

RBDP

Revista Brasileira de
Preservação Digital

RBDP

Brazilian Journal of
Digital Preservation

TRANSCRIÇÃO DA PALESTRA NA LIVE DO IBICT¹ “Forense Digital e a autenticidade dos documentos arquivísticos digitais”

Construindo pontes² Forense digital e ciência arquivística

Corine Rogers - University of British Columbia

Resumo da apresentação

A ideia principal é abordar como funcionam os processos da perícia digital para fins de preservação digital. A professora falará sobre os propósitos de preservação digital, o estabelecimento da confiabilidade nos arquivos, a relação da forense digital com a arquivística e como algumas ferramentas forenses têm sido aplicadas e adaptadas para a preservação de arquivos digitais.

Palavras-chave: Forense digital. Ciência Arquivística. Preservação digital.

Building bridges digital Forensics & Archival Science

1

Abstract

The main idea is to address how digital forensics processes work for digital preservation purposes. The professor will talk about the purposes of digital preservation, the establishment of trustworthiness in archives, the relationship of digital forensics to archival forensics, and how some forensic tools have been applied and adapted for the preservation of digital archives

Keywords: Digital forensics. Archival Science. Digital preservation.

Apresentado em: 04/10/2021

Publicado em: 08/10/2021



¹ Colaboração na transcrição realizada por Gildenir Carolino Santos (UNICAMP) e Miguel Angel Márdero Arellano (IBICT) – Agradecimentos pela revisão do texto por: Moisés Rockembach (UFRGS) e João Guilherme Nogueira Machado (Fiocruz).

² Apresentação disponível no Canal YouTube do IBICT: <https://youtu.be/WHj54GqBle8>

Slide 2

O objetivo desta palestra é apresentar a conexão entre a forense digital e a teoria arquivística e falar um pouco sobre o que elas têm em comum e o que não têm em comum e como podem se complementar.

Portanto, começarei falando brevemente sobre fluxos de trabalho porque, é claro, todo o trabalho que fazemos é baseado em fluxos de trabalho documentados para procedimentos. Sobre a Teoria do Arquivo, como o InterPARES usou a Diplomática para criar a Teoria da Diplomática Arquivística, do documento de arquivo diplomático e digital e como isso se relaciona com a Teoria forense digital e algumas das direções que as pessoas estão tomando.

Slide 3

Esses são fluxos de trabalho, o primeiro a ser avaliado pela identificação de aquisição e admissão do mundo forense digital, Michael Pollitt é um autor prolífico e especialista em forense digital e ele escreveu isso em 1995, quando a forense digital veio à tona e sendo usada em processos judiciais, é claro que a análise forense digital tem como objetivo inicial ajudar em processos criminais. E esse era um fluxo de trabalho, pois eles estavam desenvolvendo modelos para a prática forense digital. O próximo vem da primeira conferência sobre digital forensics research Workshop em 2001, onde eles identificaram o modelo que incluiu a identificação de preservação de conteúdo dessa coleção, de conteúdo de exame de evidência material e análise e apresentação levando a que, em última instância, se esperasse uma decisão em tribunal. Você pode ver as semelhanças entre esses dois fluxos de trabalho e o fluxo de trabalho de arquivamento. O próximo fluxo de trabalho é um fluxo de trabalho de arquivo genérico básico de avaliação e aquisição, arranjo e descrição, retenção e preservação e apresentação ou acesso, portanto, é um fluxo de trabalho muito genérico e adicionei aqui o fluxo de trabalho de arquivamento de Archivemática para preservação que inclui ingestão ou começa com a transferência de conteúdo, verificação de conteúdo, identificando formas que caracterizam extração de conteúdo de pacote de metadados técnicos ,para preservação descrevendo esse conteúdo., normalizar formatos de arquivo em formatos de preservação, quando apropriado, organizando o conteúdo e, em seguida, armazenando o conteúdo em armazenamento de preservação digital e também disponibilizando-o conforme apropriado para acesso público.

Portanto, podemos ver que a própria ciência forense digital é um campo interdisciplinar. Ele se estende a arquivos e gestão de documentos , e isso foi observado por vários autores. O último ponto é que a prática de arquivamento digital se baseia em ferramentas e conhecimento forense digital e vemos que em ferramentas como a Archivemática, que incorporou algumas das ferramentas forenses digitais, é claro que a forense digital está sempre olhando para frente, olhando para frente, pois a atividade criminosa está sempre procurando explorar novos aspectos da tecnologia e digital. E a perícia está sempre tentando encontrar as ferramentas que lhes permitirão descobrir essa atividade criminosa. Enquanto o trabalho de arquivo é mais retrospectivo no uso de ferramentas forenses digitais, porque normalmente trabalhamos com materiais mais antigos. Portanto, não estamos na vanguarda da tecnologia. Na verdade, estamos olhando para algumas das tecnologias antigas e descobrindo como acessar essa tecnologia antiga com ferramentas forenses digitais.

Slide 4

Portanto, há objetivos e princípios sobrepostos tanto para o trabalho forense digital quanto para o trabalho de arquivamento digital. A perícia digital se preocupa principalmente em identificar os objetos digitais e os traços ou rastros digitais desses objetos que podem servir como evidência de atividade criminosa e analisar esses objetos e aqueles vestígios de sua capacidade probatória. Então, eles estão procurando por atribuição a proveniência dos traços ou sua identidade e, então, é claro, mantendo sua integridade e verificabilidade ao longo do tempo para que possam servir como prova.

O arquivista digital também se preocupa em identificar objetos e vestígios digitais e, especificamente, aqueles que foram criados como registros de transações e ações no curso dos negócios, os fatos os eventos e avaliar sua confiabilidade, sua autenticidade e sua precisão, a fim de garantir uma memória confiável e responsabilidade histórica. E então a pergunta que fazemos é : podemos harmonizar os conceitos de confiabilidade dos registros digitais? Vamos focar no foco centralizado de registro e nos artefatos ou traços digitais que são o foco forense digital, isso é mais informação do que um foco no dado.

Slide 5

Portanto, há mudanças. Existem desafios comuns entre o trabalho forense digital e a prática de arquivamento digital e estes incluem a diversidade de conteúdo a diversidade de material digital que é apresentado a nós como arquivistas como especialistas em forense digital, o volume de material e a complexidade desse material, identificando-o e localizando-o em mídia digital e cada vez mais na nuvem. A versatilidade e proliferação das ferramentas e técnicas para criar o material e também para capturar, encontrar e capturar esse material após o fato, as considerações de longo prazo e do ciclo de vida para preservação. Então, como preservamos o conteúdo para que possa ser compreensível no futuro e os riscos à segurança e privacidade e aos direitos digitais e direitos individuais. Como podemos identificá-los? Informações pessoais e certifique-se de que estão protegidos e não estão acessíveis a pessoas que não deveriam ter acesso a eles.

Slide 6

A prática forense digital e arquivística também compartilham perspectivas teóricas. Desafios tão comuns, mas também teoria comum e esses se concentram em estabelecer autoria e identidade, garantindo integridade e rastreando o conteúdo de alterações ao longo do tempo. Portanto, integridade estabelece e verifica a autenticidade, a responsabilidade relutante e o contexto, apresentando e fornecendo acesso ao conteúdo. Portanto, temos a teoria arquivística que aborda cada um desses itens e também existem conceitos e teorias forenses digitais que abordam esses diferentes itens.

Slide 7

Independentemente da disciplina, se estamos olhando para forense digital ou ciência arquivística, acreditamos que os registros digitais eram artefatos ou vestígios. Nós os chamamos de coisas diferentes dependendo da disciplina, mas eles se relacionam com eventos passados. É por isso que os registros são criados. Portanto, independentemente de como eles foram criados e como são preservados existe uma relação entre o objeto digital e algum evento passado e sua capacidade para servir de evidência não vem de nenhuma natureza intrínseca ou valor do próprio objeto, então sabemos disso pela arquivística. É a relação do documento com o registro do objeto artefato com o evento que lhe confere essa capacidade probatória e a capacidade de servir como evidência do fato de que o evento aconteceu. Portanto, para entender esses vestígios de artefatos de registros, temos que estabelecer sua identidade e descrevê-la e comprová-la e estabelecer as relações entre o registro e o evento.

Slide 8

Então a mentalidade arquivística, a história dos arquivos é traçada aos antigos princípios jurídicos e administrativos que são expressos no Código Justiniano coisas como autoridade ou antiguidade, em vez de autoridade que o depósito público garante a confiabilidade e a cadeia de custódia, uma constante preserva a autenticidade da cadeia de custódia para os documentos. O arquivista então pergunta de um registro não o que é esse registro? O quê, ou melhor, perguntou? O que é esse

registro, e não sobre o que é esse registro, então não estamos muito preocupados com o conteúdo do documento, o assunto do documento, mas sim com os formulários e a estrutura do documento. Portanto, a nossa função profissional de arquivista é esclarecer esse significado do documento. Portanto, não estamos preocupados principalmente com informações ou narrativas, mas com os documentos estruturados quanto forma suas relações semânticas e sintáticas, e isso é muito parecido com o especialista forense digital também que não está interessado na narrativa por trás do rastreamento no computador, mas como esse rastreamento se vincula a alguma atividade tipicamente de intenção criminosa.

Slide 9

Temos os princípios arquivísticos fundamentais que baseamos nosso trabalho no princípio da proveniência a ideia de que os documentos de um criador devem ser mantidos juntos e não separados, do princípio da ordem original de que os documentos devem ser mantidos e preservados e descritos e apresentados na ordem em que o criador os criou e usou e no princípio do vínculo arquivístico, essa ideia de que os documentos estão vinculados uns aos outros pela ordem em que são gerados na apresentação de uma determinada atividade, quer estejam colocando essa atividade em movimento ou provando que essa atividade ocorreu.

Slide 10

O objeto da teoria arquivística é o registro e suas agregações são conjuntos de documentos e definimos um registro como um documento com o que queremos dizer informações registradas, e eu sei que essa ideia de registro não envolve países e sistema jurídico, portanto, talvez seja um documento, mas uma informação registrada que é criada. Ou seja, é feito ou recebido no decorrer de uma seleção uma atividade e, em seguida, toque em separar para ação posterior ou referência e a partir desta definição podemos supor que um registro surge no contexto de alguma ação como um meio ou um subproduto dessa ação e que um registro é criado por e para um ou mais agentes, e esses agentes podem ser agentes humanos ou agentes de máquina, pois estamos falando de registros digitais e que as informações neste registro lá pois se destina a ser transmitido de um agente para outro agente.

Também podemos inferir que mais de um registro pode ser criado no contexto dessa ação. Assim, a criação desse vínculo arquivístico entre os registros e os registros criados no contexto de uma ação estão relacionados por meio de seu papel na execução de documentar aquele plano, de modo que os dois se relacionam com os vínculos entre as relações.

Slide 11

As qualidades dos documentos, as qualidades dos arquivos criados no decorrer da atividade prática por organizações são imparcialidade e, por isso, este é um termo muito mal compreendido nos dias de hoje. Isso não significa que haja imparcialidade do próprio criador do documento, mas que os documentos, por serem criados no contexto no curso de uma atividade prática, são imparciais em relação a isso, essa atividade o fato de que eles estão sendo criados para executar uma ação ou documento em ação. Eles também são autênticos em relação a essa documentação. Eles se acumulam naturalmente ao longo do curso do negócio, executando suas funções. Eles estão inter-relacionados porque ocorrem de forma sequencial documentando ou pondo em movimento essa ação e podemos inferir disso que todos eles são tão únicos e, é claro, imparcialidade, autenticidade, naturalidade e inter-relação foram propostas por Hillary Jenkinson em seu manual de administração de arquivos, falando especificamente sobre o Public Records Office no Reino Unido. Então, se pensarmos nisso nesses termos, podemos entender sua intenção e, em seguida, Terry Eastwood reuniu-os e assumiu sua exclusividade deles.

Slide 12

Assim, o objeto da diplomática é um pouco diferente do objeto da arquivística, o objeto de arte da arquivística sendo os conjuntos de documentos, fundos; ou agregação de arquivamento, o objeto da diplomática é o documento único e entende o documento como um sistema conceitual. Portanto, o conteúdo da criação de documentos neste sistema é manifesto em seus elementos formais. Assim, a forma física parece o que são os elementos formais e onde eles são colocados no documento e a forma intelectual para que os elementos da forma intelectual articulem a ação e identifiquem as pessoas envolvidas no registro no documento e esses elementos de forma possam ser examinados e analisados separadamente do conteúdo. Portanto, isso remete à ideia de que não estamos olhando para a narrativa do documento, mas sim para os elementos formais, portanto, o documento é concebido como um sistema conceitual desses elementos internos e externos que consiste no ato ou atos que dão origem ao registro das pessoas envolvidas em sua criação e execução os procedimentos de criação e os elementos de forma documental.

Slide 13

InterPARES começou na década de 1990. Esta foi a pesquisa de Luciana Duranti a qual ela começou logo depois de chegar ao Canadá e continua até hoje o projeto de pesquisa totalmente financiado mais antigo no Canadá, e ela está pensando em incorporar a teoria diplomática para a Ciência Arquivística (dos arquivos) e trazendo isso especificamente para o reino digital a teoria arquivística e diplomática desenvolvida ao longo dos séculos para os registros de papel e pergaminho, toda a Fundação de leis que regem a admissibilidade de evidências documentais foi testada por meio de sua pesquisa no ambiente digital, a fim de determinar e avaliar a autenticidade e os requisitos para a criação e preservação e gestão de conteúdo digital, para que este projeto tenha como base a hipótese de que todos os documentos podem ser analisados, compreendidos e avaliados em termos de um sistema de elementos formais e que as circunstâncias de sua criação e status de transmissão independentemente da tecnologia por trás de sua criação.

Então, tomando a definição típica diplomática de compreender documentos, analisá-los de acordo com elementos formais e trazê-los de sua fundação original para o mundo digital. Portanto, a tecnologia digital, é claro, separou o conteúdo e a estrutura da forma, portanto, não podemos mais determinar a autenticidade do próprio objeto no próprio documento, porque esse objeto é composto e permanentemente novo a cada vez que ele é revisado conforme apresentado na tela. Portanto, temos que fazer inferências de autenticidade a partir do ambiente.

SLIDE 14

Os resultados dos InterPARES 1 e 2 foram requisitos de referência para a criação de documentos autênticos. Isso ocorre em qualquer contexto e em qualquer meio, mas com foco específico nos requisitos de linha de base digital que dão suporte à produção de cópias autênticas. Portanto, olhando tanto para a criação de documentos quanto para a preservação e produção de cópias desses documentos. O modelo da cadeia de preservação mapeou o processo desde a pré-criação, olhando para o desenvolvimento de um sistema de registro, passando pela criação de registros, o gerenciamento desses registros e a preservação ao longo do tempo. No último projeto InterPARES Trust desenvolvemos a apresentação como um serviço de confiança, que é um requisito funcional executável para preservação digital, isso é baseado no modelo OAIS de preservação digital, mas também adiciona os elementos de habilidades de execução para que você possa realmente testar se suas estratégias de preservação são bem-sucedidas. Existem também ontologias para registro digital para confiabilidade e modelos para a realização de análises contextuais e diplomáticas de material digital.

SLIDE 15

Este é o modelo de um documento digital e você pode ver os atributos necessários de conteúdo estável e forma fixa. Os agentes da pessoa são as ligações entre os registros das ações e o contexto dos vários contextos. Então nós temos que os atributos podem ser divididos em componentes intelectuais e componentes digitais e os componentes intelectuais compreendem pedaços de metadados que vão estabelecer a identidade do documento e provar sua integridade ao longo do ~~sobre~~ tempo e também compreender o contexto do registro e os componentes digitais incluem componentes físicos e lógicos de como o documento é realmente capturado e apresentado.

SLIDE 16

Esta é a estrutura de confiança e esta é a base de qualquer análise de registro para estabelecer confiabilidade e precisão comprovadas de autenticidade. Portanto, propomos que a confiabilidade do documento consiste na confiabilidade da autenticidade e a precisão e a autenticidade dependem do estabelecimento da identidade do documento. Portanto, a identidade única desse objeto e comprovando sua integridade ao longo do tempo e ela também inclui a comprovação da confiabilidade do sistema em certas situações e, relacionada à autenticidade, está a autenticação, que é uma declaração de autenticidade em um determinado momento. Portanto, autenticidade é uma qualidade de registros que precisa ser protegida ao longo do tempo e avaliada em diferentes pontos no tempo, em oposição à confiabilidade, que é a qualidade do valor da responsabilidade que você pode atribuir a um documento, com base em sua criação na integridade de sua forma e elementos formais e os controles sobre a criação e a confiança do autor do documento; a exatidão refere-se à precisão do conteúdo desses registros, portanto, controles sobre o conteúdo e controles sobre a transmissão. Portanto, todas essas coisas precisam ser avaliadas no ambiente digital para estabelecer a confiabilidade do conteúdo.

SLIDE 17

Como isso se relaciona com a perícia digital? Podemos ver nas diretrizes de melhores práticas, por exemplo, as diretrizes para policiais do Reino Unido que afirmam basicamente que a perícia digital não deve alterar o conteúdo, que pessoas competentes só devem ter acesso a esse conteúdo e tudo o que é feito para que o conteúdo seja totalmente documentado e a pessoa encarregada da investigação é a responsável pelo resultado final.

Isso também é exibido em vários padrões de padrões, e ambos são baseados e testados em tribunal em princípios científicos ou medições de confiabilidade. Portanto, coisas como repetibilidade, se você conduzir um experimento no conteúdo, podem ser repetidos e obter o mesmo resultado? É objetivo, então objetividade verificável você verifica a validade de seus próprios resultados e transparência e estes foram confirmados e testados na jurisprudência, esses casos são nos Estados Unidos, no Canadá também, e eu tenho certeza que o Brasil tem casos semelhantes.

SLIDE 18

Essas citações são qualidades muito interessantes do domínio da ciência forense digital. A maioria das informações digitais é uma representação precisa do que pretende estar sujeito à conhecida natureza volátil dos dados, onde um arquivo é, por exemplo, inadvertidamente modificado por alguém que abre o arquivo para lê-lo e, em seguida, salva colocando-o em uma teoria adequada (?) (confuso) para servir uma base científica para uma ciência forense digital as necessidades para satisfazer as demandas impostas pela ciência de justificar os fatos derivados como evidências usando a teoria e tudo isso está levando no domínio da forense digital uma definição de forense digital de quem Olivier em 2016 diz que um artefato digital é uma sequência de bits que tem ou representa significado frequentemente,

mas nem sempre determinado pelo contexto. Então, tudo isso se parece muito com os tipos de coisas sobre as quais falamos na teoria dos arquivos e na preservação digital.

SLIDE 19

Os princípios-chave que são relevantes para ambas as disciplinas são manter a integridade dos materiais. Portanto, todos concordamos que não queremos que o material seja alterado por quaisquer ações tomadas para que todos os documentos, todos os processos que nos comprometemos a capturar e a lista, validem e descrevam o material digital, tenham que ser documentados. Precisamos garantir a competência arquivística dos analistas, se estivermos no a (confuso) confiança forense do especialista no campo forense digital para garantir a conformidade com os regulamentos como leis e aderir a essas medidas científicas de confiabilidade que são repetibilidade, objetividade, verificabilidade e transparência.

SLIDE 20

InterPARES a fim de testar o material digital desenvolveu um modelo de análise contextual. O objetivo era permitir a documentação sistemática de informações relevantes para o contexto da investigação da análise. A primeira seção analisa o contexto administrativo, incluindo a análise do status jurídico dos controles de proveniência em vigor nas políticas da organização e a segunda seção analisa o próprio material e o administrativo e gerencial no qual os objetos digitais relevantes são criados.

SLIDE 21

E realização de uma crítica diplomática a este material digital consiste em analisar os elementos formais do material a fim de identificar, determinar a identidade e estabelecer a integridade do material a crítica é claro que depende do contexto da investigação os conceitos e procedimentos podem aplicar a quaisquer investigações, portanto, em contextos específicos, os procedimentos serão os mesmo conduzindo uma crítica diplomática de material de arquivo ou conduzindo um exame forense de material digital na condução de alguma investigação criminal. Assim, observamos ou examinamos o ambiente físico e tecnológico para começar pela apresentação digital e documental do material. Procuramos a presença ou ausência dos atributos exigidos dos registros digitais. Então, no arquivo inclui conteúdo estável de forma fixa, procuramos as pessoas ou agentes envolvidos na ação ou intenção por trás da criação do documento, o vínculo arquivístico e a hierarquia de contexto. Portanto, estes seriam então o contexto administrativo jurídico, o contexto providencial sobre o contexto processual do criador, o contexto documental e o contexto tecnológico. E se os atributos estiverem presentes, uma análise mais aprofundada deve explicar o status do material. Devemos ser capazes de determinar se o material é autêntico e confiável, entender o que é esse material e se eles estão presentes, uma análise mais detalhada determinará a confiabilidade do material.

SLIDE 22

Relacionando crítica diplomática e exame forense digital houve uma série de modelos propostos para investigação forense digital e podemos mapeá-los para os modelos de fluxos de trabalho para preservação digital, para que possamos mapear a crítica diplomática para os elementos desses modelos de processo forense digital geralmente aceitos e podemos mapear para os modelos teóricos propostos frameworks para análise forense digital também, e tenho links às citações do último slide para que os modelos incluam requisitos teóricos e metodológicos que incluam a análise do objeto, assim, procurando as propriedades necessárias e suficientes para a viabilidade das evidências digitais ou do material de arquivo digital e a validação da metodologia. Portanto, o desenvolvimento e o teste da ferramenta e os resultados desses testes podem provar a validade dos resultados.

SLIDE 23

As perguntas que podemos fazer à crítica diplomática fornecem uma estrutura para exame ou a fase de análise da investigação forense? E vice-versa, as técnicas de investigação forense digital podem se relacionar com a crítica diplomática e essa estrutura satisfará os requisitos científicos? Então olhamos para o quê do material olhamos com diplomáticos, Onde nós olhamos? Olhamos nas camadas de abstração e como vemos quais ferramentas usamos e quais são as validações dessas ferramentas?

SLIDE 24

Portanto, esta é a ligação entre a análise forense digital e o fluxo de trabalho de arquivamento. Assim, no modelo forense digital, o modelo de processo começa com a aquisição da autoridade para pesquisar o conteúdo e isso seria o equivalente no mundo dos arquivos a ter autoridade para adquirir o material, há um aspecto legal para obter acesso ao conteúdo. As próximas três partes do modelo de processo forense digital estabelecem a cadeia de custódia usando funções de *hashing* (ou função de hash; ou hashing) de imagens para estabelecer a integridade e usar ferramentas validadas para fazer isso, relacionadas à aquisição desse material. Então, quando adquirimos material de arquivo, material digital em particular, queremos ter certeza de que a cadeia de custódia está protegida, queremos estabelecer integridade e fazemos isso frequentemente com técnicas criptográficas de *hash* e usamos ferramentas validadas que são transparentes, muitas vezes chamadas de código aberto.

Analisar o conteúdo no modelo forense digital é o equivalente a descrever no fluxo de trabalho de arquivamento, garantindo que a repetibilidade está relacionada aos seguintes princípios de arquivamento, relatórios sobre o resultados da investigação, são equivalentes a produzir a descoberta e a descrição do material e, em seguida, preparar esse material para possível apresentação de um especialista em tribunal no modelo forense digital está relacionado ao fornecimento de acesso a esse conteúdo para o público no fluxo de trabalho de arquivamento.

SLIDE 25

Eu mencionei abstração antes e abstração é que todos os modelos usam abstração, é claro, mas é particularmente relevante e usada comumente em sistemas digitais esta ideia de abstração e a ciência da computação usa abstração extensivamente (confuso). Abstração é este processo de compreensão de objetos complexos, olhando apenas para os detalhes que são essenciais para um aspecto particular daquele objeto ou tarefa ou conceito e a divisibilidade dos dados Digitais em componentes ou níveis menores, onde cada componente ou nível contém seu próprio conjunto exclusivo de características e funcionalidades e não são afetados ou controlados por detalhes em outras camadas de abstração. Para que possamos usar este tipo de técnica de modelagem visa observar apenas as coisas especificamente importantes em cada nível ou camada.

SLIDE 26

Para os documentos digitais, se abstrairmos a visão dos documentos (abstrairmos a visão de documentos digitais), podemos vê-los em termos de uma camada conceitual, uma camada lógica e a camada física. Portanto, começando na parte inferior, a camada física, é claro, é a inscrição dos signos em um meio físico. Então isso pode ser *spinning Disk* ou tecnologia de estado sólido. A camada lógica é o objeto que é reconhecido e processado por hardware e software e então a camada conceitual é mais familiarizados conosco, arquivistas, este é o objeto conforme é reconhecido e entendido como uma pessoa, então as camadas conceituais, lógicas e físicas são usadas no análogo no mundo do papel, não necessariamente todo material analógico, mas no mundo do papel, onde essas três coisas estão conectadas no mundo digital eles devem ser considerados individualmente e separadamente.

SLIDE 27

Portanto, a camada lógica é onde as coisas ficam complicadas para nós. Não estamos muito preocupados com a camada física porque sabemos que os documentos digitais podem ser movidos de um meio para outro sem alterar a autoridade ou a integridade de sua identidade do registro na camada lógica é aqui que precisamos ver como estamos encontrando conteúdo, como estamos retirando conteúdo, como entendemos esse conteúdo e como estamos preservando esse conteúdo. Assim, em coisas como o software de aplicação, as ferramentas de processamento de texto que usamos nas planilhas, bancos de dados multimídia e assim por diante, o software do sistema, o sistema operacional e os utilitários e os compiladores e, em certa medida, o hardware, embora isso não seja tão relevante para os registros individuais, a menos que estejamos olhando para tentar recriar o ambiente de hardware.

SLIDE 28

Olhando para vincular as teorias da perícia digital temos vários especialistas forenses digitais que analisaram essa teoria por trás da ciência forense digital. Olivier diz que uma teoria adequada para servir como base científica para uma ciência forense digital precisa satisfazer as demandas impostas pela ciência e justificar o fato derivado como evidência usando a teoria e uma teoria científica da forense digital então precisa considerar o domínio de forense digital, isto é, os traços digitais de artefatos identificados como o artefato digital, a sequência de bits que tem ou representa um significado com frequência, mas nem sempre determinada pelo contexto.

SLIDE 29

Outra teórica é a Sarah Mocas (Portland State University) quem propôs que os fundamentos teóricos da pesquisa forense digital não deveriam incluir olhar para a integridade do conteúdo e autenticação, da não interferência da reprodutibilidade do conteúdo, também relacionada à integridade e minimização. Portanto, não fazer mais do que o necessário ou capturar mais conteúdo do que o necessário e todos esses cinco, embora expressem diferentemente da arquivística, também se relaciona muito diretamente com as teorias arquivísticas de preservação.

SLIDE 30

Finalmente Andrew propôs em 2007 um modelo de processo de análise adicional que era ligeiramente diferente dos modelos anteriores de processo, os dois princípios propostos que deveriam formar a base da análise forense digital: o princípio da consistência para que a consistência dos resultados e o princípio da estabilidade seja que o conteúdo não deve ser alterado, de modo que o conteúdo no armazenamento não deve mudar enquanto está armazenado, muito parecido com a forma fixa e o conteúdo estável e, dentro desses dois princípios, ele identificou o que considerou cinco leis. São essas as áreas de exame que tiveram de ser abordadas na qualificação de dados para apoiar conclusões e opiniões. Portanto, a lei de associação do processo e da fonte, o contexto interno e externo em que o material, acesso a esse material e quem tem acesso a ele. Qual é a intenção por trás disso e se há alguma corrupção, quais são os controles em torno disso e, em seguida, a validação, a integridade, autenticidade e precisão do material?

Slide 31

Podemos construir essas pontes entre a Ciência Arquivística e a diplomática arquivística e os princípios e teorias da forense digital. Portanto, pela teoria arquivística temos a teoria da proveniência e da ordem original e o conceito de vínculo arquivístico; partir dos princípios arquivísticos e diplomáticos temos as qualidades de arquivos que se relacionam com Jenkinson, os atributos necessários e

suficientes dos registros que formam e estabilizam o conteúdo, as ações, as pessoas envolvidas no contexto em que o documento é criado e os elementos de confiabilidade. Portanto, autenticidade, confiabilidade e precisão, temos medidas científicas de confiabilidade que se relacionam com a preservação de arquivos, preservação digital e perícia digital. Assim, os princípios científicos da repetibilidade da objetividade da verificabilidade e da transparência. Nós temos os problemas dessa capacidade de evidência documental, pelo menos em situações de lei comum de autenticidade de relevância e a regra de melhor evidência que se relaciona no ambiente digital à integridade do sistema e, então, temos os princípios de análise forense digital de Andrew, o princípio de estabilidade e consistência e as leis da associação, acessar conteúdo de contexto e validar, o fluxo de trabalho forense digital e os princípios dos princípios básicos não mudam as evidências. Portanto, mantenha a integridade da cadeia de custódia para oferecer suporte à integridade e à reprodutibilidade da autenticação, não interferência e minimização. E então, esses são apoiados tanto na Ciência Arquivística quanto na análise forense digital por meio de jurisprudência nos Estados Unidos e no Canadá em particular para relevância, as qualificações necessárias é evidência científica.

SLIDE 32

As atuais e futuras aplicações forenses digitais em arquivística, vemos isso em coisas como a preservação como um serviço de confiança que surgiu da InterPARES Trust, desenvolvendo critérios claros, objetivos e executáveis para formular e avaliar os conceitos da Ciência Arquivística, integrando ferramentas forenses digitais ao processamento de arquivos, onde coleções digitais podem ser analisadas em múltiplos níveis de representação ou níveis múltiplas camadas da tecnologia, então coisas como BitCurator e Archivemata fazem isso e, em seguida, o desenvolvimento da Ciência Arquivística computacional. Portanto, este é um campo interdisciplinar que se preocupa particularmente com a aplicação de métodos e recursos computacionais no trabalho de arquivamento e registros em grande escala. Aplicando conhecimento coletivo de ciência da computação e arquivística, e vemos isso no trabalho de Richard Marciano e Vicky Lemieux outros.

SLIDE 33

Meu próximo slide é apenas um agradecimento, mas talvez possamos ir para o último slide.

SLIDE 34

Esta é uma bibliografia muito curta das várias fontes de que falei nesta apresentação, e agora muito obrigado. Estou ansiosa para ouvir suas perguntas.

REFERÊNCIAS – SLIDE 34

ANDREW, Michael W. Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media. In: SADFE 2007: Second International Workshop on Systematic Approaches to Digital Forensic Engineering: **Proceedings**: 10-12 April 2007, Seattle, Washington, USA, edited by Northwest Security Institute and Pacific Northwest National Laboratory (U.S.). Los Alamitos, Calif: IEEE Computer Society, 2007.

COHEN, Fred. **Digital Forensic Evidence Examination**. [S.l.]: Asp Press, 2012.

COHEN, Fred. Digital Diplomats and Forensics: Going Forward on a Global Basis. *Records Management Journal*, v. 25, n. 1, p. 21–44, 2015. <https://doi.org/10.1108/RMJ-03-2014-0016>.

- DIAMOND, Elizabeth. The archivist as forensic scientist – seeing ourselves in a different way. *Archivaria*, v. 38, Fall, p. 139–54, 1994.
- DURANTI, Luciana. From digital diplomatics to digital records forensics. *Archivaria*, v. 68, Fall, p. 39–66, 2009.
- DURANTI, Luciana; CORINNE Rogers. Memory Forensics: Integrating Digital Forensics with Archival Science for Trusting Records and Data. *eForensics Magazine*, v. 2, n. 15, p. 96–111, 2013.
- EASTWOOD, Terry. What is archival theory and why is it important? *Archivaria*, v. 37, Spring, p. 122–30, 1994.
- EASTWOOD, Terry. Jenkinson’s writings on some enduring archival themes. *American Archivist*, v. 67, n. 1, p. 31–44, 2004.
- FERGUSON-BOUCHER, K. A.; ENDICOTT-POPOVSKY, Barbara. Digital forensics and records management: what we can learn from the discipline of archiving, p. 1–6, 2008.
- IRONS, Alastair. Computer forensics and records management – compatible disciplines. *Records Management Journal*, v. 16, n. 2, p. 102–112, 2006. Disponível em: <https://doi.org/10.1108/09565690610677463>.
- JOHN, Jeremy Leighton. 2012. Digital forensics and preservation: digital preservation coalition. Disponível em: http://www.dpconline.org/component/docman/doc_download/810-dpctw12-03pdf.
- KIRSCHENBAUM, Matthew G. Mechanisms: new media and the forensic imagination C. Cambridge, MA: MIT Press, 2008.
- KIRSCHENBAUM, Matthew G.; RICHARD OVENDEN; Gabriela Redwine. Digital forensics in born digital cultural heritage collections. Washington, D.C.: Council on Library and Information resources, 2010.
- LEE, Christopher. Archival application of digital forensics methods for authenticity, description and access provision. *Comma*, n. 2, p. 133–40, 2012. Disponível em: <https://doi.org/10.3828/comma.2012.2.14>.
- MARCIANO, R. et al. Archival records and training in the age of big data. Submission Draft. 2018. Disponível em: http://dcicblog.umd.edu/cas/wp-content/uploads/sites/13/2016/05/submission_final_draft.pdf.
- MARTIN, Oliver. On a scientific theory of digital forensics. In: PETERSON G.; SHENOI, S. (ed.) Advances in digital forensics XII. DigitalForensics 2016. IFIP Advances in Information and Communication Technology, Springer, Cham, v. 484, 2016. Disponível em: https://doi.org/10.1007/978-3-319-46279-0_1
- MOCAS, Sarah. Building theoretical underpinnings for digital forensics research. *Digital Investigation*, v.1, n. 1, p. 61–68, 2004.
- POLLITT, Mark M. Computer forensics: an approach to evidence in cyberspace. Baltimore, Maryland: NIST, 1995. P. 487–91. Disponível em: www.digitalevidencepro.com/Resources/Approach.pdf.

ROGERS, Corinne. Diplomatics of born digital documents: considering documentary form in a digital environment. **Records Management Journal**, v. 25, n. 1, p. 6–20, 2015.

ROGERS, Corinne; JOHN, JL. Shared perspectives, common challenges: a history of digital forensics & ancestral computing for digital heritage. *In*: THE MEMORY of the World in the Digital Age: Digitization and Preservation. Vancouver, BC: UNESCO, 2013. p. 314–336. Disponível em: http://www.unesco.org/webworld/download/mow/mow_vancouver_proceedings_en.pdf .

ZATYKO, Ken. Commentary: defining digital forensics. **Forensic Magazine**, Jan. 2007. Disponível em: <http://www.forensicmag.com/node/128.182>.