). In this sense, Lee (2012, p.518) notes some advantages of these sort of tools:

> Similarly, someone using a hex editor to view a disk image bitstream – a copy of the disk that reflects the contents of every storage sector rather than just the files – will be able to see many types of information that are not visible to someone who mounts the drive and views it through Windows Explorer. Examples of such information are contents of unallocated sectors, deleted files, and "hidden" system files. However, someone who only had the hex editor view of the disk image would not be able to experience the WIMP (windows, icons, mouse and pointer) interactions with folders, files and applications to which current users are so accustomed. Someone trying to fix a corrupted file or correct a bug in a viewing application is likely to shift back and forth between the hex editor representation and in-application rendering representation, in order to determine specifically how properties in the former are reflected in the latter and vice versa.

The text editor, as can be seen in level 3 in table 9, works as a mechanism to analyze raw data to preserve the record, and specifically

[93] In: https://www.nytimes.com/1996/12/13/nyregion/on-the-eve-of-a-new-life-an-untimely-death.html

preserves the integrity of the bits, where it is quite easy to modify or tamper with the information.

In these levels of representations outlined in table 9, it is possible to understand how the digital data is structured allowing the protection of the records and establishing methods of preservation since its creation or production. At the same time, with this knowledge, it is possible to establish a better way to migrate, refresh, emulate, or to translate the information to another digital platform with few risks to lose the authenticity of the digital record. Digital preservation is a process that should begin at the creation or production of the born-digital records to maintain the possibility of preserving the ability to reproduce them, as Thibodeau (2002, p.19) states:

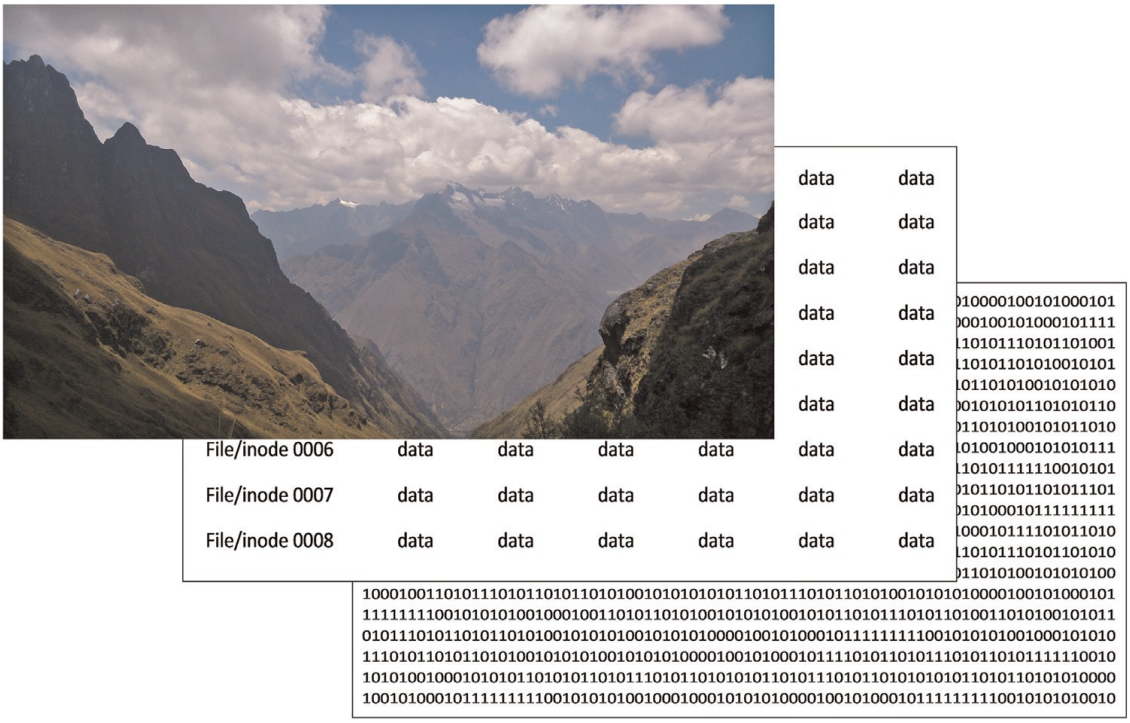
> In addition to identifying and retrieving the digital components, it is necessary to process them correctly. To access any digital document, stored bit sequences must be interpreted as logical objects and presented as conceptual objects. So digital preservation is not a simple process of preserving physical objects but one of preserving the ability to reproduce the objects. The process of digital preservation, then, is inseparable from accessing the object. You cannot prove that you have preserved the object until you have re-created it in some form that is appropriate for human use or computer system applications.

Therefore, the preservation processes for ADF, in the digital realm, produces a meaningful task. A number of institutions are fostering active digital preservation. In this process, for example, the standard ISO 14721: 2012 can create a model to preserve the information in digital platforms with Open Archival Information System (OAIS) (FLORES; PRADEBON; GRAZIELLA, 2017). This model has been considered the core archival concepts to preserve and treat the information such as package: Submission Information Package (SIP), Dissemination Information Package (DIP), and Archival Information Package (AIP) (CCSDS, 2012).

The layers outlined by Thibodeau (2002) and Rogers (2015) are represented by Årnes (2018, p.41). Image 2 displays an example of the conceptual, logic, and physical layers run on the system to produce the composition of born-digital records as a whole. In the image, observe the bitstream (the zeros and ones) fixed in the respective hardware (as is placed in image 3 and level 0 of table 9), the data (the combination between hardware

and software processes), and ultimately, the image of a landscape as is understood by human beings. With this approach and the correct tools, its internal structure can be dug into to make decisions related to the care of integrity authenticity for both archival practices and legal issues.

Image 2 – IMAGE AS SEEN BY USERS, BY THE OPERATING SYSTEM, AND IN HARDWARE



SOURCE: Årnes (2018, p.41).

Image 3 – MAGNETIC FORCE MICROSCOPY (MFM) IMAGE OF BITS ON THE SURFACE OF A HARD DISK

SOURCE: Nanosurf (2005)[94]

Throughout this process as already mentioned, the integrity of digital evidence and the chain of custody are relevant concepts addressed in Forensics, as is pointed to by Årnes (2008, p.22). The digital evidence is used by forensics experts to assure data-integrity in all the forensics phases above mentioned. In addition, archivists work with the records as evidence albeit in a documentary, legal, and historic manner.

Like the digital evidence and chain of custody, the other two core archival principles are the provenance and original order. These concepts belong to *respect des fonds* principle, which allows "[…] maintaining records according to their origin and in the units in which they were originally accumulated". Provenance principle "[…] dictates that records of different origins (provenance) be kept separate to preserve their context". Original order, on the other hand, refers to "[…] an organization and sequence of records established by the creators of the records" (PEARCE-MOSES, 2005, p.280).

In the digital environment, the two indicated principles retain their same relevance the archival processes. However, the functions operate differently in the digital systems than in traditional records. Lee (2013, p.5) highlights the concepts of the provenance and original order and how they perform along with the chain of custody in the digital contexts:

> […] Provenance "consists of the social and technical processes of the records' inscription, transmission, contextualization, and interpretation which account for its existence, characteristics, and continuing history." According to the principle of provenance, records from a common origin or source should be managed together as an aggregate unit and should not be arbitrarily intermingled with records from other origins or sources. In digital environments, it can be important to consider provenance at levels of granularity finer than an entire record, such as why a specific data element appears within a dataset and where specifically the data element was generated. It is also important to include technical components in one's notion of provenance, such as system configuration information. Closely related to provenance is the principle of original order, which indicates that archivists should organize and manage records in ways that reflect their arrangement within the creation environment. There are compelling arguments for retaining original order in a digital environment. Even if this order is messy and idiosyncratic, it conveys meaningful information about the recordkeeping context.

[94] In: https://www.nanosurf.com/en/application/mfm-measurement-of-bits-on-a-harddisk

> The chain of custody is the “succession of offices or persons who have held materials from the moment they were created.” Ideal recordkeeping systems would provide “an unblemished line of responsible custody” through control, documentation, and accounting for all states of a record and changes of state e.g., movement from one storage environment to another, or transformation from one file format to another, throughout its existence. Such a system would therefore cover the point of creation, important interactions with the record, and (when appropriate) destruction.

According to the previous quotation of Lee, the provenance and original order principles continue being used in digital Diplomatics and digital Forensics in digital contexts and can be seen as important contributions from Archival Science. Even though the concepts are addressed differently in the digital environment and the practitioners use data rather than record due to the level of granularity as it was stated by Lee, the core of the principles are to maintain the control of data. The chain of custody ensures that this data organized with the mentioned principles in the computer system is not modified without authorization.

Other forensics tools intended to protect the data integrity and assure the authenticity are the cryptographic hash and timestamps. Cryptographic Hash Function – CHF is related to a series of categories determined in digital signatures, message authentication codes (MACs), and other forms of authentication. In information-security contexts, cryptographic hash values are sometimes called (*digital*) *fingerprints*, *checksums*, or just *hash values*, even though all these terms stand for more general functions with rather different properties and purposes (SCHNEIER, 2004). Cryptographic hash to digital Forensics is explained by Årnes (2018, p.30), such as:

> […] a nonreversible mathematical function that takes an arbitrary amount of data as input and returns a fixed-size string as output. The result is a hash value, and it is mathematically infeasible to find two different files that create the same hash.

According to InterPARES (2008, p.13), cryptography is explained as [..] the practice and study of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text […]. An ancient practice when a message was sent that was meant to be revelated just for the “indicated” person.

Another standpoint of the Cryptographic Has Function, is addressed by Kirschenbaum (2008, p.55-56). The author deems the hashing process as an essential activity, mainly when worked in the imaging function:

> The integrity of a bitstream image can be verified using a technique known as hashing. […] hashing is a long-established electronic operation that has a role in domains ranging from error checking to cryptography. A hash algorithm generates a numeric value that is the mathematical surrogate for a particular bitstream. If the bitstream is altered in any way, by even so much as a keystroke, its hash value will be compromised, providing evidence of the tampering. Here is how one forensics textbook explains a cryptographic hash such as MD5 (developed by Ronald Rivest, the MIT cryptographer who worked on the popular RSA public key encryption standard):
> A cryptographic hash algorithm is a one-way form of encryption, takin a variable-length input and providing a fixed-length output. As long as the size of the original object is within the operational restraints of a particular implementation, it is statistically impossible for cryptographically secure hash algorithms to allow two different source files to have intersecting values, effectively making the hash value into the fingerprint of the original file. Such an algorithm is designed to be collision free, meaning that it is functionally impossible to create a document that has the same cryptographically secure hash value as another document. Because of this characteristic, a hash value can serve as a surrogate for the object it is derived from.
> Hashing thus demonstrates that electronic objects can be algorithmically individualized. If Locard's Exchanche Principle is the first basic tenet of forensic science, the second is individualization - the core faith that no two objects in nature are ever exactly alike, and no two objects ever break or wear down in the same way. Individualization, which we will explore in more detail later, is the principle underlying standard identification techniques like fingerprinting and DNA. An MD5 hash, which yields 2^{160} different values, is in fact a more reliable index of individualization than DNA testing[95].

Kirschenbaum explores the importance of applying the hash value as a reliable marker intended to indicate the authenticity of the data. Digital Forensics, following the quotation, enables forensics experts to attempt to establish a technical mechanism to care for the data avoiding its contamination or tampering in each phase, explained earlier.

In the end, timestamps are a tool used within digital Forensics to perceive the changes that can occur to the data or system. This element could be considered as an activity that can reinforce the chain of custody process.

[95] (Explanatory note by the author): Warren G. Kruse II and Jay G. Heiser, computer forensics (Boston: Addison-Wesley, 2002), 89; emphasis in original.

The definition appointed by Årnes (2018, p.37), establishes that the timestamps work as:

> A systems internal clock should always be noted, as should any deviations in time zones or suspicions of incorrect system clocks. The recording of correct timestamps in an investigation can help identify correlations across multiple data objects. In addition, adjustments have to be made if the clock of one digital device is off and not synchronized relative to accurate time sources. The investigator also needs to know whether the forensic tool being used will display and support different time zone settings, and how these relate to local machine times and UTC (coordinated universal time).

InterPARES (2008, p.17) addressed this timestamp element from the digital records point of view, explaining it as "[…] A binary code attached to a record indicating the time that an event occurred, such as creation, receipt, reading, modification, or deletion". The Årnes explanation approaches the concept as a whole to write "multiple data objects". On the other hand, InterPARES filters the concept in relation to the digital records.

This overview systematized the definitions of the tools analyzed by InterPARES from a Diplomatics Archival perspective, by Mathew Kirschenbaum from an American Archival perspective, and by André Årnes from a digital Forensics perspective, with the intention to make a comparison that supports better understand about the concepts and how they can be applied to born-digital records.

These two chapters explored how digital Diplomatics and digital Forensics perform to ascertain born-digital records. Digital Diplomatics addresses the record with the purpose of guaranteeing the authenticity through the external and internal elements described in the first chapter. Digital Forensics has a similar way to examine the authenticity of a record, by delving into its granular composition from the electrical functions until arriving at the record itself, the way that we understand it as human beings.

When these two sciences are contextualized in Archival Science, some core concepts should be considered and adapted to understand the concept of trustworthiness. The authenticity concept, a relevant concept to digital Diplomatics and digital Forensics should be employed to analyze two other concepts of accuracy and reliability. Therefore, authenticity, accuracy, and

reliability establishing the trust of the records in an Archival context to make a record admissible in diverse contexts as required.

5 DIGITAL ARCHIVAL FORENSICS DIPLOMATICS: A SCIENCE TO NEW USES

> Elizabeth Diamond pointed out in 1994: “If the historian is the layer in the court of the history, the archivist is the forensics scientist”. Today, her idea can be expanded as: both archivists and forensics scientists work together, as keepers of digital authenticity, to maintain trustworthiness of records in the court of History.

When the series of articles “Diplomatics: New uses for an old science” was published by Luciana Duranti (1989), the academic revolution in North America began to think about an opportunity to adapt a European science to the American reality in Archival matters. These new uses were accepted mainly in various territories of Canada and later were constituted in a key science addressed in South America. Currently, most degrees in Archival Science require the study of Diplomatics.

Can digital Forensics solve these sorts of problems? To a certain extent, it is impossible, but the contribution of digital Forensics to Archival issues is widely recognized, especially in United States and Canada. The scientific efforts to deepen and improve Forensics practices that are intended to offer better supports is beginning to materialize. As described throughout this work, digital Forensics still needs to standardize some core practices to loan better tools, methods, and concepts to other sciences, in this case, to digital Diplomatics.

Thus, as recognized in the international experience at the University of British Columbia – UBC and already described in this doctoral dissertation, some concepts from digital Forensics need to be conciliated to be suitable for Archival practices. For this reason, the Forensics chapter included a series of similar concepts but with different uses in Forensics and digital Diplomatics, such as preservation, integrity, authenticity, and authentication

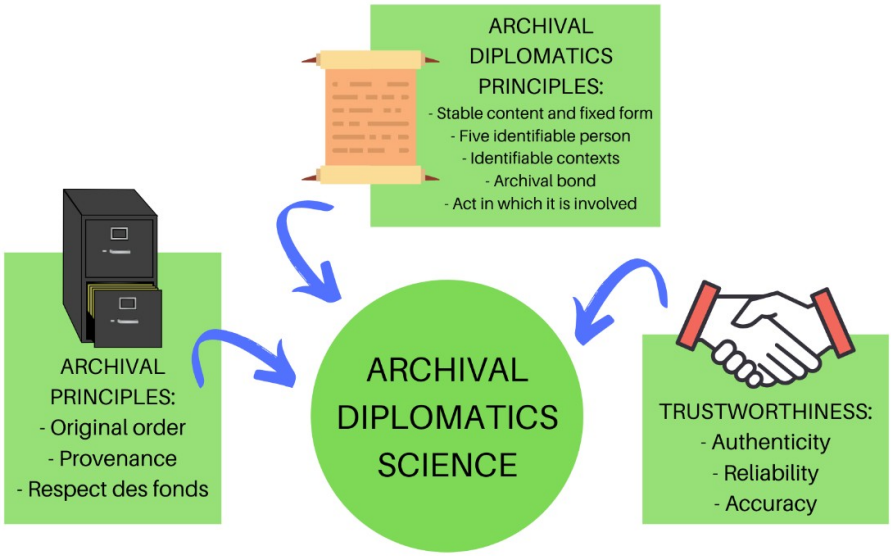
In the same manner that Diplomatics had to adapt some core concepts to become digital Diplomatics, digital Forensics is working towards these purposes. For instance, Diplomatics perceives authenticity as a core concept that deals with the examination of documents in isolation. Its contribution is relevant to analyze the authenticity of individual documents in records organically linked in Archival Science, which is called archival bond.

On the other hand, digital Forensics deals with some concepts seen by some researchers as “barriers” (DURANTI, 2010; COHEN, 2012; ROGERS, 2013) to be incorporated into the archival reality. For example, authenticity is one of those terms. The advantage is that authenticity for digital Forensics is the primary element for Forensics practitioners, establishing a relevant addition to Archival contexts.

Hence, we described how the concepts of Archival, Diplomatics, and Forensics could work together to benefit born-digital records. These issues were addressed in the international experience, and same barriers are still being worked on in North America, probably for two motives: first, the developing of a recent science and, second, for the organization to understand and apply concepts in and out of the mentioned science. Thus, as discussed in the Forensics chapter, this science in digital context is relatively new and is still being enhanced. For this reason, Forensics practitioners and archivists are combining efforts to generate better contributions.

It is necessary to establish a connection to imagine how Archival, Diplomatics, and Forensics could be ideal connection that supports the digital issues. First, Archival Science consolidates the principles that deal with records that were already stated in this dissertation: original order, provenance, and *respect des fonds.* The connection with Diplomatics to support Archival Science can expand the limits of the object of study. In this sense, digital Diplomatics principles provide some alternatives to the required characteristics of a digital record: stable content and fixed form, five identifiable persons, identifiable context, archival bond, and the act in which it is involved. This principle increases the trustworthiness of records, as is seen in figure 10:

Figure *10* – ARCHIVAL DIPLOMATICS FRAMEWORK



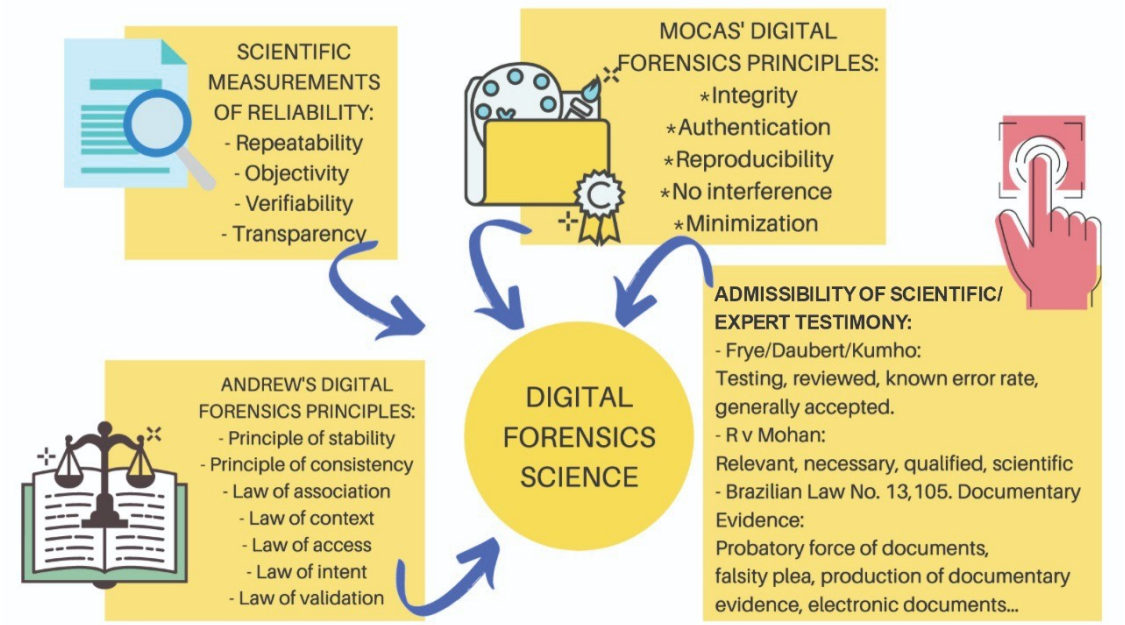
SOURCE: Quoted from Rogers (2019)

Thus, the concepts of digital Forensics are being integrated into Archival Diplomatics to create the possible field of DAFD. These Forensics concepts, as already explained, share elements from Computing and the Law. In addition, to identifying digital technological methods and tools to seize data, information, and records, Computing provides a series of scientific measurements of reliability, such as repeatability, objectivity, verifiability, and transparency, to avoid the loss or contamination of data.

Following the application of the above technological methods and tools, the use of polices, standards, and rules are relevant to guide their proper use. Thus, the digital Forensics principles described by Sarah Mocas (2004) were identified as mechanism to increase the reliability of digital Forensics process. These principles are integrity, authentication, reproducibility, non-interference (or identifiable interference), and minimization. Keeping in the same process, the chain of custody is important to not change the evidence.

Other interesting digital Forensics principles were listed by Michael Andrew (2007), namely: principle of stability, principle of consistency, law of association, law of context, law of access, law of intent, and law of validation. The principles described by both Mocas (2004) and Andrew (2007) along with the measurements of reliability are represented in figure 11:

Figure 11 – DIGITAL FORENSICS



SOURCE: Quoted from Rogers (2019)

Ultimately, the link between the elements of Archival Diplomatics and Forensics is possible, as ways to ascertain the trustworthiness of born-digital records. To do this, it is necessary to revisit how digital Forensics is analyzed in our own social reality: how the national legal norms support elements to establish better records; how the law enforcement institutions, such as the Brazilian Scientific Police, work with digital records[96]; and how the local universities and research centers work with the complexity of digital matters involving digital Forensics and Archival Diplomatics practices.

As charted in figure 10 and 11, the efforts of academics are providing interesting results, and these experiences can be adapted in our contexts and rules. Thus, figure 12 meets all the characteristics before listed to establish a robust science. Archival Diplomatics provides core elements, and its union with digital Forensics strength the mechanisms to assure trustworthiness. For this reason, it was explored how each science mentioned in this work deals in isolation with records, then, how each one of these sciences can interact to create a new science for new uses.

[96] This subject was addressed in 2018 when we got in touch with the Brazilian Police Department in São Paulo. Unfortunately, it was not received a response from this institution.

Figure 12 – ARCHIVAL FORENSICS DIPLOMATICS

SOURCE: Quoted from Rogers (2019)

Archival Forensics Diplomatics is already occurring, and even though it is still in its formative phase, the outcomes in some countries are offering practical solutions for managing, maintaining, preserving, and accessing records, in trustworthy systems and archival repositories. *BitCurator* Consortium for example, is an open-source project of how Forensics efforts are applied to records management matters. Although the project finished in 2019, the scientific products available on its site has been used for several projects to continue developing and improving the study[97].

With these experiences of the mentioned heritage institutions which include museums, library, and archives, it would be interesting to explore a technological tool such as *Bitcurator,* as a digital platform and to bring together other consolidated archival software in Brazil, such as *Archivematica* and *Atom.* The mentioned digital platforms could work in an interoperable form because each has its own functionality in records processes.

Bitcurator software works mainly with “old” digital devices, such as diskettes, Universal Serial Bus - USB, and CDs, with the adequate tools to dig

[97] The heritage institutions that continue to analyze its uses include the University of Virginia Library, Emory University, the British Library, the Library of Congress, the University of Maryland, Duke University, the Gates Archive, Stanford University, the University of Texas, the University of Oxford, Indiana University, the National Standards and Technology, the University of Illinois, Yale University, Artefactual Systems, the National Library of Australia, the New York Public Library, and Georgia Tech. In: https://bitcurator.net/people/

into the data, avoiding the loss of the original information. The tools integrated in the software allows:

- ✓ Identification and redaction or protection of private and sensitive information
- ✓ Repair of damaged files and filesystems
- ✓ Recovery of accidentally deleted or hidden data
- ✓ Generating logs of extraction and analysis activities
- ✓ Identification of files types and sizes (MUMMA, 2011).

These kinds of physical devices are being replaced by modern devices such as cloud computing and other “dematerialized” platforms. Hence, the “old” digital devices are becoming like those paper-based records saved in cardboard boxes abandoned in garages or rooms without minimal conditions. The difference is that paper records can sometimes survive hard environments or physical conditions, but digital devices are more sensitive and the risk of damage is high in a very short time.

6 CONCLUSIONS

Throughout this work, essential points were explored to understand the complexities of digital Archival and the key role of born-digital records as part of object of study. The initial project for this dissertation has altered since 2017. In that year, the project was being reviewed by the São Paulo Research Foundation – FAPESP. In 2018, the project was progressively improved with the reading and analysis of national and international scientific literature to be aligned with the current research. Then, with the study abroad opportunity in 2018 financed by FAPESP, through the Research Internship Abroad - BEPE, the InterPARES and DRF projects were explore *in situ* at the University of British Columbia – UBC. Finally in late 2019, the work was improved with the essential feedbacks from the titular committee members in the first oral defense of the proposal.

Therefore, this dissertation accomplished the objectives laid out at the beginning of the doctoral research. The born-digital records chapter was placed at the beginning of the research, because it was necessary to understand and address the internal composition of this object. The information was relevant also to establish the starting point to comprehend how born-digital records should be managed in trustworthy repositories, and how Archival Forensics Diplomatics could support methods to verify their authenticity.

Hence, a number of projects and research were analyzed that have worked and explored this sort of digital format, such as the Recordkeeping Functional Requirements Project (1993-1996), the InterPARES Project (1999-2019), the Records Continuum project (1990-), and other academic approaches that define the record as a form of representation, that is, a record not only perceived as only an instrumental object. In the latter perspective, the contribution of academics, such Jennifer Meehan (2006), Heather MacNeil (2000; 2002), and Geoffrey Yeo (2007; 2008), were relevant to analyze. With this background, it was possible to explore the requirements of born-digital records for trustworthiness to be admissible as evidence in administrative, archival, historical, technological, legal, and further contexts.

The concept of authenticity as understood in the international experience appears as a branch of a whole framework, led by the trustworthiness concept. Trustworthiness, in addition to analyzing the authenticity element, encompasses the accuracy and reliability concepts. Hence, this work addressed in several parts the importance of trustworthiness of born-digital records, but future works shall delve deeper and explore this core for the archival matters.

Following the course of this research, a pathway was performed to adapt Forensics to Archival Diplomatics in the Brazilian reality. To accomplish this issue, this dissertation explored how each one of sciences evolved in its own form through time, until its use to support the digital phenomenon. For this reason, an epistemological and historical approach was first employed to acknowledge the contribution of Diplomatics and Forensics through the time, to examine the core concepts and methods, and to explore how they are currently viewed as support mechanisms.

The paragraph described above was materialized in the historic course of Diplomatics to understand how it was suitable for Archival Science. This has been widely studied by archivists since the late of the 19th century, as was stated by Roger Bautier in the middle of the 20th century. The traditional scholars studied in Archival Science and other authors were discussed to recognize the different uses of Diplomatics and how the elements remained the same. Thus, Diplomatics was explore from its foundation with Mabillon in the 17th century, through the main exponents in the subsequent centuries until reaching the 21st century.

After analyzing the Archival Diplomatics matter, Forensics was addressed. This science is the core of this doctoral dissertation mostly for two reasons: first, for the results in the international field, where digital Forensics area is being incorporated into the Schools of Information (*ischool*) in several universities, mainly in the United States and Canada[98]; second, for the methods,

[98] Although other studies in universities and research centers exists overseas, the research in these matters have major visibility and development in North America. In the same way, North American universities and universities abroad have agreements to exchange the scientific knowledge about digital Forensics and Archival Science. An example of this is the agreements of BitCurator Project with other international scholars, such as Klaus Rechert at the University of Freiburg, in Germany, and Carl Wilson at the Open Planets Foundation, in UK: https://bitcurator.net/bitcurator-access-people/

tools, concepts, and elements that are being applied as contributions to Archival Science practices. These two points were detailed throughout this research.

Furthermore, some considerable constraints were discovered in the international experience related with the InterPARES and DRF projects, respectively. In regard to InterPARES, the project was in its final year of research, and it was difficult to obtain an academic connection with the members of the project. The objective of this initial project was to have contact with the international InterPARES members to collect scientific information. However, the meetings occurred mostly online, due to the large numbers of members involved in the project throughout the world. This issue was finally resolved in the meetings with the director of the project, and some members, such as Victoria Lemieux, Corinne Rogers, Darra Hofman, and Lois Evans.

The Digital Records Forensics Project – DRFP ended in 2011. The initiative was to explore the other areas of this project, such as the UBC Faculty of Law, and the Division of the Vancouver Police Department. However, both UBC Faculty of Law and Vancouver Police Department were active just during the period of the project. However, similar to InterPARES, Corinne Rogers, the leader of this project, kindly provided value information for the continuation this doctoral dissertation. In addition, as was stated in the beginning of this dissertation, there was the opportunity to discuss the Forensics elements in her Topics in Archival Automation Digital Records Forensics course in 2019.

That course was enlightening because it helped to link the three sciences in question: Archival, Diplomatics, and Forensics, as found in chapter five. The approach of the concepts and elements explored in each of these sciences elucidated the thresholds of Archival, Diplomatics, and Forensics as well as the manner that the elements are applied in each mentioned science and the awareness when the three are jointed to become DAFD. Therefore, the knowledge learned in the international experience was carefully systematized and analyzed to be shared in this study, accounting for ongoing Brazilian research.

Thus, the objectives drawn out in this dissertation were completely achieved. By starting with the general objective, it was possible to delve deep into the theoretical concepts of digital Diplomatics and Forensics as a way to understand how knowledge of these sciences provides relevant methods to

Archival thoughts and practices. The collected experiences permitted dividing the contribution of Diplomatics to analyze the internal and external elements of born-digital records, intended to ascertain the authenticity issue.

Diplomatics studies are being explored mainly in Canada, with the ongoing scholarly projects at the University of British of Columbia – UBC. In the United States for example, even though the relevant contribution of Diplomatics is recognized, its approach is rarely analyzed in undergraduate and graduate university courses, perhaps, due to the complexity to adapt this ancient European science to a different reality. However, for the purposes of this study, Diplomatics became a core science, because it establishes phases to identify the verification of authenticity of records analyzed individually to then approach the organicity of records in Archival scenarios.

On the other hand, Digital Forensics is being explored and applied both at universities in Canadian and the United States in a similar manner. This science has been well received by the archival scholar community, as an interesting field that needs to continue to develop future research. For this relatively new science, as was noted in digital Forensics section, the efforts and scientific contributions are growing. Digital forensics and records management professionals are combining their experience in archival practices to improve the authenticity intended to preserve the digital information for the long term.

Following with the specific objectives, the first one sought to study the constitutive elements from the born-digital records and their importance within Archival Science. Born-digital records are the mainly object of study throughout this research. Thus, the science addressed in the work intends to provide some answers to the difficulties of managing and preserving this kind of support. The complexities perceived in this digital era require creation of new mechanisms to face the difficulties related to authenticity. In this way, it was necessary to analyze the key concepts of sciences, such as History, Law, Diplomatics, Forensics, Archival, and Information Science, to understand how each one of these areas provide elements to confront the difficulties expressed above.

To fulfill the point noted earlier, it was interesting to understand the nature of digital records by making a series of clarifications in the purposes of this study. The clarifications intended to recognize the difference between data, document, information, and records. Archival Science conceptualizes record as

a core object to be managed in records management/archival processes. At the same time, records/archivist deal with data, documents, and information, which are like little pieces that are contained in records.

It was necessary to work with the concept of “record” to filter from another kind of information, defined as an object “[…] made by or received in the course of a practical activity as an instrument or a by-product of such activity […] (INTERPARES, 2007-2012). This concept, as was established in the born-digital chapter, has a series of mechanisms with legal weight to be considered as evidence for administrative purposes, legal matters, and historical objectives.

It is interesting to approach born-digital records are records created specifically by digital software and systems, and they have a series of attributes considered by the two scientific projects explored in this work: Pittsburgh and InterPARES. For the first project, the attributes of digital records are the content, the media, and the structure. Content is related to the intellectual message; media is the support where the information is fixed; and structure is the logical and physical attributes. For o the mentioned project, the metadata is the foremost element to be considered.

For InterPARES, the attributes of digital records are defined, such as content data, form data, and composition data. Content data has the same definition as in Pittsburg – the intellectual message. Form data means the systems to reproduce the record in a correct form. Composition data is how the system defines what form and content data belong to which record (DURANTI; THIBODEAU, 2006).

These two points of view, even with some similarities, have some specificities, which address born-digital records differently. The Pittsburgh project analyzed the digital records in an evidentiary approach within a recordkeeping system. The InterPARES project analyzes the digital records within the Diplomatics framework. The concept of evidence became relevant in the Digital Records Forensics Project carried out in 2008.

The relevance of the internal composition of born-digital records is the first step to understand how to deal with systems and hardware, and be sized for preservation purposes. Diplomatics and Forensics deal with essential elements and tools, respectively, to ascertain the authenticity in trusted archival

repositories that guarantee this authenticity from the creation to the final disposition. Trusted repositories were another relevant point to be considered as mechanism to assure a proper recordkeeping.

The second reached objective was to explore the historical pathway of Diplomatics and Forensics, as an epistemological process that contributes to the approach of the born-digital record. One of efforts of this research was intended to join various sciences to address the challenges of digital contexts, specifically related to born-digital records. In this whole process, History was the science that enabled exploration of the transformation processes of Diplomatics and Forensics in an individual form, until their adaptation into the digital realm. The justification to apply the contribution of History to approach the two mentioned sciences was first to lay out how the course of their history unfolded, and to analyze in an epistemological way the core concepts and elements that remain today to face the current challenges.

During the historical process, it was also interesting to explore their familiarity with records and documents. Hence, Diplomatics, Forensics, and Archival Sciences were areas that worked in an isolated form, albeit from the 20th century, some researchers in the three sciences were already working on the possibility of bringing them together to produce better results. The perspectives of Jenkinson (1957) and Bautier (1961) highlighted the efforts to establish the Archival practices.

Elizabeth Diamond (1994) analyzed the possibility of fitting Forensics into Archival Science in a retrospective way. The author started the link of how History, Archival, and Forensics could work together. The outcomes have materialized since the early 2000s, when some forensics/records management scholars, such as: Cohasset (2001), Palmer (2001), Mocas (2004), Irons (2006), Andrew (2007), Zatiko (2007), Kirschenbaum (2008), Garfinkel (2010), and Pollitt (2010) explored the interdisciplinary form to work with the three sciences in question. It is relevant to highlight the baselines provided by digital forensics scholars to establish the difference of applying Forensics in a traditional manner, digital Forensics in digital contexts, and digital Forensics adapted to Archival purposes.

The third reached objective was to analyze the contributions offered by the Diplomatics and digital Forensics within the archival and legal contexts, in

the analysis of the born-digital record as a source of evidence. Another relevant point considered in this research is when born-digital records are analyzed as evidence. The chapter of born-digital records addressed the relevance of better records to be considered as evidence in several contexts, including archival, administrative, legal, and historical. The born-digital records chapter explored mainly three academic perspectives that approach records as evidence: The Functional Requirements for Evidence in Recordkeeping: The Pittsburgh Project; InterPARES Project; and the vision of the records as forms of representation studied for some academics as appear in the mentioned chapter.

The Pittsburgh project was one of the first that explored this issue of evidence. In this process, Erlandsson (1996) provided an interesting concept that joins digital record with evidence defined as “recordness”. When records are kept in the business processes, these records can reach their level of recordness. For the InterPARES research, the evidence matter is important as well, but in a traditional Jenkinson Archival matter, which is seen as valuable evidence of the past. Finally, with Pittsburgh and InterPARES project, another thought line arises that highlights the value of evidence but depends on the purposes of records, that means, evidence for what or for who.

The application of practices to improve the authenticity of born-digital records are standard for most societies in the world. With Archival Science, we recognize the use of several models that are adapted to a determined social reality, such as the continuum or the InterPARES models. As previously mentioned, various universities in the United States ignore Diplomatics in the Archival courses.

In Brazil, the country where this research is being developing, Diplomatics is a cornerstone to Archival courses. Several traditional researchers have consolidated Diplomatics with the issues of authenticity in both physical and digital areas. Thus, the internal[99] and external elements become the supreme concepts to address the Archival elements of provenance, organicity, unicity, and indivisibility or archival integrity (BELLOTTO, 2015).

On other hand, Forensics has a strong relationship with the Law. This science works together with the legal system and is relevant in social context.

[99] In the Brazilian contexts, Heloísa Bellotto also recognizes the use of intermedia elements defining them, as the language, which is the document is written; the form of the written; the documentary specie; and the documentary typology (2015, p.9-10).

The international experience was useful to understand the conceptual elements of the Common Law system and the involvement of the scientific community as a mechanism to improve legal difficulties. Thus, famous legal cases were interesting both in the United States and Canada, because they help to create a series of standards and policies facing legal and documental issues. Those standards and policies are facing up to the challenges of the digital age.

In Brazil on the other hand, this dialogue between the Legal System and the scientific community is barely visible. The Laws and Rules appear as a supreme field carry out specifically by the judges of the Supreme Federal Court, and oftentimes, hardly reflect the social necessity of the society. Therefore, it was necessary to examine the international realities to perceive the contribution of the academic community in legal cases. This necessity is more urgent due to the intended bond between digital Forensics, Law, and Archival Diplomatics.

The fourth objective intended to explore the “authenticity” concept within Archival Science. This objective was approached in a transverse form. When we explored the concept of authenticity in the initial project, this appears as the major element to be met in relation with born-digital records. Therefore, Diplomatics and Forensics deal with authenticity as a key concept. However, for Archival Science, even though authenticity is one key element, this is accompanied with other core concepts: accuracy and reliability.

For Diplomatics, authenticity is the core element since it is the foundation that this science is built on; however, the traditional study of authenticity for Diplomatics is analyzed in singular documents. Heloísa Bellotto (2015) paints an interesting picture of how Diplomatics and Archival Science perform together: Diplomatics approach the document internally to externally, that means, from the document itself until all the archival framework (fonds, sub-fonds, series, etc.). Archival Science approach the general framework to analyze the records.

Hence, Archival Diplomatics is seen by the Canadian and InterPARES studies as just one consolidated science. In this sense, Archival Diplomatics is no longer considered in an interdisciplinary form. The traditional diplomatists continue to explore the science in its orthodox tradition, verifying the authenticity through the external and internal documentary legal form documents. On the other hand, archivists perceive the record with a permanent organic relationship

to other records, which is a whole structure determined by the provenance principle.

The issue of authenticity to digital Forensics is also a supreme element, which must be assured in all the evidence process to be considered as reliable in legal scenarios. Thus, tools, including chain of custody and imaging/hashing functions, are applied within a series of procedures, such as repeatability, objectivity, verifiability, and transparency, determined by several standards, such as the ISO:

- ISO 17025: Requirements for competence of testing and calibration laboratories.
- ISO 27001: Management standards that provides pre-incident planning that makes a forensic investigation possible.
- ISO 27037: Information technology security techniques – guidelines for identification, collection, acquisition, and preservation of digital evidence.

All this process above mentioned enables digital Forensics to reliability ascertain the authenticity of born-digital records and its incorporation into Archival processes. Forensics practitioners, even with all the limitations of this science, highlight the relevant contribution to other knowledge areas and as evolution of Forensics itself. This is the reason why the academic community defined this moment for Forensics research, such as “Forensics readiness”, that means:

> […] a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations. Being forensically ready can help organizations with quicker recovery, improved business continuity, compliance and an improved success rate in legal actions by having available relevant digital evidence (KEBANDE, KARIE, CHOO, ALAWADI, 2021, p.2).

Authenticity in this sense was the key concept from the first through the final chapter.

Hence, the general objective and the specific objectives were successfully achieved making it possible to understand the composition of the layers of born-digital records in Archival thoughts and practices. The contributions of the sciences addressed here facilitate the approach and provide

essential mechanisms to manage better records and system. Therefore, both Archival Diplomatics and Forensics are producing successfully scientific outcomes in the context where they are incorporated.

The purposes of this dissertation are to understand how Archival Diplomatics and Forensics can work together. Ongoing scientific studies are providing elements to understand that it is possible to join the three mentioned sciences to enhance and facilitate the processes of Records Management and Archival activities. As was drawn out throughout the chapters addressed here, the trustworthiness of born-digital records can be achieved following the rules, policies, and standards defined for each described science.

For this reason, it was necessary to understand each science in an individual way and develop a historical course that can analyze the core elements of its structures, foundations, and activities up to now. In addition, the historical transformations through time present elements that both appear and disappear depending on the social contexts and the objectives of the scholar community.

Diplomatics has a substantial historical pathway that started before it was considered as a science by Jean Mabillon, and this is analyzed in Diplomatics chapter. It is relevant to discuss how the science has adapted and provided elements to other science, including, Archival Science. Hence Luciana Duranti (1998) considered it an old science adapted to new uses.

The discussions between archival professionals and diplomatists in the late of 19th century and the early of the 20th century provided the results currently named Archival Diplomatics. Even though Archival Diplomatics studies have some difficulties, the academic efforts demonstrate the possibility of working with both sciences. Currently, the science has demonstrated the ability to offer relevant results, mainly in these digital contexts.

Similarly, the approach of Forensics in a historical manner permitted understanding of the core elements of the science and the changes through time and space. It was seen how the appropriation of forensics elements by other sciences was fundamental to strengthen the processes and practices. Furthermore, the historical outline showed that unlike Diplomatics, it was hard to identify a creator and foundation date for Forensics. It was a practice performed before it was consolidated science. However, its scientific uses in the 19th and

20th century could be pinpoint. The recent foundations provided by this science are being incorporated to overcome the difficulties in the digital realm.

Thus, both Diplomatics and Forensics walked in parallel as mechanisms to provide scientific answers. However, it was not possible to identify if in a historical moment, the two sciences were approached for investigative purposes by the scientific community. Both sciences addressed the issues of document authenticity in its own way. In the decade of 2000, Archival and Forensics studies started to be considered, when archivists and Forensics professionals jointed endeavors to face the digital contexts, particularly with the born-digital records issues.

Therefore, the attempt to consolidated Archival Diplomatics and Forensics sciences as only one science is a work that is under construction. The ongoing researchers prefer to keep the sciences in separate to have a better understanding: Forensics for one side and Archival, or Archival Diplomatics, for another. Luciana Duranti (2010) was the first to call digital Forensics as support to Archival processes as “Digital Records Forensics”. It was an interesting approximation, but the word “records” in the name, narrows its wide affordances. Daniel Flores (2020) proposed the name of “Digital Forensics”, but this term could be understood only to the traditional Forensics investigations and processes.

The literature analyzed throughout this work helps to establish a name more comprehensive for Archival purposes. Thus, the name of DAFD is proposed for a science that provides scientific answers to digital issues. In some specific moments, it should be also called Digital Archival Forensics - DAF, in contexts where Diplomatics is not applied. This name has the justification to explore further the elements, standards, models, tools, rules of digital Forensics, as support to Archival Diplomatics issues.

DAFD was the name most suitable to the research, after analyzing the academic literature, approaching each science in an individual manner, and examining the names given from Forensics to Archival activities. Thus, the label of the name selected will change according with the research advances through time to find the ideal name. Ultimately, baptizing this science as digital Archival Forensics can be made in an arbitrary way. However, some sciences already deal with these historical difficulties, and have been structured with arbitrary

names. In some cases, these sciences can seem or sound like anachronisms now.

Diplomatics, for example, following the point made above, is a science that currently does not address only the authenticity of diplomas but also considers changing its original name is self-defeating. Hence, Manuel Romero-Tallafigo (1994, p.14) point out that to change the original name “Diplomatics” to another name could make the quiddity of the historical structure forged since its underpinning vanish. From an Archival perspective, it would be like shattering its historical provenance.

Ultimately, DAFD meets the elements to embrace the issues that arise in the 21st century with the digital technological, specifically, both born-digital records, systems, and trusted repositories. Thus, the hypotheses established in the introduction of this dissertation were analyzed noting some aspects that should be considered for better and clear results. First, to demarcate as was warned through this study, each of the elements were provide for each science approached with the intention to avoid possible misunderstandings.

Each science analyzed contains its core concepts, standards, elements, methods, and tools as mechanism of support. In some cases, each of these concepts have similar definitions, which were necessary to explore it, because at the time they are applied the purposes mean other uses. This is seen for example, when the concept of preservation was addressed, which arises as a relevant concept to Archival, Diplomatics, and Forensics, but with different use in their practices.

Second, Archival Forensics Diplomatics, although it is science to be discuss and to enhance, meets the characteristics to be applied in different contexts in which the difficulties of born-digital records, systems, and trusted repositories must be to approach. Examples of this are the ongoing projects developed by the international academic communities that meet Forensics and Archival elements, such as *BitCurator*. A software intended to preserve the information from old-fashion digital devices, as mechanism to support the efforts made by archivists that deal with the risk of maintaining accurate information to avoid losing its authenticity. This open-source software should be more explored to future works.

Finally, the propose of this doctoral dissertation was achieved by exploring the core concepts to address the difficulties that arise in the digital contexts. It is necessary to carry out research that bonds several sciences to face digital problems to create better information for all users, in a historical moment where misinformation is threatening democracy throughout the world. This is possible with trusted sources of information where records managers and archivists have today more than ever a core commitment.

REFERENCES

ADAM, A. **A history of forensic science**: British beginnings in the twentieth century. Abingdon: Routledge, 2015.

AMARAL, S. **Falsidade Documental**. São Paulo, Brazil: Editora Revista dos Tribunais, 2ª edição,1978.

ANDREW, M. W. Defining a process model for forensic analysis of digital devices and storage media. **Second International Workshop on Systematic Approaches to Digital Forensic Engineering** (SADFE'07), Bell Harbor, WA, pp. 16-30, 2007. DOI: 10.1109/SADFE.2007.8. Available at: https://ieeexplore.ieee.org/abstract/document/4155347

ANDREWS, M. Structural Metadata: Key to Structured Content. **Story Needly, Content strategy for a post-device era**. 2017. Available at: https://storyneedle.com/structural-metadata-key-to-structured-content/

ÅRNES, A. **Digital Forensics**. River Street, Hoboken, USA: John Wiley & Sons Ltd, 2018.

ARONSON, J. D. **Genetic Witness**: Science, Law, and Controversy in the Making of DNA Profiling, New Brunswick, NJ: Rutgers University Press,2007.

ASSOCIATION OF CANADIAN ARCHIVISTS **(ACA)**. Archival Origins, Conference Program., 6-8 June 2019 Toronto. Available at: https://archivists.ca/resources/Documents/Conference%20Material/Past%20Conference%20Documents/Conference%20Programs/20190605_Archival%20Origins%20Toronto%20V%203.1.pdf.

BARRET-KRIEGEL, B. **Jean Mabillon**. Paris : Presses Universitaires de France, 1988.

BAUTIER, R. H. Leçon d'ouverture du cours de diplomatique à l'École des chartes. In : **Bibliothèque de l'école des chartes**. 1961, tome 119. pp. 194-225,1961. Available at: https://www.persee.fr/doc/bec_0373-6237_1961_num_119_1_449619

BEARMAN, D. A. Diplomatics, Weberian bureaucracy, and the management of electronic records in Europe and America. **The American Archivist**, United States, v.55, I.1 pp. 168-181, Winter, 1992. DOI: https://doi.org/10.17723/aarc.55.1.240053825k3v3648

BEARMAN, D. A. Record-Keeping Systems. **Archivaria,** Canada**,** 36 (January), 1993. Available at: https://archivaria.ca/index.php/archivaria/article/view/11932.

BEARMAN, D. A.; SOCHATS. Metadata requirements for evidence. Available at: https://www.archimuse.com/papers/nhprc/BACartic.html

BELLOTTO, H. L. **Como fazer análise diplomática e análise tipológica de documento de arquivo**. São Paulo: Arquivo do Estado, 2002.

BELLOTTO, H. L. **Arquivos Permanentes: tratamento documental.** 2 ed. Rio de Janeiro: FGV, 2004.

BELLOTTO, H. L. **Diplomática e tipologia documental em arquivos**. 2 ed. Brasília, 2008.

BELLOTTO, H. L. A Diplomática Como Chave da Teoria Arquivística. **Archeion Online**, Paraiba, v.3, n.2, p.04-13, 2015. Available at: https://periodicos.ufpb.br/ojs/index.php/archeion/article/view/27544#:~:text=A%20Diplom%C3%A1tica%20fornece%20os%20elementos,e%20o%20da%20indivisibilidade%2Fintegridade.&text=Nesse%20sentido%2C%20a%20Diplom%C3%A1tica%20%C3%A9,te%C3%B3ricas%20da%20organiza%C3%A7%C3%A3o%20dos%20arquivos**.**

BENGTSON, J. Preparing for the age of the digital palimpsest. **Journal Library Hi Tech**, United Kingdom, vol. 30, Iss: 3, pp.513–522, 2012. DOI: https://dx.doi.org/10.1108/07378831211266636. Available at: https://www.emerald.com/insight/content/doi/10.1108/07378831211266636/full/html

BLOCH, M. **Apologia da História ou o Oficio do Historiador**. Rio de Janeiro: Jorge Zahar Editor, 1949.

BOGEN, A. C.; DAMPIER, D. A. Knowledge Discovery and Experience Modeling in Computer Forensics Media Analysis. ISICT '04: **Proceedings** of the 2004 international symposium on information and communication technologies. Trinity College Dublin, June 2004, p.140-145, 2004. DOI: https://dl.acm.org/doi/10.5555/1071509.1071537. Available at: https://dl.acm.org/doi/proceedings/10.5555/1071509

BOYLE, E. L. Diplomatics. In: POWELL, M. J. (Ed.). **Medieval studies**: an introduction. 2nd ed. Syracuse, N. Y. Syracuse University Press, 1992. p.82-113

BRASIL**. Lei No. 13.105**, de 16 de março de 2015. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm

BRAGUITTONI, I. Evidência (ou prova?). **Migalhas**. 2006. Available at: https://migalhas.uol.com.br/coluna/gramatigalhas/31108/evidencia--ou-prova

BRUUN, B. M. Jean Mabillon's Middle Ages: On Medievalism, Textual Criticism, and Monastic Ideals. In: Montoya, A.; Romburgh, v, S.; Anrooij, v. W. **Early modern medievalism. The interplay between scholarly reflection and artistic production**. Danvers, MA: Brill, 2010. p. 427-444

BUCKLAND, M. Information as thing. **Journal of the American Society for Information Science**, United States, 42:5, June 1991. 351-360. Available at: https://doi.org/10.1002/(SICI)1097-4571(199106)42:5<351::AID-ASI5>3.0.CO;2-

BYERS, N. **ECfAIR- Email Classification for Archival and Institutional Repositories: A Semi-Supervised Classification Method for Email Collections.** Master's Project Proposal. University of North Carolina at Chapel Hill – UNC. School of Information and Library Science – INLS. 2020.USA. Available at: https://www.npbyers.com/files/ProposalFinal.pdf

CAMARGO, A. M. A. Sobre o valor histórico dos documentos. Arquivo Rio Claro. Rio Claro, SP, n. 1, p. 11-16, 2003. Available at: http://www.arquivoestado.sp.gov.br/site/assets/difusao/curso_usp/AULA_4_Arquivo_Rio_Claro_n01_2003.pdf

CAMARGO, A. M. A. Historiadores e arquivistas: um diálogo possível. **Revista do Instituto Histórico e Geográfico de Sergipe.** N.48, v.1, 2018. Available at: https://seer.ufs.br/index.php/rihgse/article/view/12165

CANADA EVIDENCE ACT. R.S.C. **An Act respecting witnesses and evidence.** 1985. Available at: https://laws-lois.justice.gc.ca/eng/acts/c-5/fulltext.html

CLANCHY, M., T. **From memory to writing record. England 1066-1307.** Singapore: Blackwell Publishing, 2013.

CARRIER, B.; SPAFFORD, E. H. Getting Physical with the Digital Investigation Process**.** United States, **International Journal of Digital Evidence.** v.2, Issue 2, Fall 2003. Available at: https://www.semanticscholar.org/paper/Getting-Physical-with-the-Digital-Investigation-Carrier-Spafford/915b524318e2f0689b586ba7ae89ea39e9b22ce3?p2df

CHARTERS, I. **The evolution of digital forensics**. Civilizing the cyber frontier. 2009, San Francisco, California, USA. Available at: http://www.guerilla-ciso.com/wp-content/uploads/2009/01/the-evolution-of-digital-forensics-ian-charters.pdf

CHOW, K. P.; SHENOI, S. **Advances in digital forensics VI**. CHOW, K. P. and SHENOI, S (Eds.). Sixth IFIP WG 11.9 International Conference on Digital Forensics Hong Kong, China, January 4-6, 2010 Revised Selected Papers. Germany: Springer, 2010. Available at: https://www.springer.com/gp/book/9783642155055

CLOUD SECURITY ALLIANCE. **Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing**. 2013. Available at: https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf

COHASSET A. I. **What's new: Electronic commerce forms: Requirements, issues, and solutions**., Chicago, Il., USA 2001. Available at: https://perma.cc/532N-CYF8

COLLIER, P. A.; SPAUL, B.J. A forensic methodology for countering computer crime. **Artificial Intelligence Review 6,** Netherlands, 203–215, 1992. Available at: https://doi.org/10.1007/BF00150234. Available at: https://link.springer.com/content/pdf/10.1007/BF00150234.pdf

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis** – RDC-Arq. Rio de Janeiro: Arquivo Nacional, 2015. Available at: http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE**). Glossário Documentos Arquivísticos Digitais**. Rio de Janeiro: Arquivo Nacional, 2020. Available at: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pdf

COOK, T. "The Concept of the Archival Fonds in the Post-Custodial Era: Theory, Problems and Solutions". **Archivaria** 35, Canada (January), 1992. Available: https://archivaria.ca/index.php/archivaria/article/view/11882.

COOK, T. Electronic Records, Paper Minds: The Revolution in Information Management and Archives in the Post-Custodial and Post-Modernist Era. **Archives & Manuscripts**, Australia, 22(2), pp. 300-328, 1994. Available at: https://publications.archivists.org.au/index.php/asa/article/view/8433

CORTES-ALONSO, V. Nuestro modelo de análisis documental. **Boletín de ANABAD** (Asociación Española de Archiveros, Bibliotecarios, Museólogos y Documentalistas). Madrid: ANABAD, n.3, p.419-434, 1986. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=802380

DAULBERT V. MERREL DOW PHARMACEUTICALS. **Inc., 509 U.S. 579**. 1993. Available at: https://supreme.justia.com/cases/federal/us/509/579/

DAY, M. The Long-Term Preservation of Web Content. In: **Web Archiving**. (Ed.) MASANÈS, J. Berlin, Ed..Springer, 1st ed, pp. 177-199, 2006. Available at: https://www.researchgate.net/publication/226640969_The_Long-Term_Preservation_of_Web_Content

DELMAS, B. **Arquivos para quê**? Textos escolhidos. São Paulo: Instituto Fernando Henrique Cardoso, 2010.

DIAMOND, E. The archivist as forensic scientist – seeing ourselves in a different way. In: **Archivaria**. Canada, v. 38: 139-154, 1994. Available at: https://archivaria.ca/index.php/archivaria/article/view/12031.

DICIONÁRIO JURÍDICO. **Academia Brasileira de Letras Jurídicas**. (Org.) J.M. Othon Sidou. Rio de Janeiro: Forense Universitária. 3ra edição. 1995.

DIGITAL RECORDS FORENSICS PROJECT**, DRFP** (2008-2011). Available at: http://www.digitalrecordsforensics.org/index.cfm

DOSSE, F. **A História**. São Paulo: Fundação Editora da Unesp (FEU), 2012.

DUCHEIN, M. "Theoretical Principles and Practical Problems of Respect Des fonds; In Archival Science". ***Archivaria***, Canada,16 (January), 64-82, 1983. Available at: https://archivaria.ca/index.php/archivaria/article/view/12648.

DURANTI, L. Diplomatics: New Uses for an Old Science, Part I. **Archivaria,** Canada**,** 28 (January), 7-27, 1989. Available at: https://archivaria.ca/index.php/archivaria/article/view/11567

DURANTI, L. Diplomatics: New Uses for an Old Science, Part II. **Archivaria,** Canada, 29 (January), 4-17, 1989. Available at:https://archivaria.ca/index.php/archivaria/article/view/11605.

DURANTI, L. Diplomatics: New Uses for an Old Science, Part III. **Archivaria,** Canada, 30 (January), 1990. Available at:https://archivaria.ca/index.php/archivaria/article/view/11659.

DURANTI, L. Diplomatics: New Uses for an Old Science, Part IV. **Archivaria,** Canada, 31 (January), 1990. Available at:https://archivaria.ca/index.php/archivaria/article/view/11716.

DURANTI, L. Diplomatics: New Uses for an Old Science, Part V. **Archivaria**, Canada, 32 (January), 1991. Available at:https://archivaria.ca/index.php/archivaria/article/view/11758.

DURANTI, L. Diplomatics: New Uses for an Old Science, Part VI. **Archivaria,** Canada, 33 (January), 1991. Available at:https://archivaria.ca/index.php/archivaria/article/view/11795.

DURANTI, L. Archives as a Place**. Archives & Manuscripts**, *Australia,* 24, 2, 1996. pp. 242-255. Available at: https://www.academia.edu/11346519/Archives_as_a_Place

DURANTI, L. The impact of digital technology on archival science. **Archival Science 1,** Netherlands**,** 39–55, 2001. DOI: https://doi.org/10.1007/BF02435638
Available at: https://link.springer.com/article/10.1007%2FBF02435638

DURANTI, L. From Digital Diplomatics to Digital Records Forensics". **Archivaria***,* Canada, 68 (January), 39-66, 2010. Available at: View of From Digital Diplomatics to Digital Records Forensics (archivaria.ca)

DURANTI, L. Digital Records Forensics: A New Science and Academic Program for Forensic Readiness**. Journal of Digital Forensics, Security and Law**, USA, v. 5: n. 2, Article 4. DOI: https://doi.org/10.15394/jdfsl.2010.1075. Available at: https://commons.erau.edu/cgi/viewcontent.cgi?article=1075&context=jdfsl

DURANTI, L. **Concepts, principles and methods guiding the reliable and accurate creation of digital records that can be preserved**. ARST555. 16 September 2019. 71 Slides. UBC - School of Information.

DURANTI, L. THIBODEAU, K. The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES. **Archival Science**, Netherlands, 6, 13–68, 2006. DOI: https://doi.org/10.1007/s10502-006-9021-7. Available at: https://link.springer.com/article/10.1007%2Fs10502-006-9021-7

DURANTI, L. ENDICOTT-POPOVSKY, B. Digital Records Forensics: A New Science and Academic Program for Forensic Readiness. **The journal of the digital forensics, security and law.,** USA, v. 5: no.2, Article 4. 2010. DOI: https://doi.org/10.15394/jdfsl.2010.1075. Available at: https://commons.erau.edu/jdfsl/vol5/iss2/4/

DURANTI, L. FRANKS, C. P. **The Encyclopedia of Archival Writers**, 1515-2015. United States: The Rowman & Littlefield Publishing Group Inc. 2019

ERLANDSSON, A. **Electronic records management: A literature review.** Paris, France. ICA Studies, 1996.

EVANS, R. J. **Rituals of retribution**. Capital punishment in Germany.1600-1987.USA: Oxford University Press, 1996.

FARNAM S., M., I**. Plato's argument against writing**. Available at: https://fs.blog/2013/02/an-old-argument-against-writing/

FLORES, D.; PRADEBON, D. S.; GRAZIELLA, C. Análise do conhecimento teórico-metodológico da preservação digital sob a ótica da OAIS, SAAI, ISO 14721 e NBR 15472**. Brazilian Journal of Information Science**: Research Trends, Brazil, v., 11, nº 4, Dec. 2017, Available at: http://revistas.marilia.unesp.br/index.php/bjis/article/view/7511

FLORES, D.; LUZ, C. **Chain of custody (CoC) and chain of preservation (CoP): Authenticity in the platforms of management and preservation of records**. 2017. Available at: https://www.academia.edu/34470855/Chain_of_Custody_CoC_and_Chain_of_Preservation_CoP_authenticity_in_the_platforms_of_management_and_preservation_of_records

FLORES, D.; A cadeia de custódia. Relação interdisciplinar: Direito, Arquivologia, Diplomática e CFD. **Webinar. Preservação Digital: o Case do TJDFT na Implementação do RDC-Arq**. 2020. Available at:

https://www.researchgate.net/publication/344228637_A_Cadeia_de_Custodia_e_a_Ciencia_Forense_Digital_-_CFD_para_a_garantia_da_Autenticidade_e_Confiabilidade_dos_Documentos_fontes_de_prova

FRYE V. UNITED STATES. **72 F. Supp. 405** (D.D.C. 1947). Available at: https://law.justia.com/cases/federal/district-courts/FSupp/72/405/2238888/

GALENDE-DÍAZ, J.C.; García-Ruipérez, M. El concepto de documento desde una perspectiva interdisciplinar: de la diplomática a la archivística**. Revista General de Información y Documentación**. Madrid, Spain, v.13, n.2, 7-35, Available at: https://revistas.ucm.es/index.php/RGID/article/view/RGID0303220007A/9914

GARFINKEL, S. L. Digital forensics research: the next 10 years**. Digital investigation**., United Kingdom, v. 7, S64-S73,2010. DOI: https://doi.org/10.1016/j.diin.2010.05.009. Available at: https://www.sciencedirect.com/science/article/pii/S1742287610000368?via%3Dihub

GINZBURG, C. **Relações de força. História, retórica, prova**. São Paulo: Editora Schwarcz, 2002.

GOLDBERG, S. **Culture clash**: law and science in America. New York: New York University Press, 1994.

GROß, H. G. A. **Criminal investigation**. A practical handbook for magistrates, police officers, and lawyers. Printed by G. Ramasawmy Chetty & Co., 1960.

HEAD, C. R. Archives, documents, and proof: Diplomatics, the *ius archivi* and state practice in the seventeenth and early eighteenth centuries. **“Things: Material Cultures of the Long Eighteenth Century”.** University of California-Cambridge University-Huntington Library Interdisciplinary Workshop**,** 2012.

HEDSTROM, M. “Building Record-Keeping Systems: Archivists Are Not Alone on the Wild Frontier”. **Archivaria,** Canada 44 (January), 44-7, 1997. Available at: https://archivaria.ca/index.php/archivaria/article/view/12196.

HEREDIA-HERRERA, A. **Archivística general**. Teoría y práctica. 5ta ed. Sevilla: Diputación Provincial de Sevilla, 1991.

HEREDIA-HERRERA, A. En torno al tipo documental**. Arquivo & Administração**, Rio de Janeiro, v. 6, n. 2, 2007. Available at: http://hdl.handle.net/20.500.11959/brapci/51509.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 27037**.Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 14721:2012.** Space data and information transfer systems -Open Archival Information System (OAIS)- Reference Model.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS PROJECT - **INTERPARES** (1999-2018). Available at:www.interpares.org.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS 2 PROJECT - **INTERPARES 2** (2002-2007). Available at: http://www.interpares.org/ip2/ip2_index.cfm.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS 2 PROJECT – **INTERPARES.** INTERPARES. Appendix 2. **Template for Analysis.** 7 November 2000. Available at: http://www.interpares.org/display_file.cfm?doc=ip1_template_for_analysis.pdf

IRON MOUNTAIN INCORPORATED **(NYSE: IRM)**: https://www.ironmountain.com.br/about-us.

IRONS, A. Computer forensics and records management – compatible disciplines. **Records Management Journal**, United States, v. 16 Issue: 2, pp.102-112, 2006. DOI: http://dx.doi.org/10.1108/09565690610677463. Available at: https://www.emerald.com/insight/content/doi/10.1108/09565690610677463/full/html

JENKINSON, J. Archives and the science and study of diplomatic (1957). **Selected writings of Sir Hilary Jenkinson**. Great Britain: Alan Sutton Publishing Limited, 1980.

JOHN, J. J. Latin Paleography. In: POWELL, M. J. (Ed.). **Medieval studies**: an introduction. 2nd ed. Syracuse, N. Y. Syracuse University Press, 1992. p.1-81.

JOHNSON, A. **The historian and historical evidence**. United States of America: Kennikat Press, Inc. 1965.

KEBANDE, V. R.; KARIE, N. M.; CHOO, R. K.; ALAWADI, S. Digital forensic readiness intelligence crime repository. **Security and Privacy**., United Kingdom**,** E1,51, 2021. DOI: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.151 Available at: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.151

KIRSCHENBAUM, M. G. **Mechanisms**. New media and the forensic imagination. London, England: The MIT Press, 2008.

KUMHO TIRE CO. V. CARMICHAEL**. 526 U.S. 137**. 1999. Available at: https://supreme.justia.com/cases/federal/us/526/137/

LAAKSO, M.; MATTHIAS, L.; JAHN, N**. Open is not forever: a study of vanished open access journals. ArXiv**, USA, v1, pp. 1-15, 2021. DOI: 10.1002/asi.24460. Available at: Open is not forever: A study of vanished open access journals (arxiv.org)

LANGLOIS C. V.; SEIGNOBOS, C. **Introduction to the Study of History.** Produced by Chuck Greif and the Online Distributed, 2009.

LAWLESS, C. **Forensic Science: a sociological introduction**. Routledge, 2016.

LEE, C. A. Digital Curation as Communication Mediation. In: **Handbook of Technical Communication. (**Eds.) Alexander Mehler and Laurent Romary in cooperation with Dafydd Gibbon. De Gruyter Mouton. Germany, 2012, pp.508-530. DOI: https://www.degruyter.com/document/doi/10.1515/9783110224948.507/html

LEE, C. A.; WOODS, K.; KIRSCHENBAUM, M.; CHASSANOFF, A**. From Bitstreams to Heritage**: Putting Digital Forensics into Practice in Collecting Institutions. A Product of the BitCurator Project. September 30, 2013. Available at: https://drum.lib.umd.edu/handle/1903/14736

LEMIEUX, V. L., et al: Blockchain Technology and Recordkeeping. Project Underwritten by: **ARMA Canada Region**. May 30, 2019. Available at: http://armaedfoundation.org/research-program_menu/research-reports/

MABILLON, J. **De re diplomatica libri VI.** In quibus quidquid ad veterum instrumentum antiquitatem, materiam, scripturam & stilum; quidquid ad sigilla, monogrammata, subscriptiones ac notas chronologicas; quidquid inde ad antiquariam, historicam, forensemque disciplinam pertinet, explicatur & illustratur: accedunt commentarius de antiquis regum Francorum palatiis, veterum scripturarum varia specimina, tabulis LX comprehensa, nova ducentorum, & amplius, monumentorum collection*".* 1681.

MACNEIL, H. **Trusting Records:** Legal, Historical and Diplomatic Perspectives. © 2000 Springer Science+Business Media Dordrecht. 2000

MACNEIL, H. Providing Grounds for Trust II: The Findings of the Authenticity Task Force of InterPARES. ***Archivaria***, Canada, *54*, 24-58, 2002. Available at: https://archivaria.ca/index.php/archivaria/article/view/12854

MCKEMMISH, R. What is forensics computing? **Trend Issues Crime Crim Justice**, Australia, n, 118, 1999. Available at: https://www.aic.gov.au/sites/default/files/2020-05/tandi118.pdf

MCKEMMISH, S. Introducing Archives and Archival Programs. In: **Keeping Archives**., Judith Ellis (ed.), 2nd ed. (Melbourne, Aus.:D. W. Thorpe, 1993)

MEEHAN, J. “Towards an Archival Concept of Evidence”. **Archivaria,** Canada**,** 61 (September), 127-46, 2006. Available at: https://archivaria.ca/index.php/archivaria/article/view/12538.

MERLINONE. 2020. Available at: https://merlinone.com/about-us/

MERTON, R. K. **On the shoulders of giants**. New York: The University of Chicago Press, 1993.

MITTERMAIER, C. J. A. **Tratado da prova em matéria criminal, ou exposição comparada dos princípios da prova em matéria criminal, etc., de suas aplicações diversas na Alemanha, França, Inglaterra, etc**. Rio de Janeiro, A. A. da Cruz Coutinho, 1871. Available at: http://www.dominiopublico.gov.br/download/texto/bd000146.pdf

MOCAS, S. Building theoretical underpinnings for digital forensics research. **Digital Investigation**, USA, v.1, i.1, pp.61-68, 2004. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1742287603000057?via%3Dihub

MONTOYA-MOGOLLÓN, J. B. **A emergência de uma “adequada” produção e organização de documentos arquivísticos digitais em organizações.** 2017. 123 f. Dissertação (Mestrado em Ciência da Informação) - Faculdade de Filosofia e Ciências. Universidade Estadual Paulista, Marília, 2017.

MONTOYA-MOGOLLÓN, J. B.; TROITIÑO, R. S. M. The diplomatic and digital forensic science in born-digital records: the quest for authenticity. **Journal of Integrated OMICS**., Portugal, v. 8, n. 1, 2018. DOI: 10.5584/jiomics.v8i1.219 Available at: https://www.jiomics.com/index.php/jiomics/article/view/132

MONTOYA-MOGOLLÓN, J. B.; TROITIÑO, R. S. M. Diplomática Forense: revisão histórica para a abordagem do documento nato-digital de arquivo. **Investigación Bibliotecológica: archivonomía, bibliotecología e información**, México, [S.l.], v. 33, n. 78, p. 47-62, ene. 2019. ISSN 2448-8321. DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2019.78.57928 Available at:http://rev-ib.unam.mx/ib/index.php/ib/article/view/57928/51966.

MUMMA, C. The archivist detective – digital forensics for archivists. AuthentiCity. **The City of Vancouver Archives Blog**. December 15, 2011. Available at: https://www.vancouverarchives.ca/2011/12/15/the-archivist-detective-digital-forensics-for-archivists/

NATIONAL COUNCIL FOR SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENT -**CNPq.** Brasília**,** 2018. Available at: https://www.gov.br/cnpq/pt-br

ONLINE ETYMOLOGY DICTIONARY. Available at: https://www.etymonline.com/word/meta-#etymonline_v_14705

PALMER, G. A Road Map for Digital Forensic Research. In: From the **proceedings of The Digital Forensic Research Conference DFRWS** 2001, pp. 1-42, USA, Utica, NY (Aug 7th - 8th) Available at:https://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

PAZIN, M. C. C. **Obrigação, controle e Memória. Aspectos legais, técnicos e culturais da produção documental de organizações privadas.** Tese de doutorado do Programa de Pós-Graduação em História Social, do Departamento de História da Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo. 2011. Available at: https://teses.usp.br/teses/disponiveis/8/8138/tde-22082012-090854/publico/2011_MarciaCristinaDeCarvalhoPazinVitoriano_VRev.pdf

PEARCE-MOSES, R. **A glossary of archival and records terminology**. USA, Chicago: The Society of American Archivists. 2005. ISBN 1-931666-14-8. Available at: https://www2.archivists.org/glossary

PIQUERAS, M. Conceptos, métodos, técnicas y fuentes de la diplomática. In: **Introducción a la paleografía y la diplomática en general**.

RIESCO-TERRERO, A. (ed.). Madrid-España: Editorial Síntesis, 1999, p.191-207.

POLLITT, M. A history of digital forensics. CHOW, K. P.; SHENOI, S. **Advances in digital forensics VI**. CHOW, K. P.; SHENOI, S (Eds.). Sixth IFIP WG 11.9 International Conference on Digital Forensics Hong Kong, China, January 4-6, 2010 Revised Selected Papers. Germany: Springer, 2010. DOI: https://doi.org/10.1007/978-3-642-15506-2_1. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-642-15506-2_1.pdf

PREMIS. **Preservation Metadata. Maintenance Activity**. 2020. Available at: http://www.loc.gov/standards/premis/

R. V. MOHAN. **Supreme Court Judgments**. 1994. Ontario. Available at: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1131/index.do

RESIDE, D. “Not day but today”: a look at Jonathan Larson’s Word Files. **New York Public Library**, USA, 2011. Available at: https://www.nypl.org/blog/2011/04/22/no-day-today-look-jonathan-larsons-word-files

RLG-OCLC. Trusted Digital Repositories: Attributes and Responsibilities. Report. **Mountain View**, Canada, 2002. Available at: https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

ROBERTS, D. Defining electronic records, documents and data. **Archives and Manuscripts,** Australia**,** v. 22, n. 1, pp. 14-26, 1994. Available at: http://publications.archivists.org.au

RODRIGUES, A. C**. Diplomática contemporânea como fundamento metodológico da identificação de tipologia documental em arquivos**. 2008. 258 f. Tese (Doutorado em História) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, 2008. Available at: https://teses.usp.br/teses/disponiveis/8/8138/tde-27112008-151058/publico/TESE_ANA_CELIA_RODRIGUES.pdf

ROGERS, C. Digital Records Forensics: Integrating Archival Science into a General Model of the Digital Forensics Process. In: Clive Blackwell (PC Chair). Cyberpatterns 2013. **Proceedings of the Second International Workshop on Cyberpatterns**: Unifying Design Patterns with Security, Attack, and Forensic Patterns. England, 8-9 July 2013.

ROGERS, C. Diplomatics of born-digital documents – considering documentary form in a digital environment**. Records Management Journal**, United States, v, 25 Iss. 1 pp. 6 – 20, 2015. DOI: http://dx.doi.org/10.1108/RMJ-03-2014-0021 Available at: https://www.emerald.com/insight/content/doi/10.1108/RMJ-03-2014-0021/full/html

ROGERS, C. A literature review of authenticity of records in digital systems. From “machine-readable” to records in the cloud. **Revista Acervo**, Brazil, v.29, n.2, pp.16-44, Jul-Dic. 2016. Available at: http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/715/742

ROGERS, C. **Characteristics of digital records: diplomatic and technical models.** Topics in Archival Automation Digital Records Forensics course. ARST 556H. January 30, 2019. 71 slides. UBC - School of Information.

ROGERS, C. **Digital forensics – intro and history**. Topics in Archival Automation Digital Records Forensics course. ARST 556H. February 06, 2019. 63 slides. UBC - School of Information.

ROGERS, C. **Digital forensics – Theory and Models**. Topics in Archival Automation Digital Records Forensics course. ARST 556H. February 13, 2019. 49 slides. UBC - School of Information

ROGERS, C. **Evidence and admissibility.** 2019. Topics in Archival Automation Digital Records Forensics course. ARST 556H. February 27, 2019. 64 slides. UBC - School of Information.

ROMERO-TALLAFIGO, M. **Ayer y hoy de la diplomática**, ciencia de la autenticidad de los documentos. Carmona: S&C ediciones. Universidad Internacional Menéndez Pelayo, 1994.

ROMERO-TALLAFIGO, M. Nueva diplomática, nueva metodología para la Historia del Documento, **Signo. Revista de Historia de la Cultura Escrita**, Spain, 14, pp.139-183, 2004. Universidad de Alcalá. Available at: https://core.ac.uk/reader/58907982

RONDINELLI, C. R. **O conceito de documento arquivístico frente à realidade digital**: uma revisitação necessária**.** 2011. 270f. Tese (Doutorado em Ciência da Informação) – Universidade Federal Fluminense. Programa de Pós-Graduação em Ciência da Informação, Instituto de Arte e Comunicação Social, Instituto Brasileiro em Ciência e Tecnologia, Niterói, 2011.

SANTIAGO, C. Você sabe o que significa não repúdio? **Solutiresponde**, Brazil, 2018. Available at: In: https://solutiresponde.com.br/voce-sabe-o-que-significa-nao-repudio-descubra-neste-post/

SHEETZ, M. **Computer forensics: an essential guide for accountants, lawyers, and managers**. USA: John Wiley & Sons, Inc., 2007.

TSCHAN, R. A Comparison of Jenkinson and Schellenberg on Appraisal. **The American Archivist**, United States, 65, no. 2 ,176-95, 2002. DOI: https://doi.org/10.17723/aarc.65.2.920w65g3217706l1 Available at: https://meridian.allenpress.com/american-archivist/issue/65/2

SILVA, G. A. A. **A perícia forense no Brasil**. 125f. São Paulo. Dissertação (Mestrado em Engenharia Elétrica). Universidade de São Paulo, Brazil – Escola Politécnica, 2010. Available at: https://teses.usp.br/teses/disponiveis/3/3142/tde-11082010-152328/pt-br.php

SMEDT, C. D. Bollandistas. Trad. de P. Royo. **Enciclopedia Católica Online** (ecwiki), 2008. Available at: http://ec.aciprensa.com/wiki/Bollandistas.

SCHNEIER, B. Cryptanalysis of MD5 and SHA: Time for a New Standard. Crypto researchers report weaknesses in common hash functions. **Computerworld**. The voice of business technology. 2004. Available at: https://web.archive.org/web/20141021150622/http://www.computerworld.com/article/2566208/security0/opinion--cryptanalysis-of-md5-and-sha--time-for-a-new-standard.html

STARN, R. Truths in the archives. **Common Knowledge**, United States, vol.8, no.2, p.387-401, 2002. Project MUSE. Available at: https://muse.jhu.edu/article/7608

SWORD AND SCALE 66. Mike Boudet. United States: 11 January, 2015. **Podcast**. Available at: https://www.swordandscale.com/sword-and-scale-episode-34

TENNIS, J., T. Metadata in the Chain of Preservation Model: Draft Metadata Specification Model. **InterPARES 2 Project.,** Canada**,** February 2008. Available at: http://www.interpares.org/display_file.cfm?doc=ip2_cop_metadata_model_v2.pdf

THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS - CCSDS. **Reference model for an open archival information system (OAIS).** Recommendation for Space Data System Practices. USA, Washington, D.C.: 2012. Available at: https://public.ccsds.org/pubs/650x0m2.pdf

THE I INTERNATIONAL CAPARICA CONFERENCE IN TRANSLATIONAL FORENSICS. **FORENSICS**., Portugal, Lisbon, 2017. Available at: http://books.bioscopegroup.org/books/awgk/#p=2

THE PRESERVATION OF DIGITAL RECORDS COURSE. School of Library and Information Studies., Canada, The University of British Columbia – **UBC.** Available at: https://slais.ubc.ca/arst-555/. 2019.

THIBODEAU, K. Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years. In: **Conference proceedings documentation abstracts**, Inc. Institutes for information science Washington, D.C. Council on Library and Information Resources Washington, D.C. April 24-25, 2002. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.89.3273

TOGNOLI, B. N. **A construção teórica da diplomática**: em busca da sistematização de seus marcos teóricos como subsídio aos estudos arquivísticos. 1 ed. São Paulo: Cultura Acadêmica. 2014.

TOGNOLI, B. N.; RODRIGUES, A. C. An Analysis of the theoretical and practical application of Diplomatics to archival description in Knowledge Organization. In: RIBEIRO, F.; CERVEIRA, M. E. (Eds.). International Society for Knowledge Organization (ISKO). **Advances in Knowledge Organization**, Vol. 16, 2018. p. 43-51. DOI: https://doi.org/10.5771/9783956504211 Available at: https://www.nomos-elibrary.de/10.5771/9783956504211/challenges-and-opportunities-for-knowledge-organization-in-the-digital-age?hitid=0&search-click

TROITIÑO, R.S.M**. O Juízo dos Órfãos de São Paulo: Caracterização de Tipos Documentais (séc. XVI-XX).** Tese de doutorado do Programa de Pós-Graduação em História Social, do Departamento de História da Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo. 2010. Available at: https://www.teses.usp.br/teses/disponiveis/8/8138/tde-27042010-103207/publico/SONIA_MARIA_TROITINO_RODRIGUEZ.pdf

TROITIÑO, R.S.M. A tipologia documental como instrumento para a seriação de documentos. In: Marta Ligia Pomim Valentim (org.) **Estudos avançados em Arquivologia**, Marília, SP, Brazil, Cultura Acadêmica Editora, 2012 p. 242-258. Available at: https://www.marilia.unesp.br/Home/Publicacoes/estudos_avancados_arquivologia.pdf

UNIVERSITY OF BRITISH COLUMBIA – UBC.POLICY MATTERS. 11TH ANNUAL INTERNATIONAL SEMINARS AND SYMPOSIUM (ACA@UBC). Available at: http://acasymposium2019.sites.olt.ubc.ca/.

UNIVERSITY OF MARYLAND – UMD. MARYLAND INSTITUTE FOR TECHNOLOGY IN THE HUMANITIES. THE UNIVERSITY OF MARYLAND, MITH. Available at: https://mith.umd.edu/.

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL - UNC SCHOOL OF INFORMATION & LIBRARY SCIENCE - SILS. Available at: https://www.unc.edu/school/information-library-science/.

VAN GELDER, L. On the Eve of a New Life, an Untimely Death. **The New York Times**., USA, 1996. Available at: https://www.nytimes.com/1996/12/13/nyregion/on-the-eve-of-a-new-life-an-untimely-death.html

WAI-ARIA. **Accessible Rich Internet Applications** (WAI-ARIA) 1.1. Joanmarie Diggs; Shane McCarron; Michael Cooper; Richard Schwerdtfeger; James Craig. W3C. 2017. W3C Recommendation. Available at: https://www.w3.org/TR/wai-aria-1.1/

WHITCOMB, C. M. An historical perspective of digital evidence: a forensic scientist's view. **International Journal of Digital Evidence**, USA, v, 1, Issue 1, Spring 2002. Available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

WIKIPEDIA. **The free encyclopedia**. Available at: https://en.wikipedia.org/wiki/Main_Page

WILLIAMS, C. D. Diplomatic Attitudes: From Mabillon to Metadata. **Journal of the Society of Archivists**, United Kingdom, 26:1, 1-24, 2007. DOI: https://www.tandfonline.com/doi/full/10.1080/00039810500047417 Available at: https://www.tandfonline.com/doi/pdf/10.1080/00039810500047417?needAccess=true

WORDPANDIT. **Meta Root Word**. Learning Inc. Available at: https://wordpandit.com/meta-root-word/

YEO, G. Concepts of Record (1): Evidence, Information, and Persistent Representations. **The American Archivist**, United States, v, 70, No. 2 (Fall - Winter), pp. 315-343, 2007. Available at: https://www.jstor.org/stable/40294573?seq=3&cid=pdf-reference#references_tab_contents

YEO, G. Concepts of Record (2): Prototypes and Boundary Objects. **The American Archivist**, United States, v, 71, No. 1 (Spring - Summer), pp. 315-343, 2008. Available at: https://www.jstor.org/stable/40294496?seq=1#metadata_info_tab_contents

ZATYKO, K. **Commentary: Defining digital forensics**. In: Forensic Magazine, (Feb/March), pp. 1-5, 2007.