Marcelo Alcides C. Gomes, PhD

Sócio | Risk Consulting Forensic & Litigation

E-Discovery

Data Analytics e novas tecnologias nos procedimentos de Perícia Contábil

E-Discovery e Perícia Contábil

Definição – Forense Digital

- É uma disciplina da ciência forense que trata dos aspectos de coleta, preservação, recuperação, inspeção e análise de dados digitais armazenados em dispositivos eletrônicos.
- Sua principal aplicação consiste em oferecer credibilidade técnica para suportar ou refutar hipóteses em um determinado caso.

Termos sinônimos

- Computação forense, Digital Forensics, Cyber Forensics, DFIR, Digital Investigation.

Planejamento, Execução e Procedimentos Periciais

Planejamento

Conhecer o objeto e a finalidade da perícia permitindo a escolha da metodologia e das ferramentas que serão utilizadas para executar os trabalhos

Desenvolver um plano de trabalho conhecendo os prazos estabelecidos e acompanhar seu cumprimento

Identificação de riscos que possam comprometer os trabalhos periciais
Identificar a legislação aplicável para o tema que se discute

Dividir as tarefas a serem executadas pelos membros da equipe de acordo com um plano de trabalho

Realizar reunião técnica para conhecer Assistentes e apresentar o plano de trabalho

Planejamento, Execução e Procedimentos Periciais

Execução

Elaborar Termo de Diligência para solicitar dados, documentos e informações das partes

Realizar visitas as dependências das partes ou ativos sob análise, se couber

Elaborar atas de todas as reuniões técnicas e visitas realizadas

Preparação de WP´s de todos procedimentos executados

Planejamento, Execução e Procedimentos Periciais

PROCEDIMENTOS

Exame é a análise de livros, registros de transações e documentos

Planejamento, Execução e Procedimentos Periciais

PROCEDIMENTOS

Exame é a análise de livros, registros de transações e documentos

Vistoria é a diligência que objetiva a verificação ou constatação de situação, coisa ou fato

Planejamento, Execução e Procedimentos Periciais

PROCEDIMENTOS

Exame é a análise de livros, registros de transações e documentos

Vistoria é a diligência que objetiva a verificação ou constatação de situação, coisa ou fato

Indagação é a busca de informações mediante entrevista com os conhecedores do objeto ou de fato relacionado aos trabalhos

Planejamento, Execução e Procedimentos Periciais

PROCEDIMENTOS

Exame é a análise de livros, registros de transações e documentos

Vistoria é a diligência que objetiva a verificação ou constatação de situação, coisa ou fato

Indagação é a busca de informações mediante entrevista com os conhecedores do objeto ou de fato relacionado aos trabalhos

Investigação é a pesquisa que busca constatar o que está oculto por quaisquer circunstâncias

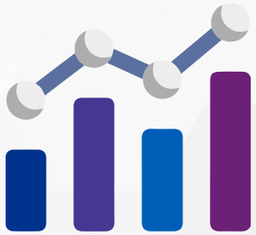
Planejamento, Execução e Procedimentos Periciais

PROCEDIMENTOS

Arbitramento é a determinação de valores, quantidade, ou a solução de controvérsia por critério técnico-cientifico

Planejamento, Execução e Procedimentos Periciais

PROCEDIMENTOS

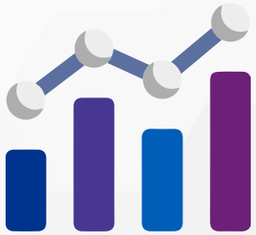


Arbitramento é a determinação de valores, quantidade, ou a solução de controvérsia por critério técnico-cientifico

Mensuração é o ato de qualificação e quantificação física de coisas, bens, direitos e obrigações

Planejamento, Execução e Procedimentos Periciais

PROCEDIMENTOS



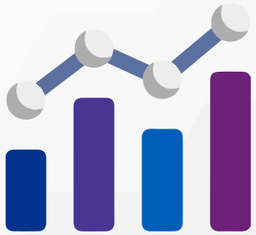
Arbitramento é a determinação de valores, quantidade, ou a solução de controvérsia por critério técnico-cientifico

Mensuração é o ato de qualificação e quantificação física de coisas, bens, direitos e obrigações

Avaliação é o ato de estabelecer valor de coisas, bens, direitos, obrigações, despesas e receitas

Planejamento, Execução e Procedimentos Periciais

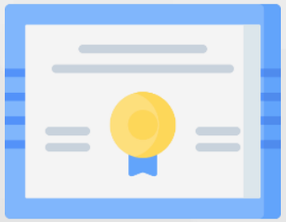
PROCEDIMENTOS



Arbitramento é a determinação de valores, quantidade, ou a solução de controvérsia por critério técnico-cientifico

Mensuração é o ato de qualificação e quantificação física de coisas, bens, direitos e obrigações

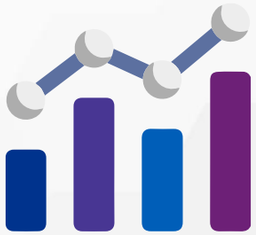
Avaliação é o ato de estabelecer valor de coisas, bens, direitos, obrigações, despesas e receitas



Certificação é o ato de atestar a informação obtida na formação da prova pericial

Planejamento, Execução e Procedimentos Periciais

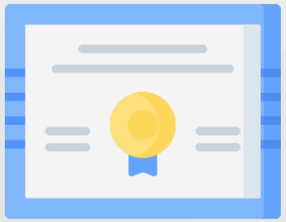
PROCEDIMENTOS



Arbitramento é a determinação de valores, quantidade, ou a solução de controvérsia por critério técnico-cientifico

Mensuração é o ato de qualificação e quantificação física de coisas, bens, direitos e obrigações

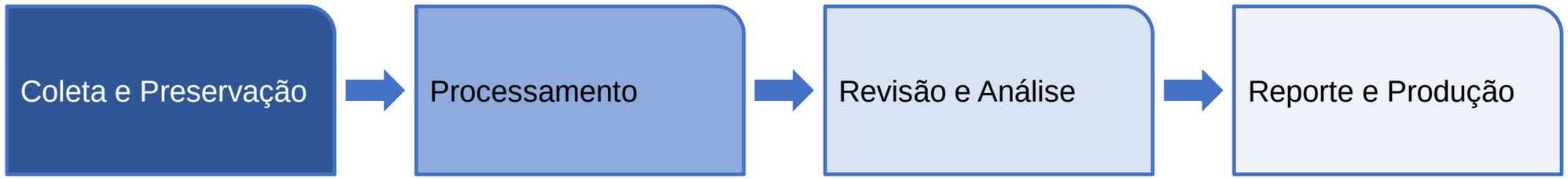
Avaliação é o ato de estabelecer valor de coisas, bens, direitos, obrigações, despesas e receitas



Certificação é o ato de atestar a informação obtida na formação da prova pericial

Testabilidade é a verificação dos elementos probantes juntado aos autos e o confronto com as premissas estabelecidas

Metodologia Simplificada



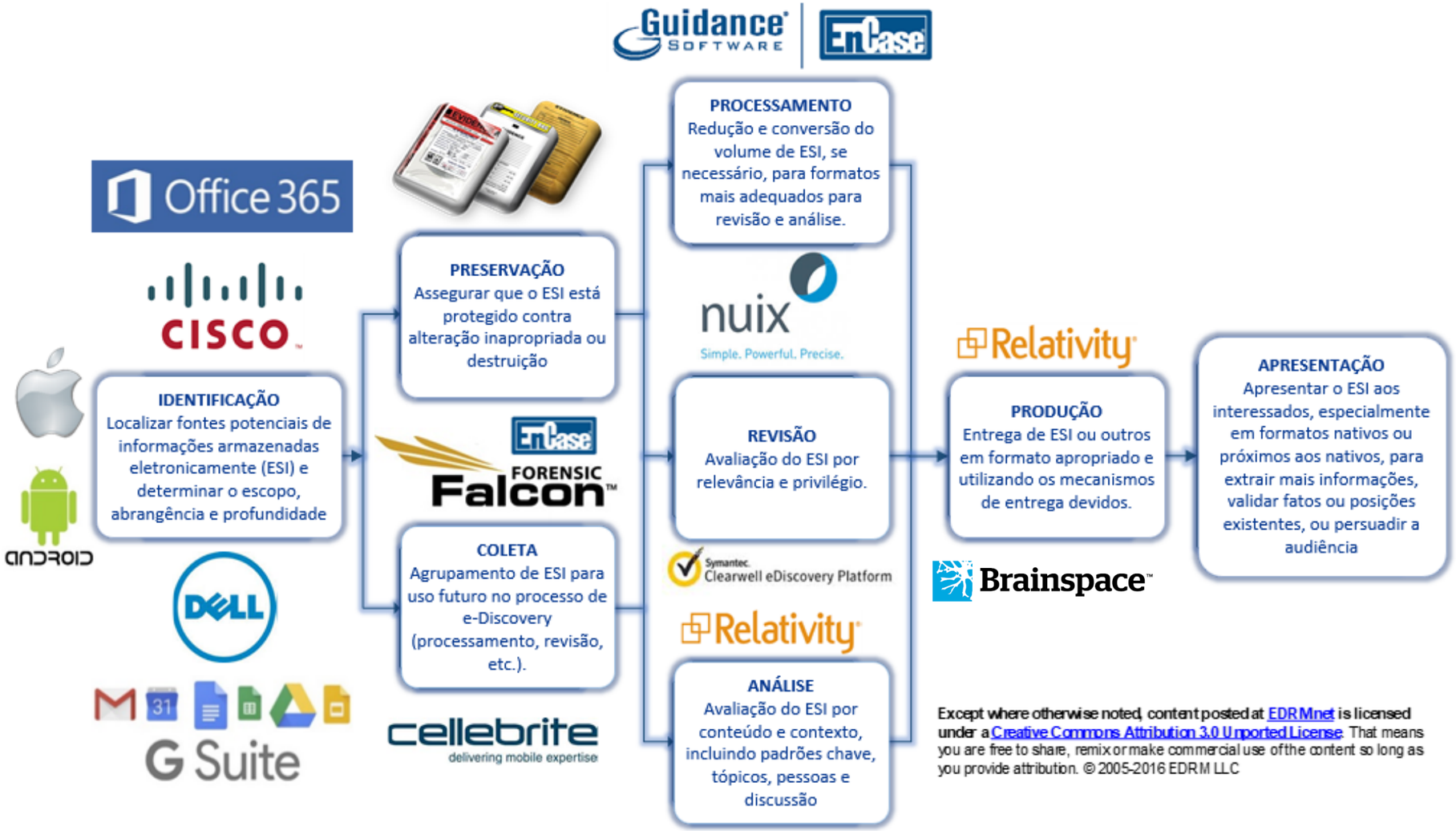
- Escopo das fontes de dados da sua investigação
- Aquisição de dados para permitir análises

- Transformação do conteúdo em escopo para permitir realização de buscas
- Técnicas de diminuição defensiva
- Técnicas de OCR, Recuperação de dados apagados

- Análise detalhada do conteúdo relevante
- Revisão de documentos eletrônicos
- Seleção dos documentos relevantes identificados

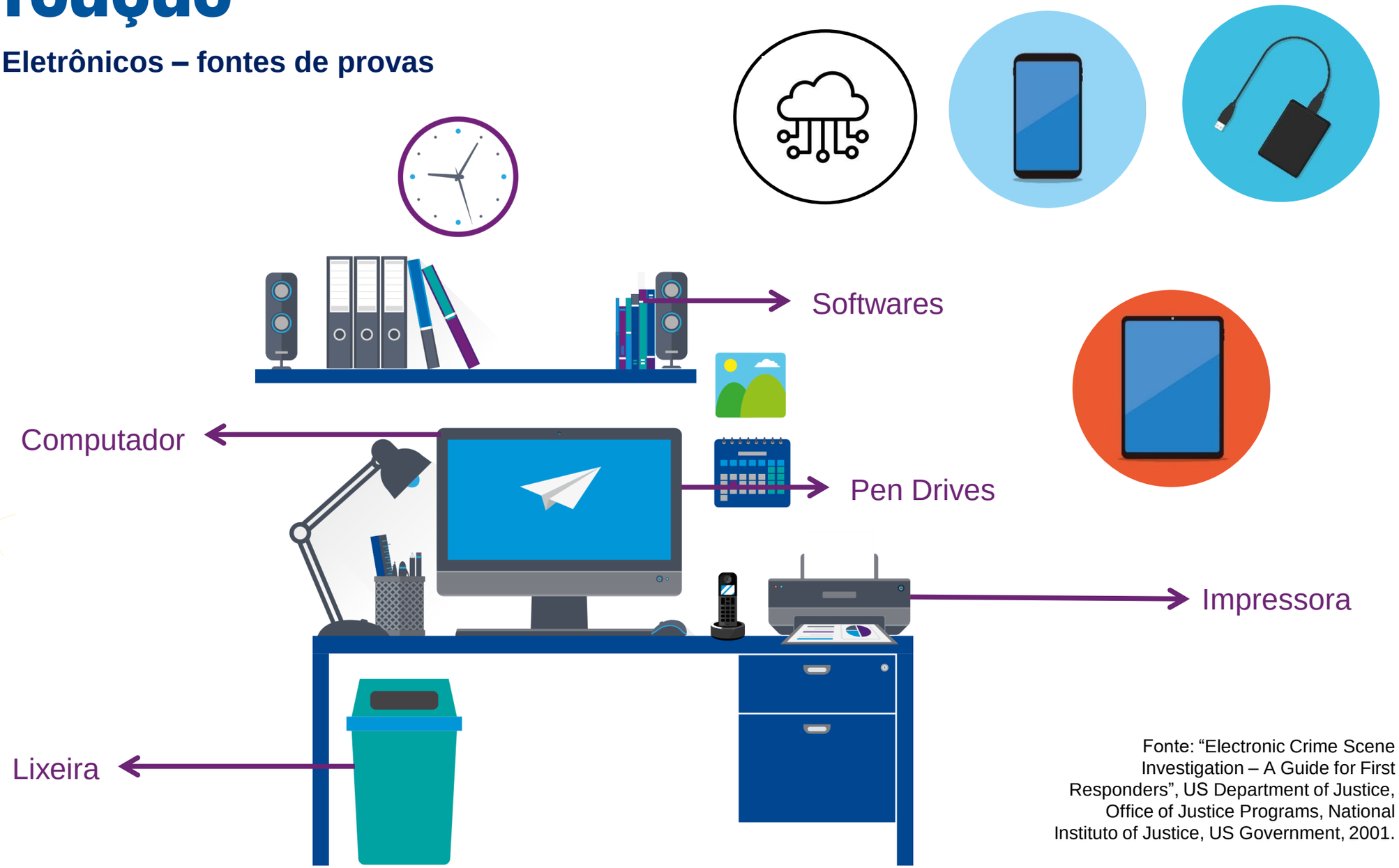
- Produção de documentos eletrônicos mantendo sua cadeia de custódia
- Exportação dos documentos e metadados em formato aceitável (DOJ, CADE)

Modelo eDRM – Exemplos de Ferramentas



Identifcação

Dispositivos Eletrônicos – fontes de provas



Fonte: “Electronic Crime Scene Investigation – A Guide for First Responders”, US Department of Justice, Office of Justice Programs, National Instituto of Justice, US Government, 2001.

Noções Básicas de Direito Digital

Evidência ou Prova Computacional

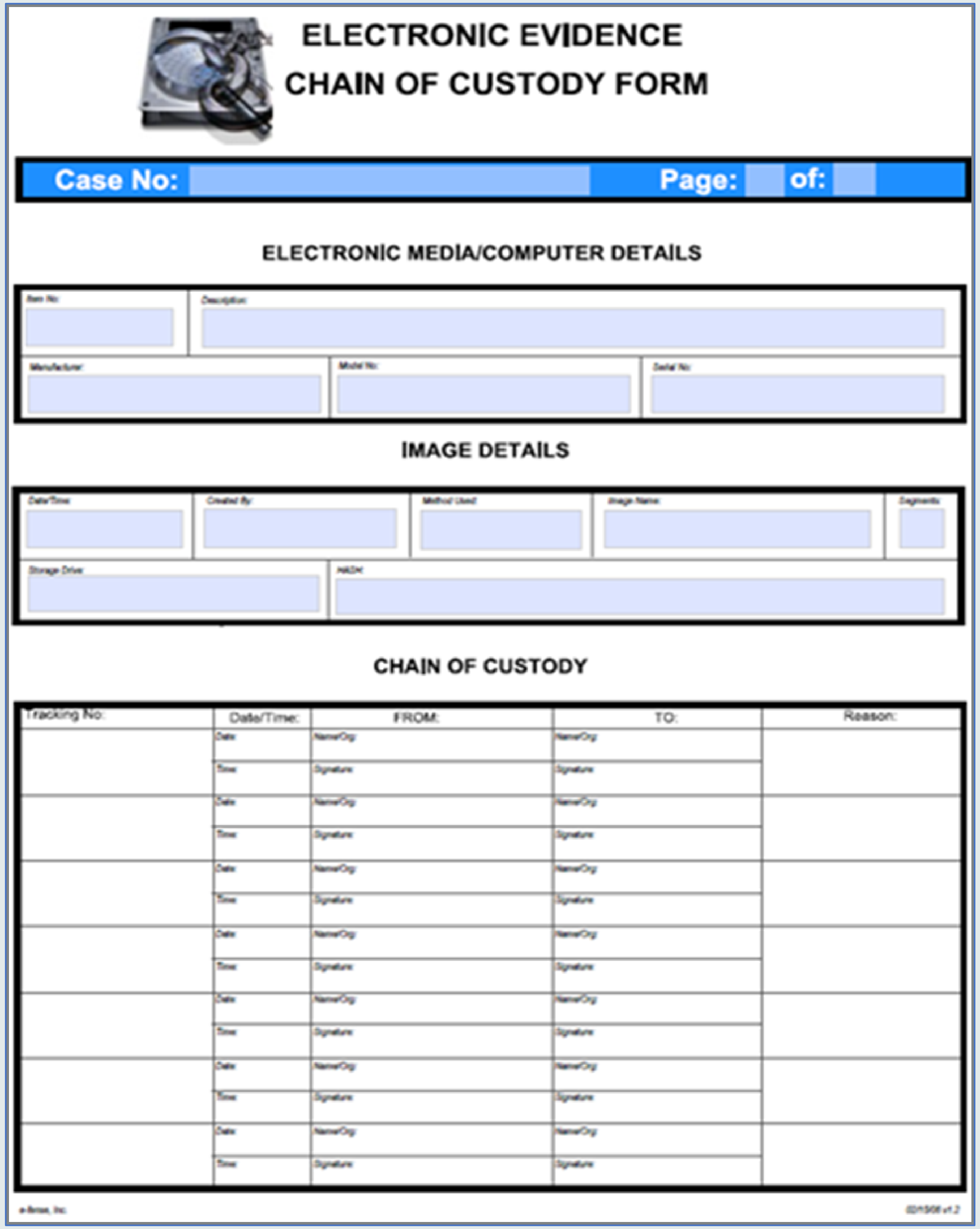
“A prova eletrônica é hábil a comprovar a ocorrência de um fato e, ***se colhida corretamente****,* ***faz prova mais eficaz do que aquela colhida por outro meio****. Para o correto uso e* ***admissibilidade da prova*** *eletrônica em Juízo, devem ser observados os* ***padrões técnicos de manuseio, coleta e guarda.*** *As provas eletrônicas somente estarão a salvo de serem declaradas inválidas, caso sejam mantidas suas* ***integridade*** *e* ***autenticidade*** *no procedimento de captura de evidências”*

- Patrícia Peck, advogada e especialista em Direito Digital

Aspectos centrais:

- Coleta forense obedecendo padronização técnica para manuseio e guarda;
- Manutenção de integridade e autenticidade da prova, incluindo possibilidade de verificação e confirmação a qualquer tempo quanto a este fator, no procedimento de captura de evidências.

Procedimentos de cadeia de custódia da prova digital



ELECTRONIC EVIDENCE
CHAIN OF CUSTODY FORM

Case No: Page: of:

ELECTRONIC MEDIA/COMPUTER DETAILS

Item No:	Description:	
Manufacturer:	Model No:	Serial No:

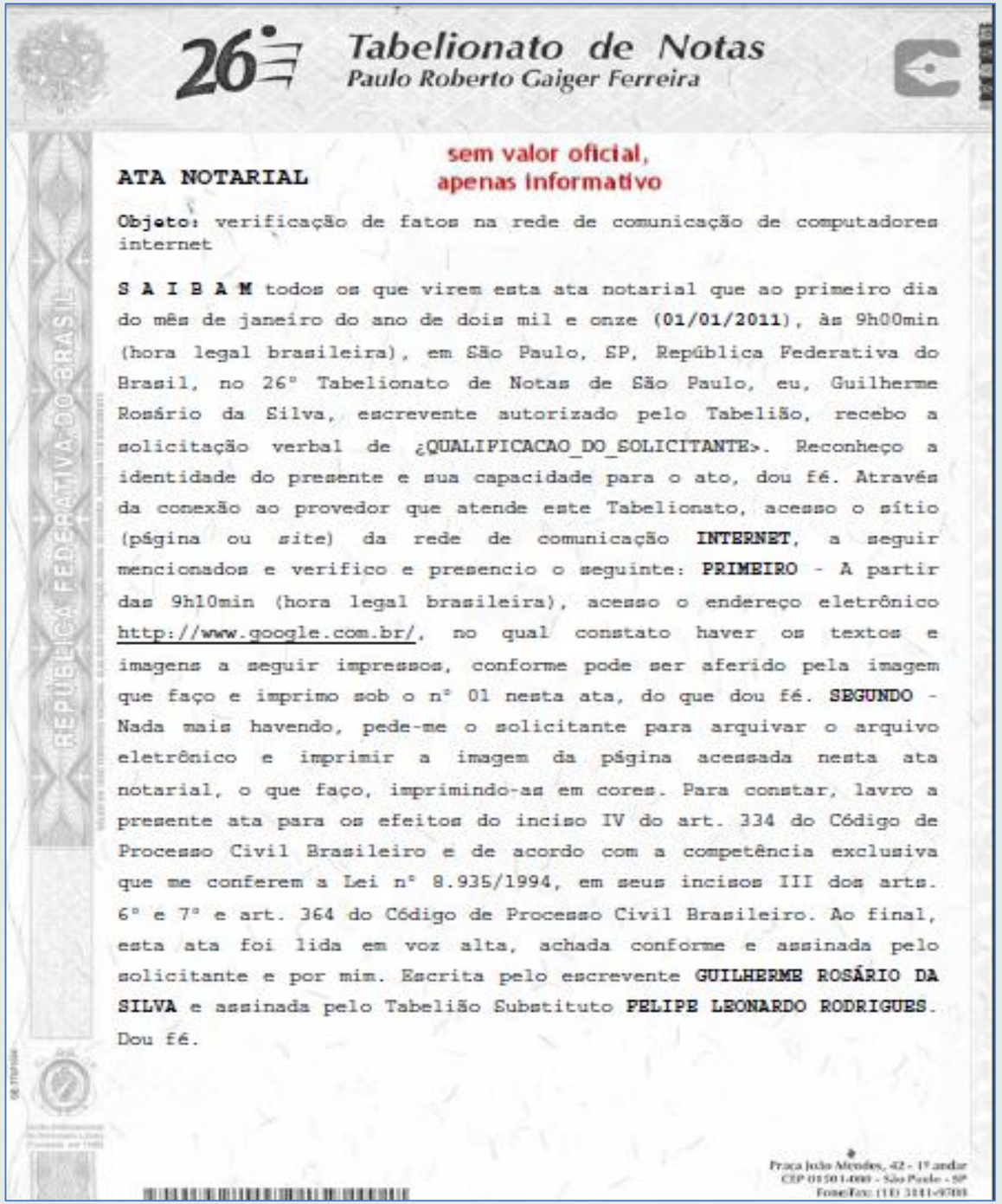
IMAGE DETAILS

Date/Time:	Created By:	Method Used:	Image Name:	Segments:
Storage Drive:	HASH:			

CHAIN OF CUSTODY

Tracking No:	Date/Time:	FROM:	TO:	Reason:
	Date / Time	Name/Org / Signature	Name/Org / Signature	
	Date / Time	Name/Org / Signature	Name/Org / Signature	
	Date / Time	Name/Org / Signature	Name/Org / Signature	
	Date / Time	Name/Org / Signature	Name/Org / Signature	
	Date / Time	Name/Org / Signature	Name/Org / Signature	
	Date / Time	Name/Org / Signature	Name/Org / Signature	
	Date / Time	Name/Org / Signature	Name/Org / Signature	

Procedimentos de cadeia de custódia da prova digital



26º Tabelionato de Notas
Paulo Roberto Gaiger Ferreira

sem valor oficial,
apenas informativo

ATA NOTARIAL

Objeto: verificação de fatos na rede de comunicação de computadores internet

S A I B A M todos os que virem esta ata notarial que ao primeiro dia do mês de janeiro do ano de dois mil e onze (**01/01/2011**), às 9h00min (hora legal brasileira), em São Paulo, SP, República Federativa do Brasil, no 26º Tabelionato de Notas de São Paulo, eu, Guilherme Rosário da Silva, escrevente autorizado pelo Tabelião, recebo a solicitação verbal de ¿QUALIFICACAO_DO_SOLICITANTE>. Reconheço a identidade do presente e sua capacidade para o ato, dou fé. Através da conexão ao provedor que atende este Tabelionato, acesso o sítio (página ou *site*) da rede de comunicação **INTERNET**, a seguir mencionados e verifico e presencio o seguinte: **PRIMEIRO** - A partir das 9h10min (hora legal brasileira), acesso o endereço eletrônico http://www.google.com.br/, no qual constato haver os textos e imagens a seguir impressos, conforme pode ser aferido pela imagem que faço e imprimo sob o nº 01 nesta ata, do que dou fé. **SEGUNDO** - Nada mais havendo, pede-me o solicitante para arquivar o arquivo eletrônico e imprimir a imagem da página acessada nesta ata notarial, o que faço, imprimindo-as em cores. Para constar, lavro a presente ata para os efeitos do inciso IV do art. 334 do Código de Processo Civil Brasileiro e de acordo com a competência exclusiva que me conferem a Lei nº 8.935/1994, em seus incisos III dos arts. 6º e 7º e art. 364 do Código de Processo Civil Brasileiro. Ao final, esta ata foi lida em voz alta, achada conforme e assinada pelo solicitante e por mim. Escrita pelo escrevente **GUILHERME ROSÁRIO DA SILVA** e assinada pelo Tabelião Substituto **PELIPE LEONARDO RODRIGUES**. Dou fé.

Praça João Mendes, 42 - 1º andar
CEP 01501-000 - São Paulo - SP
Fone/Fax: (11) 3111-9700

Cópias Simples vs Cópia Forense

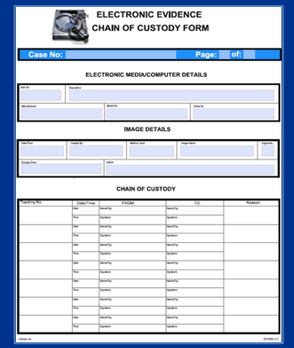
Cópia Simples

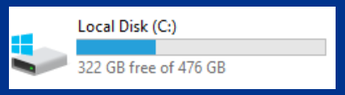
- **Famoso “Ctrl-C / Ctrl-V”**
- **Simples, rápido e barato**
- **Não gera registro de logs ou hash e, portanto, não possibilita rastramento e cadeia de custódia**

Cópia Forense

- **Requer uso de ferramentas ou programas específicos, portanto, é mais complexo**
- **Gera logs de sucesso / falha**
- **Gera código hash do dado copiado**
- **Deve ser acompanhado por Cadeia de custódia**

Aquisição de dados (Visão Completa)





FORENSIC Falcon®

EnCase®

ACCESSDATA
ForensicToolkit (FTK)

www.kpmg.com.br

/kpmgbrasil

Hash

Algoritmo que transforma qualquer dado/arquivo de entrada, independente de seu tamanho, em um código de tamanho fixo e único de saída - (“DNA” do arquivo)

	Dado de Entrada (palavra)	Cálculo Hash	Código Hash MD5 (32 caracteres)
Exemplo1	Compliance		9c0408c775a2b61052a2e700a89f396f
Exemplo2	#Compliance		c7827ae064804ed1d37cd4fa75a0cb78

Principais características do HASH

- Irreversibilidade (via única)
- Não previsibilidade

Existem diversas ferramentas e utilitários disponíveis que fazem cálculo de hash de dados. Exemplos: Encase, FTK Imager, HashMyFiles, Get-FileHash (Powershell), etc.

- Validar a integridade de cópias forense

Cálculo Hash

Original

101100
010110
100101

Código hash [original]

9c0408c775a2b61052a2e700a89f396f

Validação [match!]

Imagem forense

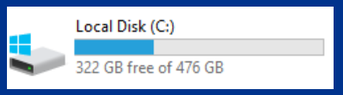
Cálculo Hash

9c0408c775a2b61052a2e700a89f396f

Código hash [cópia]

Destino

Aquisição de dados (Forense)



FORENSIC Falcon®

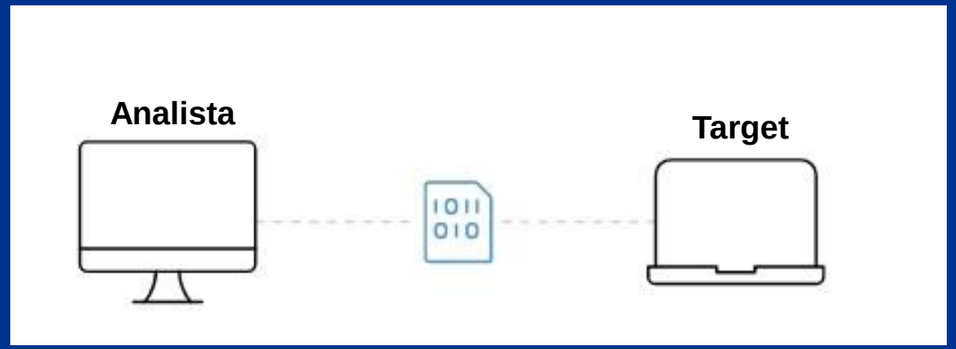
EnCase®

ACCESSDATA ForensicToolkit (FTK)

www.kpmg.com.br

/kpmgbrasil

Coleta remota (Computadores)



Instala um agente remotamente no *target* (transparente)

O agente permite comunicar-se com o sistema remoto

O analista seleciona o conteúdo de interesse e transfere via rede para o destino

Principais desafios

- Velocidade de transferência entre target-destino
- Interrupções (queda de conexão internet, usuário desconecta do *wifi)*
- Necessidade de abrir algumas portas / exceções de firewall (em alguns casos)
- Sem uso de ferramentas adequadas, pode-se gerar resultados indesejados (arquivos protegidos que não copiaram)
- A coleta de smartphones demonstrou alguma evolução, mas ainda se restringe à uma gama limitada de aparelhos e depende do custodiante se conectar a um dispositivo com software forense instalado (Ex: Cellebrite Commander) – "*no stealth*"

www.kpmg.com.br

/kpmgbrasil

Exemplos de ferramentas

MAGNET AXIOM

F-Response

Dispositivos Móveis

Tipos de dispositivos

- Smartphones e Tablets
  - Android
  - iOS (Apple)
- Memory Cards

Desafios

- Senhas / Proteções de segurança
- Volatilidade dos dados
- Variedade de versões e modelos

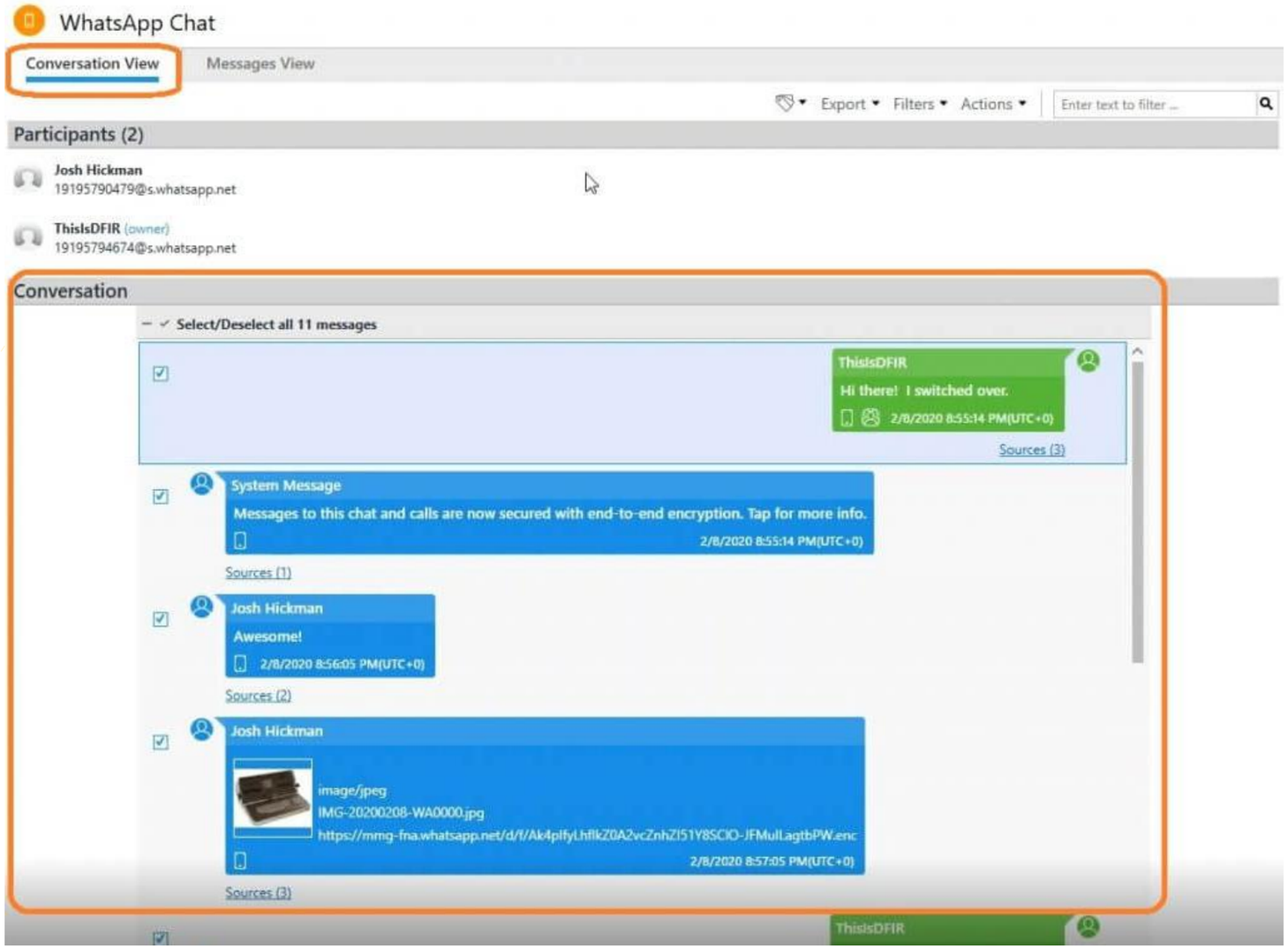
Dispositivos Móveis

XRY™ cellebrite delivering mobile expertise MAGNET AXIOM

Principais fontes de dados

- **Visão da ferramenta Cellebrite**

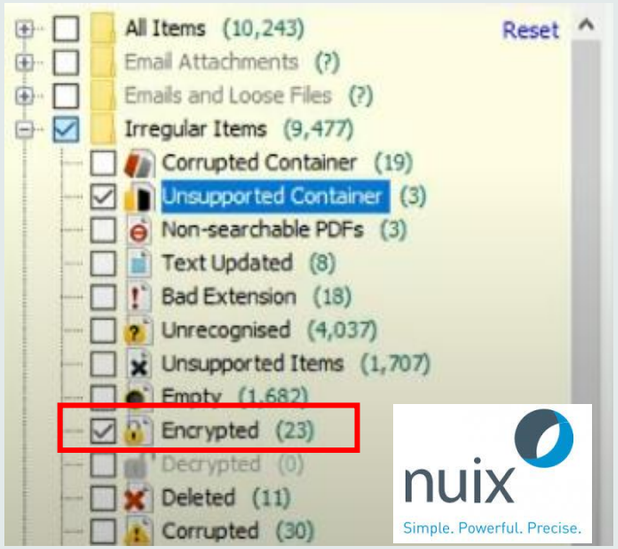
- **Conversa de WhatsApp coletada**



Processamento

- Consolidação e normalização dos dados coletados (incluindo arquivos recuperados)
- Indexação
- OCR

- Exceções – identificação de arquivos criptografados, corrompidos, etc



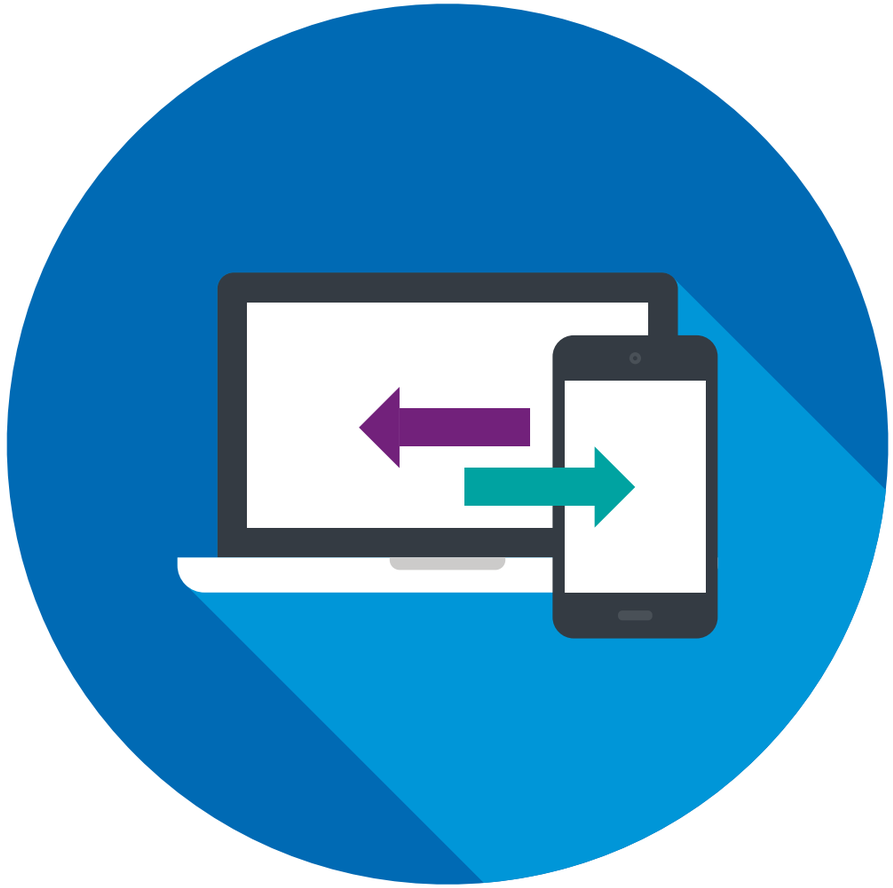
Técnicas de Diminuição Defensiva

- Identificação e **exclusão de arquivos conhecidos** (deNIST, Sistema)
  - Utiliza-se uma base pública de arquivos conhecidos para excluí-los da base

- **Deduplicação por HASH**
  - Com base no codigo hash de cada arquivo, é realizada a exclusão de arquivos duplicados

- Threading de **cadeias de e-mails** (mais inclusivo)
  - Identificamos qual a mensagem de e-mail mais inclusiva de cada cadeia de e-mails

Formas de busca - Termos



Busca por termos

- Operadores e funções dtSearch
- Busca em todo conteúdo **dos arquivos**

Exemplos buscas simples (operadores lógicos):

I. ”EmpresaA” **AND** “Pagamento”
II. (“Aprovação” **OR** “Validação) **AND** “Orçamento”

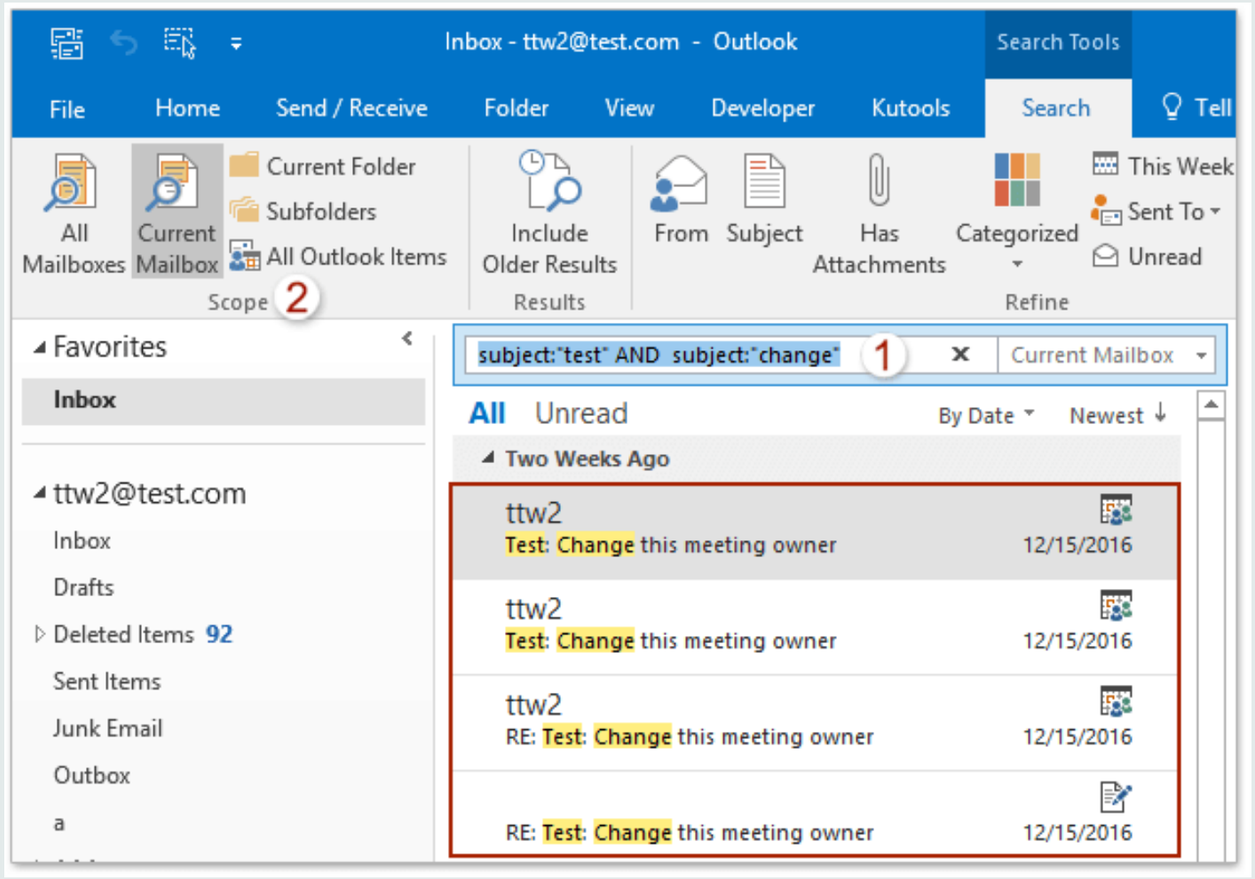
Exemplos buscas avançadas (proximidade)

I. “fazer” **w/2** “acordo”
II. (“fazer” **w/2** “acordo”) **AND** “por fora”

Revisão via Outlook

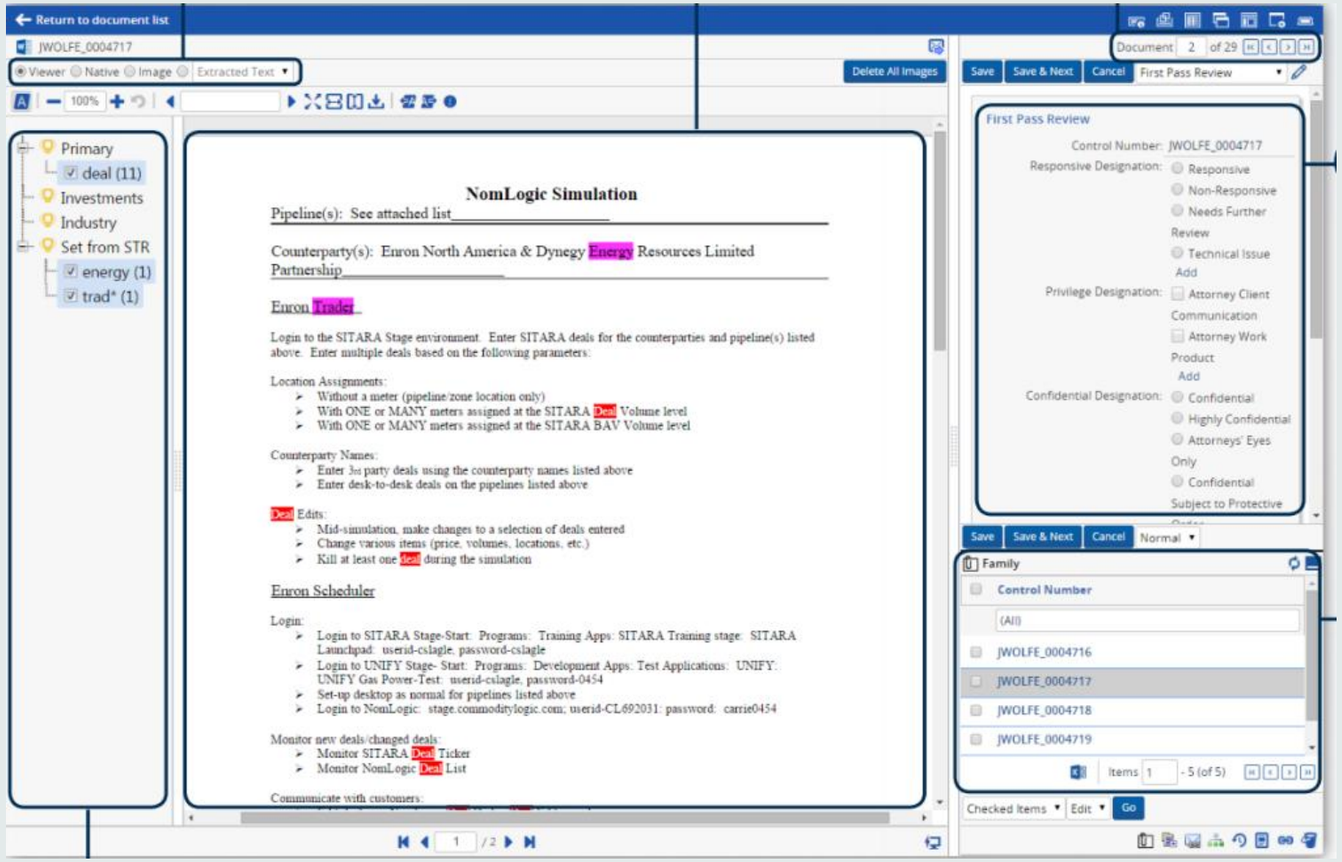
- Busca simples via Outlook para encontrar conteúdo relevante

- Desvantagens:
  - Não permite combincação e buscas mais complexas
  - Não permite manter rastreamento do que foi revisado vs restante
  - Diversos documentos podem ser revisados sem necessidade



Buscas e Revisão com ferramentas apropriadas

- Auxilia determinar o esforço e dimensionamento de equipe
- Ajuda identificar palavras / termos que podem estar causando falso-positivos
- Identifica oportunidades de refinamento por meio de combinações mais efetivas
- Permite rastramento do que foi revisado vs pendente
- Distribuição de documentos para equipe de revisores

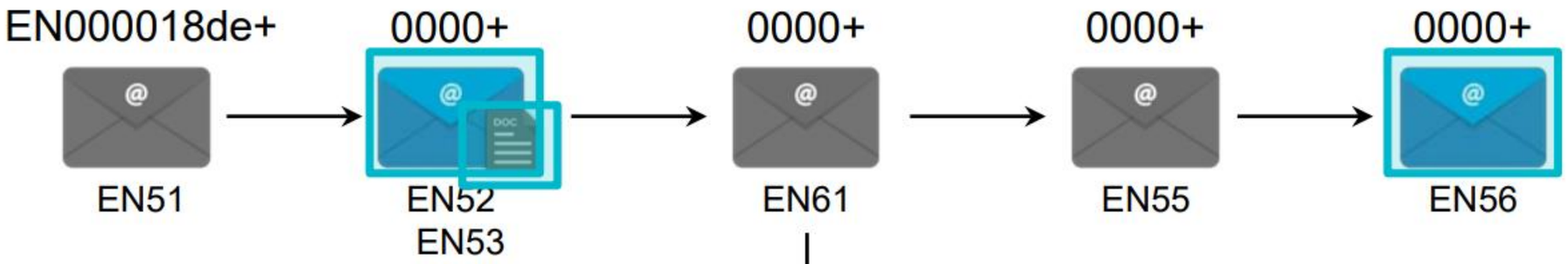


Terms Summary

Term	Documents with hits	Documents with hits, including Family	Unique hits
"fantasy football"	450	9,538	409
"Raptor Natural Pipeline"	21	76	0
blair OR brawner OR (Ken Lay) OR (Sara Shackleton)	6,494	12,200	6,076

Analytics – Email Threading (Inclusive message)

Relativity

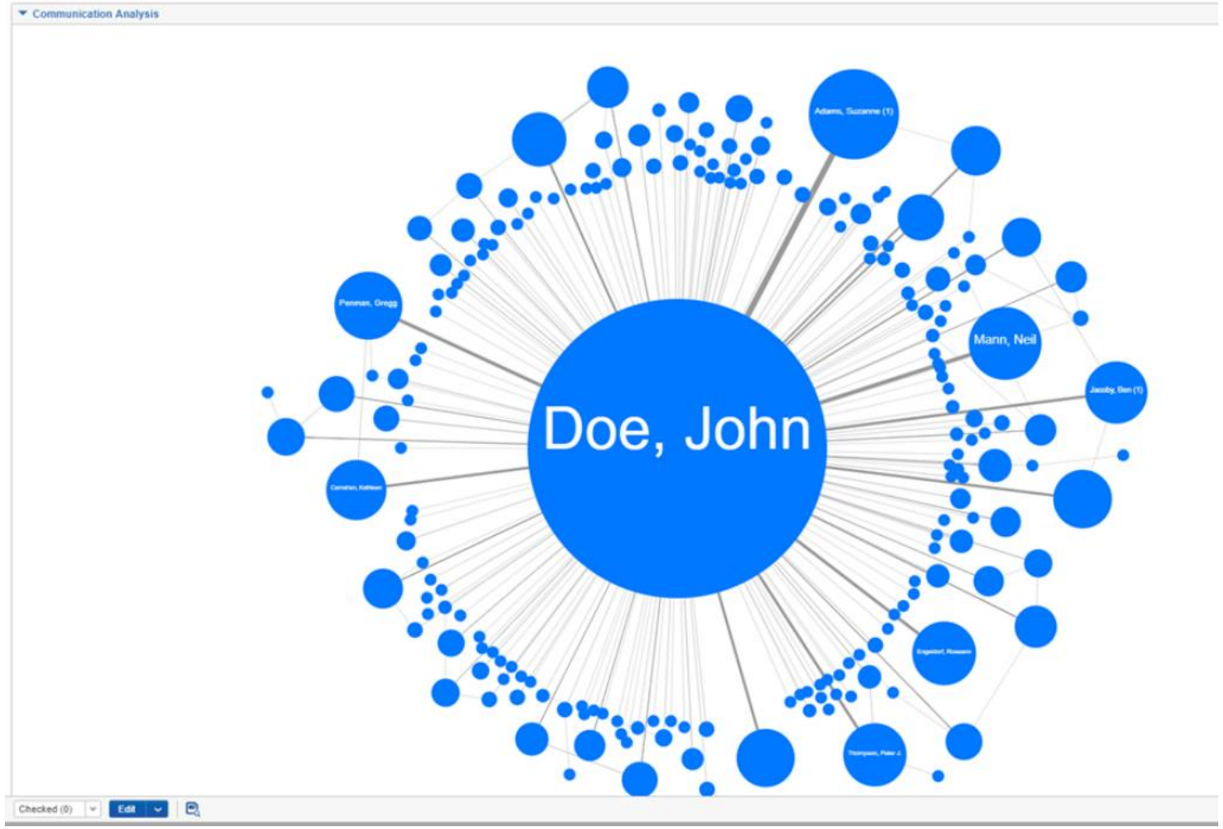


4 of 8 Documents

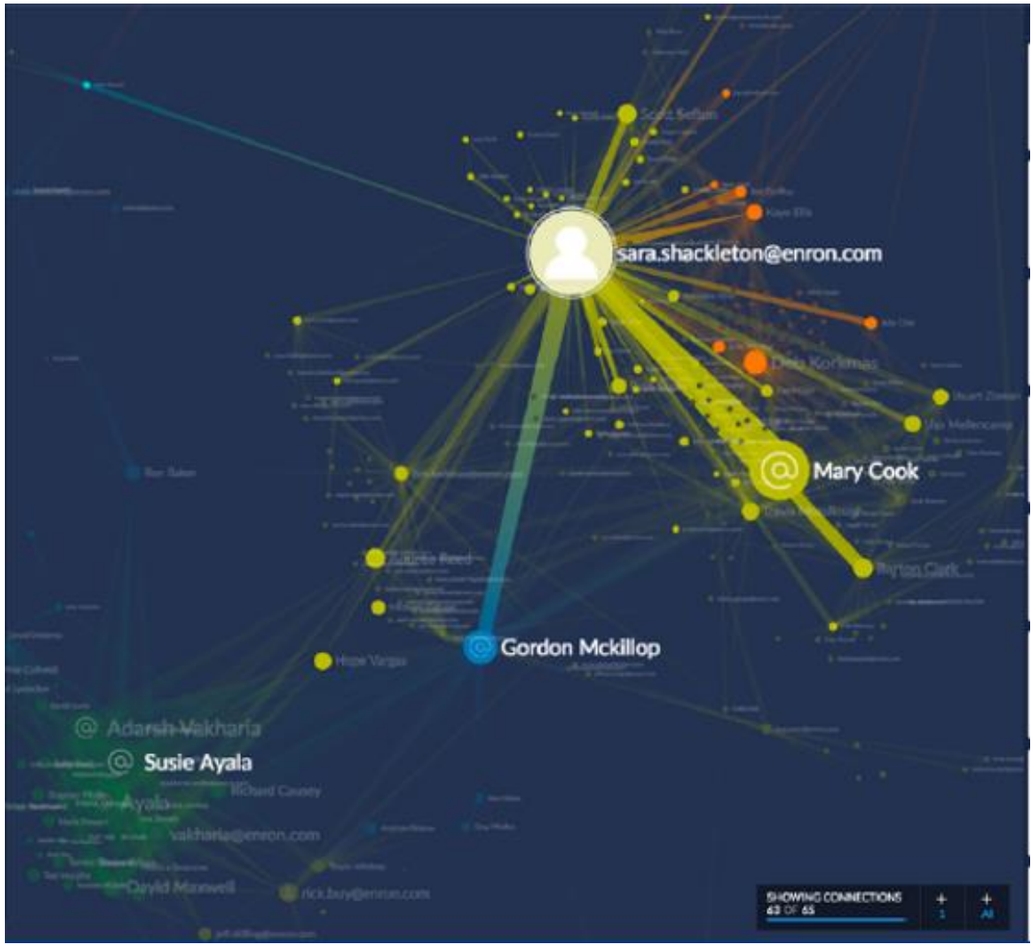
(Don't forget the attachment on the second email)

Analytics – Communications

Relativity

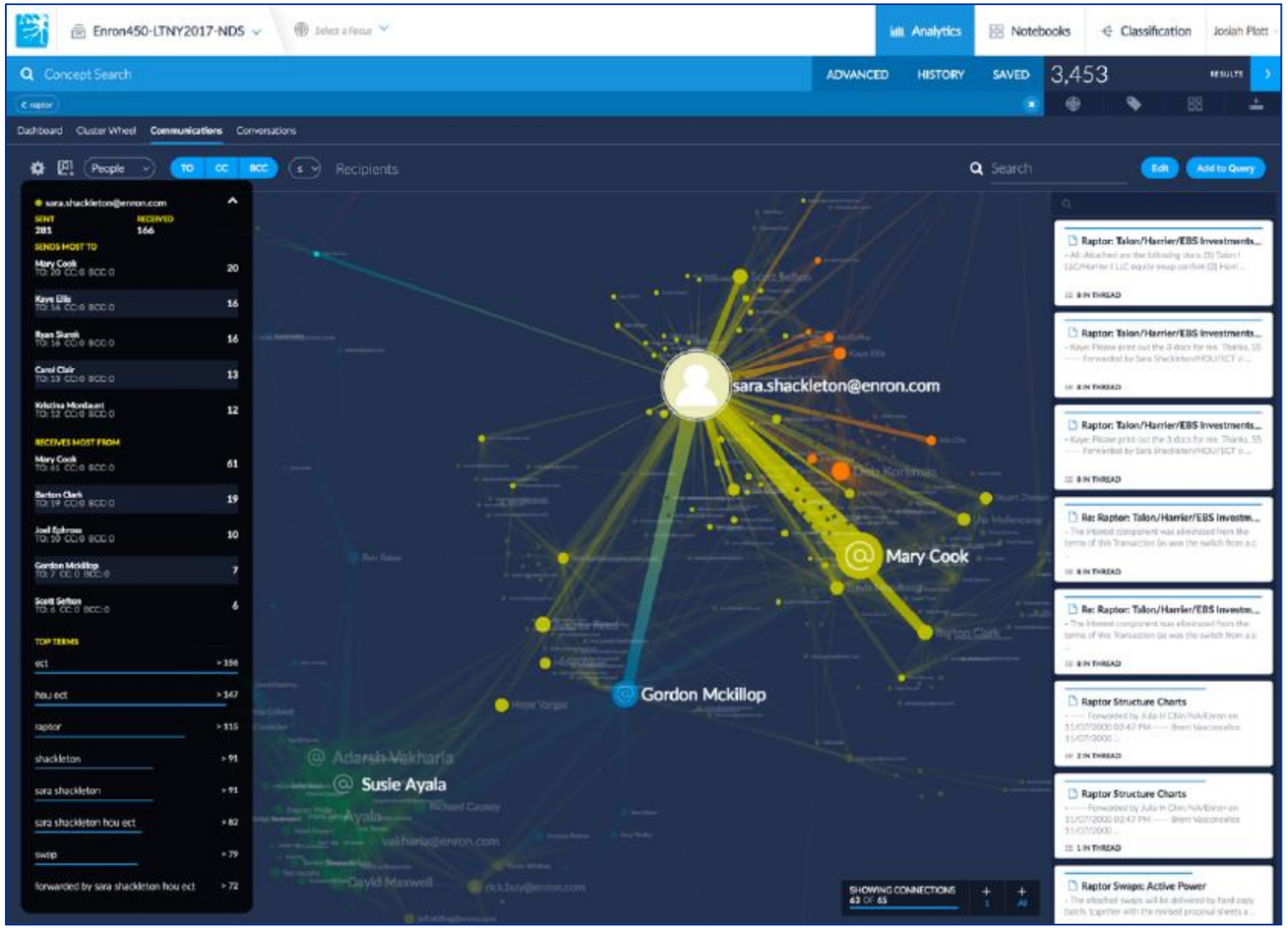


Brainspace™



Principais Ferramentas – Análise e Revisão

Tecnologia e IA para revisão de documentos

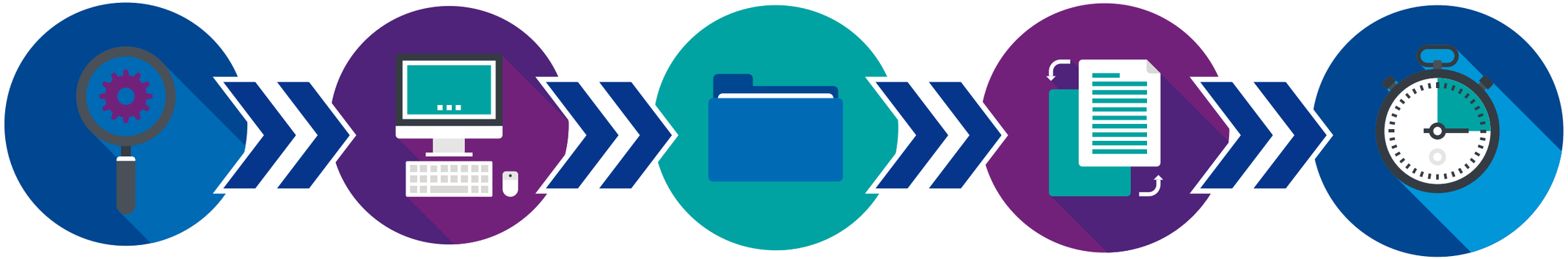


Um poderoso conjunto de **ferramentas de visualização interativas e de busca** para revelar a história por trás dos dados.

Aplicação de técnicas de machine learning para identificar documentos relevantes de maneira mais rapida.

Inteligência Artifical – Assisted Review

A codificação preditiva usa tecnologia de aprendizagem de máquinas para ajudá-lo a revisar menos documentos e diminuir seus custos associados. O uso do Continuous Multi-Modal Learning (CMML) ajuda a encontrar os documentos relevantes primeiro dando mais agilidade ao processo.



Busca conceitual ou keyword

Treino do modelo CMML

Documentos organizados por relevância

Treino continuo com base na revisão

Fluxo de revisão automatizado

Obrigado!