DOI: http://dx.doi.org/10.5769/C2011002

Um método para sistematização do processo investigatório de análise da informação digital

Fomentando a cognição na atividade policial

Levi Roberto Costa[1], and Hélvio Pereira Peixoto[2]
(1) Setor Técnico-Científico, Departamento de Polícia Federal, Rio de Janeiro, Brasil, costa.lrc@dpf.gov.br
(2) Diretoria Técnico-Científica, Departamento de Polícia Federal, Brasília, Brasil, peixoto.hpp@dpf.gov.br

***Abstract* — This paper presents a novel method for systematizing the investigation of digital information, seeking to accelerate criminal investigations in which a computer was used in an incidental manner; i. e., when a computer was used only to store electronic documents possibly related to the crime (similar to a physical filing cabinet that would contain documents, annotations, photos, etc.). It can also be used in criminal investigations where it was not possible to determine, at a glance, from the seized data storage items, which one(s) would have had a direct role as *corpus delicti* or were instrumental to the crime. The method also presents a digital document selection mechanism that enables an investigator to choose, between the seized items, the one(s) that might have something related to what is being investigated. Its main features and benefits include: give investigators quick access to digital data; reduces or eliminates the need for the forensic expert to know details and hypotheses of the investigations; capacity to processes big volumes of data and no need to discard information that appears irrelevant, since it might be important to another investigator at future time.**

Keywords — forensic analysis; information; electronic documents; automation; computer forensics; digital investigation; digital forensics.

***Resumo* — O artigo apresenta um método para sistematizar o processo investigatório da informação digital, visando tornar célere a apuração de delitos comuns cujo envolvimento de computadores se deu de forma incidental. Ou seja, quando computadores foram meros contentores de documentos eletrônicos possivelmente relacionados ao delito (por analogia, espécie de arquivos físicos que guardam documentos, anotações, fotografias etc.). O método, que se baseia em uma infra-estrutura de computadores, bases de dados, rede de comunicação, software e pessoas para alcançar os objetivos que propõe, também é aplicável em investigações criminais onde computadores tiveram um envolvimento direto no crime, como corpo de delito ou instrumento da prática delitiva, mas que, *a priori*, não foi possível aos investigadores identificar, com precisão, dentre outros materiais encontrados no local das diligências, quais seriam estes equipamentos. Sua adoção permite estabelecer uma sistemática de triagem em que policiais são capazes de apontar os materiais arrecadados que apresentem alguma relação com os fatos em apuração. Seus principais benefícios e funcionalidades incluem: - viabilizar o trabalho tradicional de investigação a partir de dados em formato digital - a objetividade do perito, que não deve ser exposto ao contexto das hipóteses da investigação - a evolução do conhecimento em ciclo - tratamento do grande volume sem exclusão de informação julgada irrelevante, visto que em outro momento essa informação pode vir a ser importante em fases futuras da investigação.**

Palavras-chave — análise forense; informação; documentos eletrônicos; automatização; forense computacional; digital; investigação digital; perícia de informática.

1. Introdução

Adquirir conhecimento oriundo de documentos eletrônicos[1] ganhou grande importância para a atividade policial no contexto da investigação criminal [2]. Esta modalidade de documento vem substituindo gradualmente os documentos tradicionais. Na Polícia Federal, por exemplo, a demanda cresceu vertiginosamente nos últimos anos:

> *"Anualmente são demandados exames periciais em mais de 6.000 discos rígidos e computadores apreendidos pela Polícia Federal. O volume de dados contidos nesse material é da ordem de 720 terabytes, o que corresponde a aproximadamente 36 vezes o conteúdo da maior biblioteca do mundo. Informações de vital importância para a investigação e persecução penal fazem parte dessa imensa massa de dados."* [4].

Embora os documentos armazenados em computadores possam ser relevantes para resolução de delitos, os investigadores se deparam com óbices para analisá-los livremente, tal como fariam no caso de uma caderneta de anotações ou um extrato bancário.

A natureza digital do documento eletrônico impõe certos cuidados para que seja mantido o valor probante da prova dele resultante [2]. Diferente do que ocorre comumente com documentos tradicionais - que podem ser tocados, lidos, analisados facilmente e ter suas alterações identificadas, por vezes, a olho nu - os documentos eletrônicos são latentes e intangíveis, e suas alterações podem ser indetectáveis em razão de sua natureza digital. Em virtude disso, os materiais são enviados a peritos criminais para que se preserve a

[1] O que se entende por documentos eletrônicos ou digitais são os arquivos produzidos por usuários de computadores de forma direta, como planilhas, vídeos, imagens, textos, apresentações e mensagens, e de forma indireta, como os arquivos temporários criados pelo uso da internet e aplicativos, por exemplo.

cadeia de custódia, requerendo que sejam analisados ou que tenham os documentos eletrônicos extraídos para posterior apresentação aos investigadores.

Surge, então, outra dificuldade. O grande volume de dados contidos nos materiais enviados aos peritos criminais requer um grande esforço e consome um tempo significativo para que se possa atender ao requisitado. "*As ferramentas disponíveis atualmente não permitem o tratamento eficiente desse volume de dados, tanto pela falta de recursos automáticos de busca e triagem, quanto pela falta de recursos de colaboração satisfatórios.*" [4].

Embora os problemas enumerados acima tenham potencial de impactar negativamente uma investigação criminal, ainda carecem de estudo no meio acadêmico [18, 19, 20].

Motivados em prover uma solução alternativa para os problemas supramencionados, os autores apresentam neste artigo um método para sistematização do processo investigatório de análise da informação digital. Os resultados são promissores e abrem caminho para uma discussão sobre novas alternativas de interação e integração entre a perícia criminal e a investigação envolvendo documentos eletrônicos.

O artigo foi assim estruturado: na próxima seção são abordados conceitos inerentes ao processo investigatório de análise de informações, enquanto na seção III é examinado o problema no trato com documentos eletrônicos em investigações criminais. Para ampliar a contextualização, a seção IV apresenta uma revisão bibliográfica acerca de requisitos de uma nova geração de ferramentas forenses. Na seção cinco são apresentadas uma sinopse do projeto de pesquisa em pauta e as características do método proposto. A seção VI apresenta a síntese do ferramental e seus principais componentes, seguida das seções VII e VIII que tratam, respectivamente, dos procedimentos propostos para o processo investigatório de análise da informação digital e para o processo pericial de extração e apresentação de documentos eletrônicos. A seção IX aborda a cognição na atividade de investigação criminal, demonstrando, graficamente, em quais etapas na geração de conhecimento e inteligência atuam cada um dos componentes da solução proposta. A seção X apresenta uma revisão bibliográfica de projetos relacionados. A seção onze apresenta experimentos, cujos resultados seguidos das conclusões estão na seção XII. Na seção XIII são apresentadas sugestões de trabalhos futuros.

2. O Processo Investigatório de Análise de Informações

O processo investigatório de análise de informações não se resume a uma simples análise isolada de conteúdo de documentos eletrônicos ou tradicionais, pois "*mesmo o mais simples dos casos demanda um exaustivo trabalho de busca, classificação e análise de informações das mais diversas fontes*" [3]. Pode ser então definido por intermédio de um ciclo composto das etapas de obtenção, reunião e análise de informação, mostrado na Fig. 1 [3].

Portanto, a simples coleta de dados ou informações não é suficiente para elucidar uma conduta criminosa [1]. Faz-se indispensável analisar e cruzar dados e informações para que se possa adquirir o conhecimento necessário à reunião de um conjunto robusto de provas que levem a elucidação do delito [1].

Uma investigação criminal exige "*um processo de transformação de grandes volumes de dados díspares em informações sintéticas e conclusivas*". [1]. Além disso, "*parece claro que a atividade de investigação e o seu sucesso dependem da capacidade do investigador de encontrar informações, saber reconhecer, entre tantas, quais as informações pertinentes, quais delas se erigem em indícios e quais se podem apresentar como provas judiciárias.*" [3].

A complexidade dos delitos contemporâneos exige uma ampla integração dos meios de prova. [1]. Sobretudo, um processo de análise de informações deve permear a investigação criminal. Cada novo conhecimento adquirido pode se constituir em peça fundamental para produção de novo conhecimento, até que se alcance a percepção da materialidade do delito e seja possível identificar a sua autoria e a provável dinâmica de perpetração da conduta [3].

Um processo de análise de informações tem por objetivo obter e aportar informações e conhecimento na investigação criminal, utilizando como veículos os relatórios de análise apresentados de forma sucessiva e complementar (relatórios parciais) [3]. Tais relatórios se destinam também a apresentar os pontos ainda não elucidados pela investigação: os ditos "vazios" de informação. Tais pontos obscuros devem ser objeto de novas diligências que aportem na investigação novas informações, que depois de cotejadas com o que se conhece, gerem novas conclusões. E assim por diante, até que se alcance o esclarecimento dos fatos (relatório final) [3].

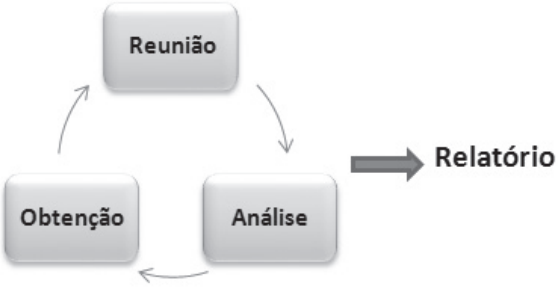

Figure 1. Diagrama do processo de análise – adaptado de [3].

Segundo Carlos Mariath [1], "*Vê-se, pois, que a investigação criminal afasta-se, hodiernamente, do modelo empírico-intuitivo de outrora e passa a ser concebida como um método científico por meio do qual o investigador depara-se com um problema (crime) e, a partir da observação e exame de dados e informações conhecidos (premissas), dá início a um processo de raciocínio que o conduzirá à formulação de suposições (hipóteses), as quais, depois de testadas (cotejadas com outros dados e informações), comprovadas ou não, resultarão em uma conclusão...*".

3. O Problema no Trato com documentos eletrônicos em investigações criminais

Nos casos em que as informações se derivam de documentos em formato digital, surgem substanciais diferenças no processo investigatório de análise da informação [2]. Tais diferenças se apresentam em relação à forma, o escopo, o alcance e até em relação ao papel de cada ator, pois as análises investigatórias de informações oriundas de documentos em formato digital acabam, em parte ou na totalidade de suas etapas, realizadas por peritos criminais, enquanto que as análises de informações oriundas de documentos em formato tradicional são realizadas por investigadores [2].

Em relação ao escopo, a análise de informações desempenhada por investigadores visa esclarecer a conduta investigada, utilizando-se de um ciclo – por vezes de longa duração, permeando a investigação – de busca, reunião e análise de informações [2,3]. Investigadores aduzem que conhecer profundamente um fato sob investigação é condição indispensável a dirimir coisa realmente relevante [3].

Quando as análises investigatórias são desempenhadas por peritos criminais, os trabalhos adquirem outro aspecto, pois visam responder às inquirições (quesitos) [2] com as informações disponíveis nos vestígios relacionados ao crime que se investiga. Nestes casos, em geral, os peritos não conhecem detalhes dos suspeitos investigados ou da conduta perpetrada. Algumas vezes, os quesitos são o primeiro e único contato que os peritos terão com o caso antes de iniciar os exames. Caso os quesitos não contemplem com exatidão as características[2] de apresentação dos documentos eletrônicos relevantes, há risco de que o trabalho pericial não revele de pronto todos os elementos necessários à elucidação do fato ou da conduta investigada.

Os peritos criminais produzem respostas objetivas às questões encaminhadas a eles [7]. Não apresentam, portanto, conjeturas por resultado de seus exames. Já os investigadores se utilizam de premissas para dar início a raciocínios que, por sua vez, resultarão na elaboração de suposições, as quais poderão ser refutadas ou comprovadas futuramente [1], seja por análises complementares em outros documentos, seja por laudos periciais criminais.

Em relação ao alcance, um processo de análise investigatória da informação deve abranger a totalidade do material arrecadado [2]. Assim, para que os documentos eletrônicos sejam examinados no processo de análise investigatória da informação, tem sido usual a requisição de perícias que apresentam quesitos que não conduzem "inquirições", apenas determinam a apresentação de documentos eletrônicos tipicamente produzidos por usuários de sistemas computacionais [2].

Outra maneira amplamente utilizada para aportar os documentos eletrônicos no processo de análise investigatória da informação é a definição, por intermédio de quesitos, de critérios a serem satisfeitos para que um documento seja ou não apresentado pelo perito criminal. Os documentos que satisfaçam aos critérios definidos, de acordo com um juízo de valor realizado pelo perito criminal, são apresentados. É muito usual que palavras-chave façam parte do rol de critérios elencados na requisição pericial [2].

As duas formas podem, em algumas circunstâncias, resultar em situações indesejáveis:

- A primeira, em virtude do grande volume de documentos eletrônicos, que armazenados em mídias óticas, aportam no processo de análise. Nesses casos, trabalhar com as mídias óticas, resultantes do processo pericial, tende a ser improdutivo, pois o volume de dados recebido pode tornar o trabalho de análises muito árduo ou até inviável;
- A segunda, por resultar no descarte prematuro de informações. Mesmo não tendo sido este o objetivo do investigador ao elaborar os critérios para seleção de documentos. Ao se definirem critérios objetivos para a apresentação, definem-se também critérios de exclusão. Por conseguinte, como os investigadores não terão mais, *a priori*, acesso aos demais documentos existentes no material arrecadado, também, de forma indireta, foram por eles definidas as regras que resultarão em descarte de documentos.

Segundo [3], durante uma investigação criminal, não cabe ao policial dispensar informações por julgá-las irrelevantes. Um dado ou informação aparentemente irrelevante ao longo de uma investigação, cruzado com outras informações obtidas posteriormente, pode vir a se tornar a peça que faltava para a elucidação do delito.

Acrescenta [3] que a dispensa de qualquer dado ou informação trata-se de erro grosseiro e irremediável. A relevância ou não do dado ou informação somente poderá ser aferida ao final dos trabalhos investigatórios, pois o que parece irrelevante no início ou no meio de uma investigação pode ser de grande importância ao final.

Por fim, em relação ao ator no processo de análise investigatória, cabe aos investigadores, os conhecedores dos fatos investigados, o papel de analista da informação [2], sujeito cognoscente que reúne as informações e constrói o conhecimento que leva a concluir pela tipicidade da conduta: o juízo de valor de tipicidade [3].

Quando as análises são realizadas por peritos criminais o desconhecimento de detalhes sobre o fato em apuração pode acarretar a não identificação de dados relevantes ao apuratório. Segundo [14], "*dados são interpretados individualmente, por essa razão o que se torna informação para um determinado sujeito cognoscente, pode não ter nenhum sentido para outro sujeito cognoscente*.".

4. Uma Nova Geração de Ferramentas Forenses

Pesquisadores têm debatido as características de uma nova geração de ferramentas forenses, que sejam capazes

[2] Critérios de relevância dos documentos para a equipe de investigação

de oferecer respostas mais eficientes para os novos desafios da computação forense na atualidade. Dentre os desafios frequentemente mencionados pelos pesquisadores estão o tratamento com grandes volumes de dados, as grandes quantidades de mídias de armazenamento de dados comumente envolvidas em processos investigatórios e a expansão da capacidade de armazenamento das mídias computacionais.

Segundo [18], as ferramentas forenses estão voltadas à identificação de evidências e deveriam ser repensadas para ajudar em investigações. O pesquisador aponta para uma iminente crise no campo da forense computacional e discute a necessidade de torná-la mais eficiente. Ele propõe uma nova direção do campo das pesquisas forenses computacionais, enfatizando, dentre outros pontos, a concepção de soluções que adotem arquiteturas modulares, modelos alternativos de análise, processamento paralelo e recursos de colaboração e automatização.

Na visão de [19], uma nova geração de ferramentas forenses deve prover capacidade de processamento paralelo e distribuído, automação e agendamento de processos. Deve ser construída segundo técnicas de engenharia de software que observem o problema principal e o decomponham em problemas mais simples, originando a construção de uma solução modular com entradas e saídas claramente definidas.

Na ótica de [20] uma alternativa para oferecer respostas ao grande volume de dados que frequentemente são submetidos a exames forenses computacionais é a adoção de métodos seletivos de coleta de dados. Outras soluções apresentadas para tornar mais eficiente o tratamento de grandes volumes de informação incluem processamento analítico distribuído, processos de buscas baseados em mineração de dados, classificação de arquivos para facilitar o processo de análise, e análise colaborativa geograficamente distribuída. Segundo o pesquisador as abordagens computacionais atuais para busca, recuperação e análise de evidências digitais são simplistas e fortemente dependentes do esforço de um investigador. As novas ferramentas devem prover soluções mais inteligentes, para melhoria tanto da eficiência quanto da efetividade do processo de análise, utilizando, por exemplo, algoritmos de mineração de dados que revelem tendências para dados e informações que seriam indetectáveis ou dificilmente percebidas somente por uma análise e observação humana, fazendo com que investigadores obtenham conhecimentos investigativos sem precedentes.

5. Características do Método Proposto

O método proposto é composto por um *Framework* para um ferramental forense especializado, um procedimento para o processo investigatório de análise da informação digital e um procedimento para o processo pericial de extração e apresentação de documentos eletrônicos. Ele visa sistematizar e, por consequência, tornar célere a apuração de delitos comuns cujo envolvimento de computadores se deu de forma incidental. Ou seja, quando computadores foram meros contentores de documentos eletrônicos possivelmente relacionados ao delito (por analogia, espécie de arquivos físicos que guardam documentos, anotações, fotografias etc.). É aplicável também em investigações criminais onde computadores tiveram um envolvimento direto no crime, como corpo de delito ou instrumento da prática delitiva, mas que, *a priori*, não foi possível aos investigadores identificar, com precisão, dentre outros materiais encontrados no local das diligências, quais seriam estes equipamentos. Sua adoção permite estabelecer uma sistemática de triagem em que policiais são capazes de apontar os materiais arrecadados que apresentem alguma relação com os fatos em apuração.

O método pode ser operacionalizado em um ferramental que considere características desejáveis em soluções para tratar problemas complexos e que envolvam grandes volumes de dados. Em particular, ele orienta o desenvolvimento de ferramentas que empreguem componentes[3] com as seguintes características:

- Decomposição do problema a ser resolvido – a análise investigatória pode ser decomposta em diversas dimensões (tipos de mídias, tipos de documentos, locais de arrecadação, especialidade e *skills* dos policiais envolvidos, etc.).
- Análise investigatória colaborativa - a análise investigatória pode ser realizada em equipe, composta, inclusive, por membros geograficamente distribuídos.
- Componentes autônomos e especializados – visando paralelismo e eficiência, um conjunto de componentes (ou agentes) especializados que trabalham sem supervisão ou dependência dos demais. Componentes podem ser substituídos por outros componentes, sem que ocorra impacto ao restante do ferramental. Novos componentes, especializados na busca de informações ou no tratamento de diferentes tipos de documentos eletrônicos, podem ser agregados ao ferramental a qualquer momento sem impactar o trabalho desenvolvido pelos demais. Embora os componentes sejam, em geral, sistemas computacionais, nada impede que ações sejam realizadas por componentes humanos. Em sendo componentes computacionais, é possível também a utilização de diversos tipos de sistemas computacionais (desenvolvidos em diferentes linguagens de programação e que executem em diferentes plataformas computacionais), desde que respeitem as regras de interface nos repositórios de dados.
- Interação assíncrona entre os componentes – Por serem autônomos e efetuarem interações entre si de forma assíncrona, não existem restrições na ordem das interações entre os componentes, que podem trabalhar paralelamente, cada um em sua capacidade ou velocidade máxima.

3 Entenda-se por componentes qualquer agente humano ou construído em *software*, *hardware* ou uma combinação deles, com um propósito ou conjunto de propósitos definido.

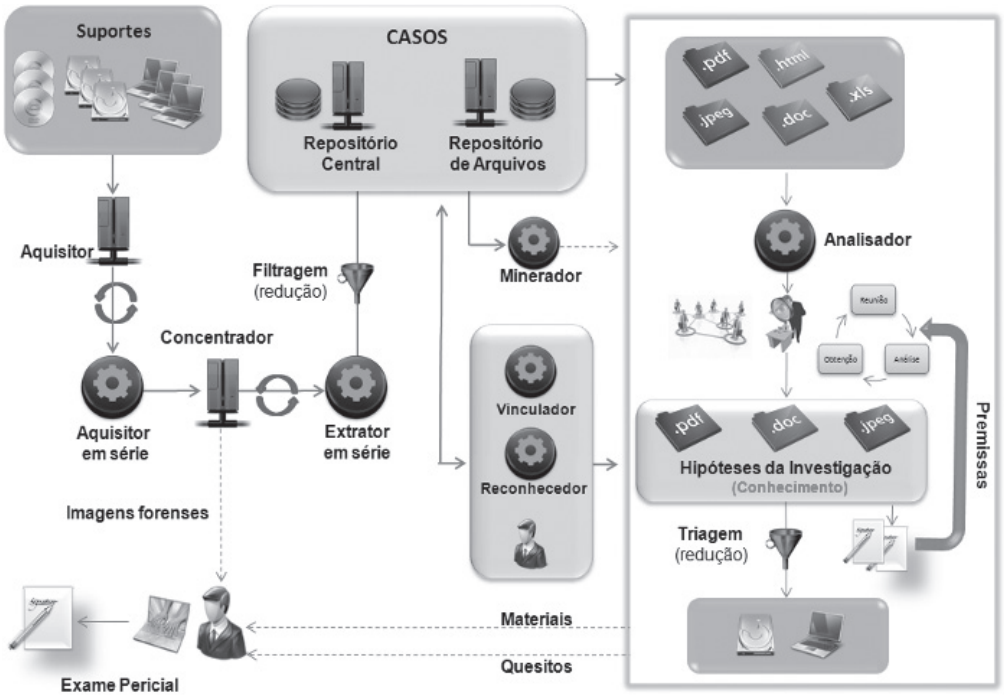

Figure 2. Diagrama geral do ferramental

- Recursos automáticos de busca - visando descobrir arquivos conhecidos, arquivos com certas características e conexões entre alvos ou casos.
- Aquisição e compartilhamento de conhecimento - visando a ampliação da aquisição de conhecimento na investigação, transformando o conhecimento tácito do analista em explícito da investigação policial.

6. O Framework e Seus Principais Componentes.

Resumido graficamente na Fig. 2, o *Framework* visa tornar ágil a aquisição, a extração de documentos eletrônicos, a análise e a correlação de vestígios em grandes volumes de dados e de mídias digitais, colaborando na busca pela excelência na produção de provas e na apuração de delitos. Ele consiste em um conjunto de componentes autônomos e assíncronos, cada um atuando numa atividade específica do processo de extração de vestígios digitais e da sistematização do processo investigatório de análise da informação digital, por meio de interfaces simples e conhecidas da Perícia Criminal: contêiner de fotografia ou ilustrações, contêiner de documentos eletrônicos, contêiner de resultados de buscas, além de outros.

A. O componente autônomo aquisitor de imagens forenses

O componente aquisitor foi projetado para sistematizar e permitir a automatização da criação de imagens forenses. Ele opera de forma autônoma e assíncrona em relação ao demais componentes da solução (veja Fig. 3).

O componente foi concebido para suportar, de uma só vez, o oferecimento de vários suportes (múltiplas mídias alvos da investigação) para o processo pericial de preservação e produção de imagens forenses. Após a alimentação dos compartimentos de mídias e ativado o processo aquisitor, o componente funciona de forma autônoma, minimizando a intervenção humana para substituição de mídias questionadas, reduzindo períodos de ociosidade computacional e maximizando a capacidade produtiva da equipe pericial responsável pelo processo de verificação da integridade das cópias produzidas.

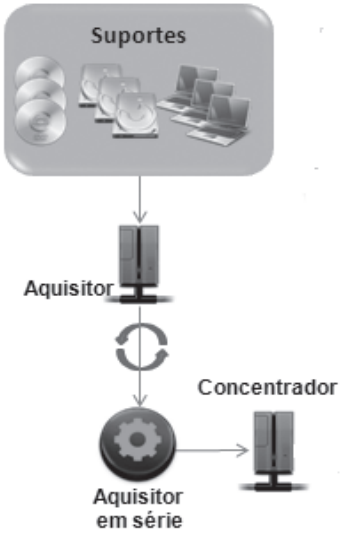

Figure 3. Diagrama do componente aquisitor

Diversos componentes aquisitores podem trabalhar simultaneamente e de forma assíncrona. Quanto maior o número de componentes operando simultaneamente, maior será a capacidade produtiva. Por exemplo, um grupo aquisitor

composto de dez componentes aquisitores - cada qual com 10 compartimentos de disco - e um componente concentrador é capaz de processar até cem materiais diferentes com mínima intervenção. A qualquer momento, 10 materiais estarão sendo processados simultaneamente e independentemente. Uma segunda alternativa de configuração está em dividir o grupo de dez aquisitores, utilizados no exemplo anterior, em 5 grupos composto cada um por 2 aquisitores e 1 componente concentrador e extrator. Neste caso, distribui-se a E/S, a carga de transmissão de dados e de processamento entre os 5 componentes concentradores e extratores, maximizando a produtividade.

No processo de aquisição, cabe ao Perito Criminal validar e certificar a integridade dos suportes (das mídias) e das imagens forenses geradas pelo componente aquisitor.

O componente extrator, que será descrito à frente, inicia um novo processo de extração tão logo uma nova imagem forense esteja concluída e haja disponibilidade computacional no componente para processá-la. Portanto, aquisitores e extratores podem trabalhar paralelamente para aumentar a capacidade produtiva.

B. O componente concentrador de imagens forenses

O componente concentrador, exemplificado na Fig. 4, possui duas funções essenciais:

- Fornecer um repositório onde os componentes aquisitores armazenam as imagens forenses.
- Fornecer recursos de processamento para o componente autônomo extrator de documentos eletrônicos.

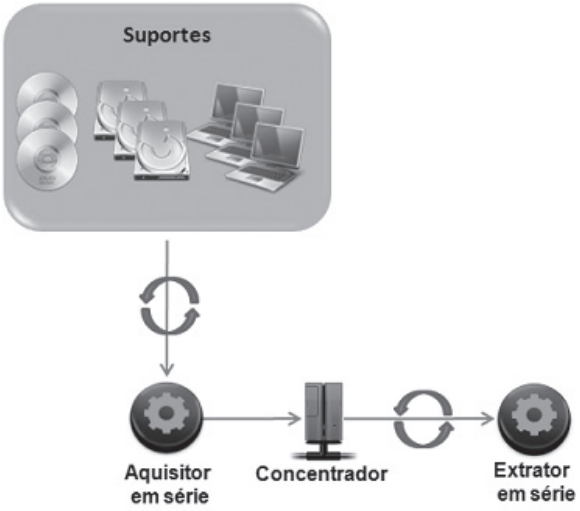

Figure 4. Diagrama do componente concentrador de imagens

Um componente extrator se utiliza dos recursos de processamento do componente concentrador para operar a extração e o processamento de documentos eletrônicos contidos nas imagens forenses disponibilizadas. Um exemplo de processamento seria apartar os arquivos irrelevantes para o processo de análise da informação digital dos demais produzidos por ação de um usuário do ambiente computacional, por não se classificarem por documentos eletrônicos (como por exemplo, arquivos comuns de programas e sistemas operacionais).

As imagens forenses processadas pelo componente extrator podem ser descartadas ao fim do processo de extração, caso seja necessário, em decorrência da carência de recursos computacionais de armazenamento.

C. O componente autônomo extrator de documentos eletrônicos

O componente extrator trabalha de forma autônoma e assíncrona extraindo documentos eletrônicos de imagens forenses. Para que um componente extrator possa iniciar suas atividades, basta que uma nova imagem forense esteja disponível no concentrador, conforme ilustrado na Fig. 5.

Diversos componentes extratores podem trabalhar simultaneamente de forma independente. Quanto maior o número de componentes extratores, maior será a capacidade produtiva. Enfatiza-se que o componente extrator também é capaz de trabalhar com aquisitores de diferentes tipos de imagens forenses, como, por exemplo, aquelas geradas por dispositivos dos tipos *Talon* e *Dossier* da *Logicube Corp* [22]. Desta forma, uma estação de trabalho combinada a um aquisitor especialista pode substituir os componentes aquisitor e concentrador, para que a solução se adapte e passe a trabalhar sob outra arquitetura. Inclusive, a arquitetura baseada em aquisitores e concentradores pode trabalhar de forma concomitante com uma arquitetura baseada em aquisitor especialista.

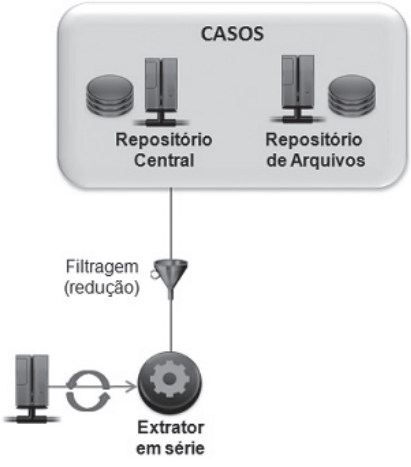

Figure 5. Diagrama do componente extrator

Uma vez extraídos, os documentos eletrônicos podem ser analisados de imediato pela equipe de investigação. Contudo, o ferramental só será capaz de executar buscas textuais ou semânticas após o término de um processo de indexação. Pode-se optar por trabalhar com indexações parciais, mas a equipe de investigação deve estar atenta para o fato de que a capacidade de minerar dados textuais estará limitada apenas aos documentos conhecidos até um determinado momento e que as buscas realizadas ficarão desatualizadas tão logo novos

materiais em processamento passem pelos componentes aquisitores e extratores.

D. O componente de gerenciamento de investigações

O método proposto organiza investigações em casos. O caso é um contêiner lógico que organiza os demais elementos da investigação. Os diversos elementos que compõem um caso não se misturam aos elementos de outro caso. Por exemplo, documentos eletrônicos de uma investigação permanecem isolados de documentos de outra investigação. Da mesma forma, investigadores membros de equipe de análise de um caso específico não possuirão acesso a elementos de outro caso em que não participam como membro de equipe de análise.

Caso se julgue necessário, logo após as extrações, ou a qualquer tempo, poderão ser emitidos relatórios de extração de dados com base em modelos de documentos[4]. Ao gerador de relatórios poder-se-á determinar a elaboração de imagem de disco ótico contendo os arquivos extraídos de cada material arrecadado ou de um grupo deles, agrupando os arquivos, se desejado, em categorias diversas.

Os principais elementos de um caso são:

1) *Analista:* Investigadores que utilizam o sistema para obter acesso a documentos eletrônicos extraídos de materiais arrecadados.
2) *Equipe de análise:* Usuários investigadores autorizados a participar do ciclo de análise de informações de um caso.
3) *Documentos / Referências:* São relatório associados ao material questionado. A relação entre materiais e relatórios (documentos) não é obrigatória, surgem nos casos em que são elaboradas referências externas aos documentos eletrônicos existentes no sistema.
4) *Metadados:* São dados que descrevem um determinado documento eletrônico extraído de seu suporte, como por exemplo, nome, autor, e datas de criação e modificação.
5) *Artefatos:* Representam os documentos eletrônicos, propriamente ditos, extraídos de seus suportes.
6) *Premissas:* São proposições que devem ser investigadas para alcançar uma conclusão. Premissas dão origem aos termos de buscas.
7) *Termos de buscas:* São palavras-chave ou conceitos utilizados para procurar documentos eletrônicos.
8) *Resultados de buscas:* São contêineres lógicos que organizam os documentos eletrônicos resultantes de pesquisas por fragmentos textuais.
9) *Árvore de diretórios ou estrutura de pasta e subpastas:* São contêineres lógicos que organizam os documentos eletrônicos resultantes de suportes.
10) *Repositório de arquivos em formato gráfico:* São contêineres lógicos que organizam fotografias e outros arquivos gráficos, resultantes de suportes.
11) *Hipóteses:* São contêineres lógicos que organizam os documentos eletrônicos inicialmente considerados relevantes pelos investigadores, a fim de que, posteriormente, as hipóteses formuladas sejam testadas, cotejadas com outras informações e dados, e se chegue a conclusões.
12) *Dossiê:* São contêineres lógicos que reúnem as diversas hipóteses de um caso.

E. O componente de mineração de dados

O componente de mineração de dados funciona de forma independente e assíncrona em relação ao demais componentes da solução. Ele opera na retaguarda do ferramental e é composto por três módulos: o módulo indexador, o módulo de buscas por fragmentos de texto e o módulo de buscas semânticas. Cada um dos módulos opera de forma assíncrona e independente, um em relação ao outro.

O módulo indexador é o responsável pela indexação de conteúdo de documentos eletrônicos e os módulos de buscas textuais e semânticas são responsáveis pelo atendimento às requisições de buscas solicitadas por intermédio do componente de análise investigatória da informação.

Diversos processos de indexação podem executar simultaneamente, de forma independente. Os índices podem ser gerados para todo um caso ou atualizados a cada conjunto de documentos eletrônicos que aporte no caso (conjunto de documentos originários de um mesmo material arrecadado).

Os índices gerados durante o processo de indexação são armazenados em um banco de dados e são utilizados, posteriormente, em minerações de dados associadas às buscas comandadas pelos investigadores. Cada caso possui seu próprio banco de dados de índices, o que garante que as buscas de um caso não apresentem por resposta os documentos de outro caso.

A arquitetura do componente de mineração de dados pode ser estendida com relativa facilidade para trabalhar com novos formatos de arquivos. Baseado em tecnologia madura e testada com milhões de documentos e volumes de dados na escala dos *terabytes*, é projetado para oferecer alto desempenho de busca mesmo quando utilizado com *hardware* modesto.

O ferramental pode ser estruturado com diversos computadores que operem os componentes contêineres de arquivos, indexação e mineração de dados, para aumentar a capacidade de processamento, armazenamento de dados e distribuição de processos.

O componente minerador de dados se utiliza dos recursos de processamento do componente repositório de arquivos para operar indexações e buscas.

[4] Um modelo de documento é uma matriz que orienta a construção de relatórios quanto à sua forma ou aparência final.

F. O componente vinculador

O componente vinculador foi concebido para operar de forma independente e assíncrona em relação ao demais componentes da solução, conforme a Fig. 6. Ele atua na retaguarda do ferramental descobrindo e apontando possíveis conexões entre alvos. Conexões estas que poderiam passar despercebidas, ocultas por um grande volume de dados.

Segundo [21], a *análise de vínculo "pode ser considerada uma técnica de mineração de dados na qual é possível estabelecer conexões entre registros com o propósito de desenvolver modelos baseados em padrões de relações."*.

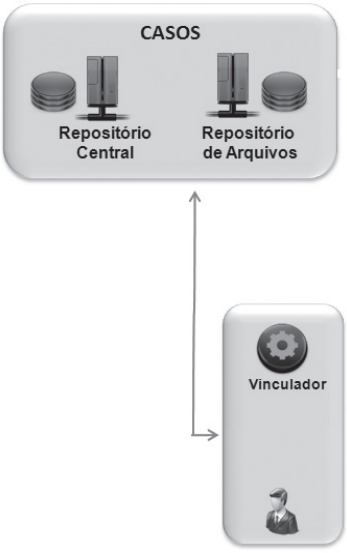

Figure 6. Diagrama do componente vinculador

Para descobrir vínculos o componente trabalha com classes de dados e informações predeterminadas ou descobertas com base em dados do caso. Estão relacionadas a seguir, como exemplo, algumas classes básicas de dados:

1) *Endereços de email:* São dados de endereçamento de arquivos (remetentes ou destinatários) utilizados para cruzar informações e descobrir conexões com base em mensagens trocadas entre comunicantes.
2) *Alvo:* São dados de pessoas ou empresas utilizados para cruzar informações e descobrir conexões com base nos dados dos próprios alvos.
3) *Arquivo:* São valores referenciais calculados, com base no conteúdo de arquivos, utilizados para cruzar informações e descobrir conexões entre pessoas ou empresas investigadas.
4) *Metadados de arquivo:* São dados de arquivos (editor, data de edição etc.) utilizados para cruzar informações e descobrir conexões entre pessoas ou empresas investigadas.

O componente foi concebido para também operar em um modelo complexo, envolvendo múltiplos casos, descobrindo e apontando a existência de possíveis vínculos entre alvos e investigações sem violar o sigilo da informação pela divulgação não autorizada de dados ou informações.

G. O componente Reconhecedor

O componente reconhecedor funciona de forma independente e assíncrona em relação ao demais componentes da solução. Ele opera na retaguarda do ferramental e possui por função reconhecer e apontar arquivos que apresentem padrões conhecidos, conforme a Fig. 7.

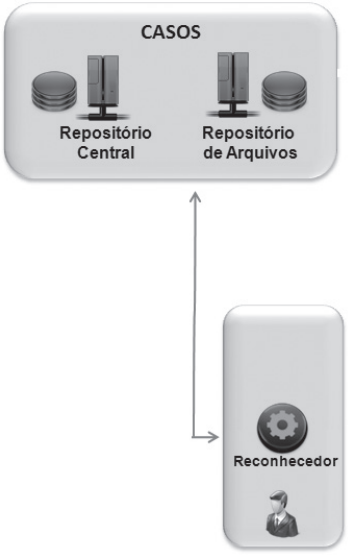

Figure 7. Diagrama do componente reconhecedor

O reconhecimento de arquivos pode ser realizado, por exemplo, a partir de uma análise de padrão do conteúdo do próprio arquivo – combinando a existência de palavras-chaves em certas posições do texto - ou mesmo a partir de um banco de dados de arquivos conhecidos.

H. O componente repositório de arquivos

O componente repositório de arquivos possui as seguintes funções essenciais:

- Fornecer um repositório onde os componentes extratores armazenam os documentos eletrônicos extraídos de materiais arrecadados.
- Prover um serviço de comunicação (*web service*) entre o componente repositório de arquivos e o componente de análise investigatória da informação. Ele intermedia o acesso restrito (*download de arquivos)* aos documentos eletrônicos de um caso. Somente investigadores membros da equipe de análise devem ter acesso aos documentos.
- Fornecer recursos de processamento para o componente de mineração de dados.

I. O componente repositório central

O componente repositório central possui as seguintes funções essenciais:

- Armazenar os metadados de documentos eletrônicos de cada caso, dados de auditoria e outros dados de gestão do ferramental.

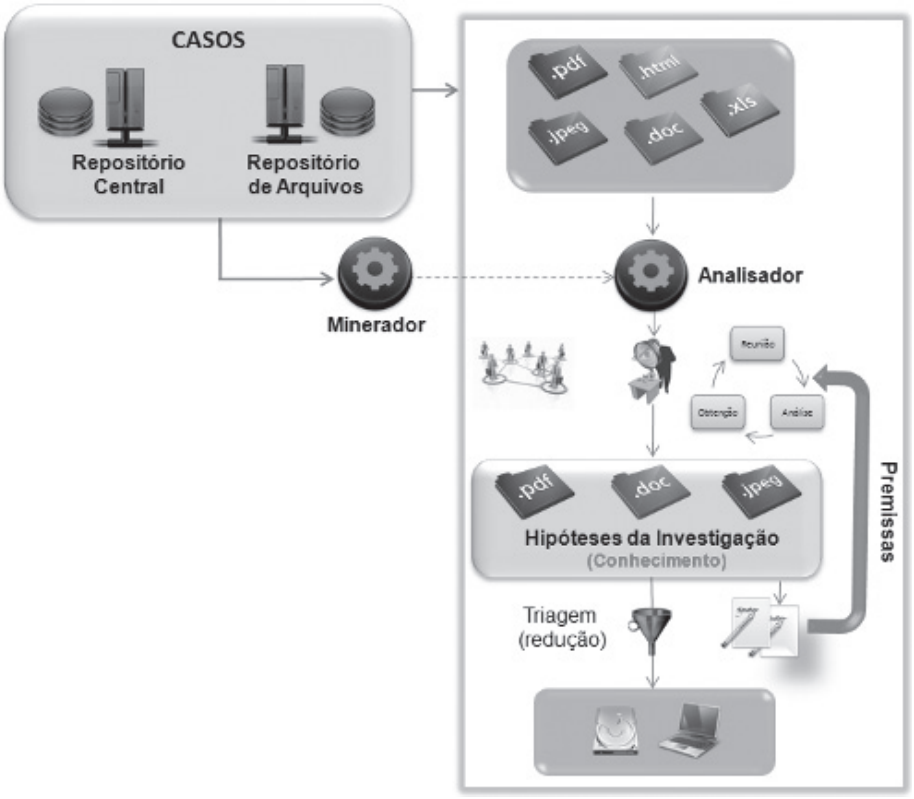

Figure 8. Diagrama do componente de análise

- Fornecer recursos de processamento (servidor *web*) para o componente de análise investigatória da informação.

J. O componente de análise investigatória da informação

O componente de análise investigatória de informação, representado na Fig. 8, foi desenvolvido para minorar as diferenças apontadas no método utilizado para trabalhar com a informação em formato tradicional e digital.

Entre outros objetivos, busca-se que investigadores realizem as análises de documentos tradicionais e eletrônicos, de maneira integrada, complementar e simultânea, para fomentar a cognição, a partir destas fontes de dados, na atividade policial.

Antes de dar início ao processo de análise, os investigadores poderão preparar e operacionalizar ações a fim de que possam ter disponíveis, concomitantemente, os documentos tradicionais arrecadados e todos aqueles em formato digital que puderam ser extraídos do material computacional apreendido.

Desta forma, os insumos necessários ao desempenho dos trabalhos estarão à disposição para início do ciclo de análises. As análises de documentos eletrônicos permearão a investigação criminal pelo tempo necessário à condução do apuratório.

O componente de análises é disponibilizado por meio de uma interface *Web* em rede privada. Ele permite a formação de equipes de análises pela adição de investigadores a um caso. Os investigadores trabalharão de forma colaborativa, efetuando análises de documentos eletrônicos, mesmo se estiverem geograficamente dispersos, em prédios, cidades ou até estados diferentes.

Embora um investigador possa fazer parte de diversas equipes e o componente permita a existência concomitante de múltiplos casos, ao acessar o ferramental ele deverá optar dentre os casos que participa aquele em que deseja trabalhar. A qualquer momento, o investigador deve poder alternar de um caso para outro.

O componente de análise se utiliza do componente de mineração de dados para alcançar a capacidade de efetuar buscas avançadas por palavras-chave combinadas com outros critérios (como combinação lógica e tipologia de artefatos). As buscas são realizadas, ao mesmo tempo, em todos os documentos eletrônicos extraídos de todos os materiais arrecadados, e assim confere agilidade à geração de conhecimento no apuratório.

Durante as análises os investigadores poderão relacionar seus achados em contêineres lógicos de hipóteses, fazendo anotações e outros metadados associados, explicitando e compartilhando o conhecimento entre os membros de sua equipe de análises. Dessa forma, o conhecimento tácito dos investigadores se transforma em conhecimento explícito do órgão policial e permite que novos investigadores sejam integrados à equipe de análise com rapidez e eficiência.

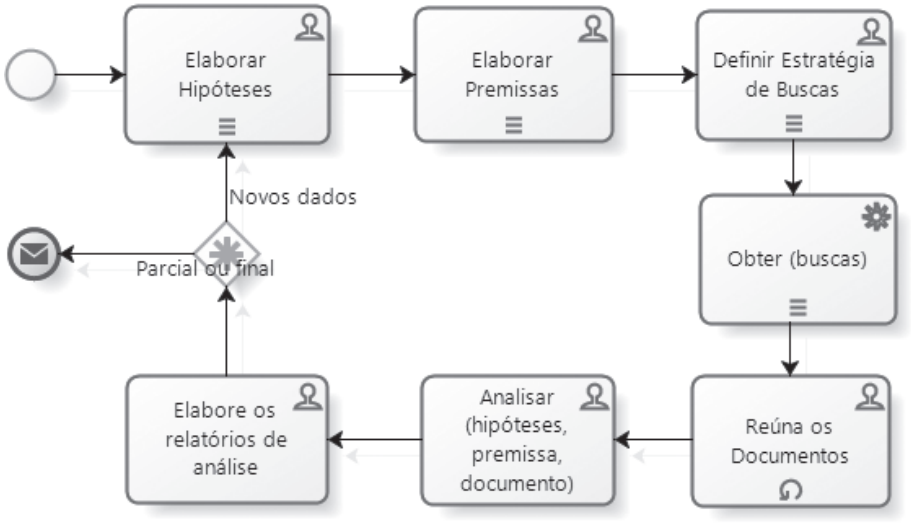

Figure 9. Procedimento para o processo investigatório de análise da informação digital

7. O Procedimento para o Processo Investigatório de Análise de Informações Digitais.

Um procedimento para o processo investigatório de análise de informações digitais foi concebido, e está ilustrado na Fig. 9. Composto por sete passos ele apresenta as etapas de alto nível sugeridas para a execução do trabalho de análise de documentos eletrônicos em investigações criminais.

Para realizar a análise de informações digitais combina-se a adoção do procedimento para o processo investigatório de análise de informações digitais e o uso do componente de análise investigatória de informação.

Antes, porém, para que investigadores obtenham acesso ao conteúdo do material arrecadado, algumas ações devem ser levadas a cabo seguindo certas formalidades e exigências da persecução penal, visando, entre outras coisas, a manutenção do valor probante da prova resultante do processo de análises.

Assim, para que os documentos eletrônicos possam ser disponibilizados para os investigadores, é necessário o envio formal do material apreendido a uma unidade de Perícia Oficial, que procederá aos trabalhos periciais relativos à extração do conteúdo do material arrecadado. Para desempenhar esta tarefa os peritos se utilizarão dos demais componentes do ferramental, de uso típico da função pericial. Este trabalho visa à garantia da cadeia de custódia de provas, a integridade e autenticidade dos documentos eletrônicos repassados à equipe de investigação e à Justiça.

O trabalho de peritos criminais conferirá os elementos que permitirão assegurar verificações futuras da integridade de cada documento em relação à sua fonte e a autenticidade em relação à sua origem, que em conjunto com a cadeia de custódia, poderão ser úteis em contendas relacionadas a repúdios futuros por parte de investigados.

De forma resumida, o procedimento assim estrutura as análises investigatórias:

1) *Elaborar hipóteses:* Elabore as hipóteses que orientarão a investigação na busca por documentos que conduzam informações relevantes ao apuratório.

As hipóteses irão antecipar, por deduções ou conjeturas, certas características da conduta investigada. Por exemplo: uma hipótese do tipo "Tício participa da intermediação fraudulenta de benefícios previdenciários" ou "Tício gerencia os "laranjas" que participam do esquema." Irá orientar que se estabeleçam premissas que permitam encontrar documentos que apontem para os fatos investigados.

2) *Elaborar premissas:* Defina proposições, possíveis fatos ou princípios que permitam planejar os argumentos de buscas por informações.

Utilizando-se das hipóteses exemplificadas no passo anterior, as premissas a serem estabelecidas poderiam ser: "Tício *acessa o sítio da Previdência para agendar atendimentos para "*Mércio*", um dos "laranjas" da fraude*", "Tício *possui conexões (vínculos) com outros alvos investigados, trocou mensagens, participa de contratos etc.*", por exemplo.

3) *Definir estratégia de buscas:* Defina a estra*tégia de* buscas a ser utilizada ("buscas textuais", "buscas semânticas", "buscas em pastas" ou "buscas por fotografias, figuras ou outros arquivos gráficos").
4) *Obter (buscas):* Organize e comande a execução de buscas, utilizando-se das hipóteses, das premissas estabelecidas, dos termos de buscas e das técnicas escolhidas. Optando pelo uso do recurso de buscas textuais, os termos de pesquisa poderiam conter os seguintes fragmentos de texto:
   a) O endereco do sítio da previdência e dados da página de agendamento.
   b) Dados de laranjas conhecidos (Mércio) e endereco do sítio da previdência.
   c) O endereço de email de alvos.

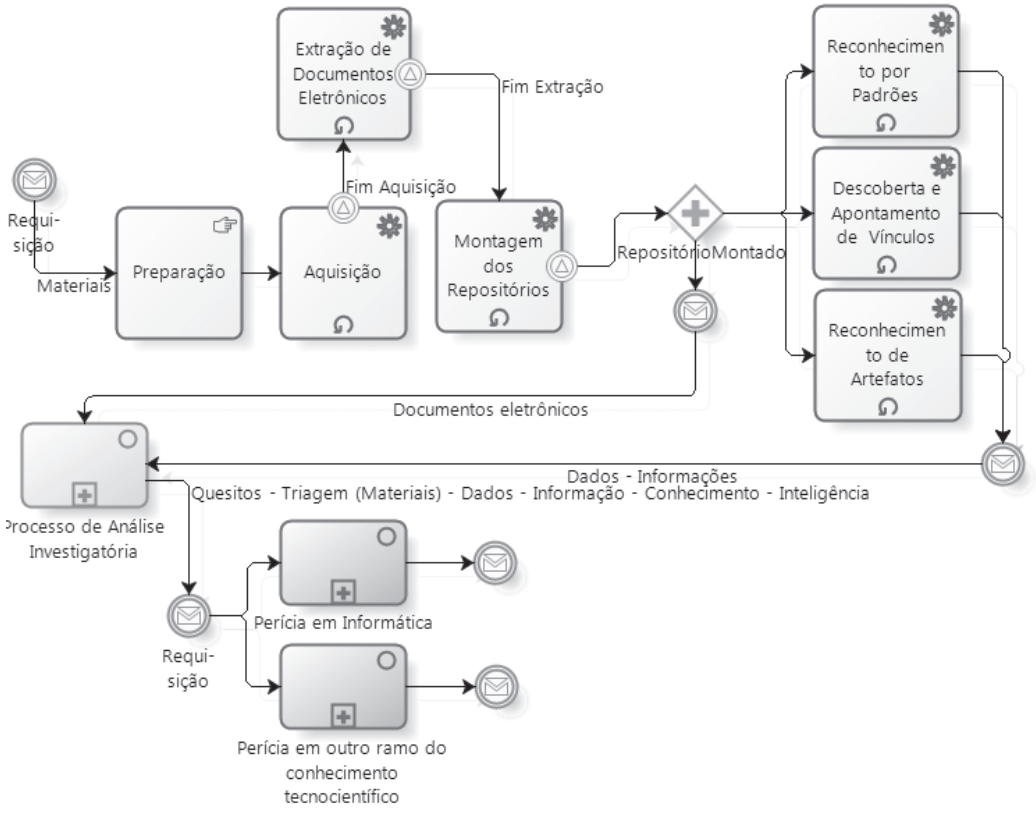

Figure 10. Procedimento forense computacional

d) Dados conhecidos por intermédio de escutas telefônicas ou de oitivas relacionado ao Tício.
e) Dados obtidos de documentos tradicionais já analisados e considerados relevantes
f) As palavras-chave "contrato", " Tício" e "Mércio".

5) *Reunir os documentos:* Organize as análise de conteúdos dos resultados das buscas, estruture as equipes de buscas e distribua os trabalhos de análise entre os investigadores, de acordo com a técnica ou técnicas de busca escolhidas. Inicie as análises dos resultados de buscas e/ou de contêineres de buscas em pasta ou buscas por fotografias ou outros arquivos em formato gráfico. Adicione os documentos encontrados aos contêineres de hipóteses correspondentes. Documente os conhecimentos adquiridos, retroalimentando o processo de buscas por documentos relevantes.
6) *Analisar (hipóteses, premissas e documentos):* Analise o conhecimento reunido nos contêineres de hipóteses, forme conclusões possíveis.
7) *Elaborar relatórios:* Caso exista um conhecimento formado, elabore o relatório de análise para aportar os resultados do processo investigatório de análise na investigação criminal. Avalie se o conhecimento adquirido sugere a elaboração de novas premissas ou novas hipóteses, retome as análises ou conclua os trabalhos.

Ao final dos trabalhos de análise ou mesmo durante o andamento destes, pode ocorrer necessidade de perícias em informática ou em outro ramo das ciências forenses, como contabilidade, por exemplo. Caberá aos investigadores formular os quesitos e encaminhar a requisição de perícia para exame específico.

8. O Procedimento para o processo pericial de extração e apresentação de documentos eletrônicos

Um procedimento forense computacional integrado ao procedimento para o processo investigatório de análise de informações digitais foi concebido (Fig. 10). Composto por onze passos, ele apresenta as etapas de alto nível sugeridas para a execução do trabalho pericial que antecedem os trabalhos de análise investigatória da informação.

De forma resumida, o procedimento forense computacional assim estrutura os trabalhos periciais:

1) *Preparação:* Reunir os materiais que terão o conteúdo extraído.
2) *Aquisição:* Montar os materiais nos copiadores forenses. As imagens forenses serão executadas automaticamente. Os resultados desta etapa deverão ser certificados pelo perito criminal responsável.
3) *Extração de documentos eletrônicos:* As extrações serão executadas automaticamente. Os resultados desta etapa deverão ser certificados pelo perito criminal responsável.

4) *Montagem dos repositórios:* As montagens de repositórios serão executadas automaticamente. Os resultados desta etapa deverão ser certificados pelo perito criminal responsável.
5) *Reconhecimento por padrões:* As análises de padrões serão executadas automaticamente, de acordo com os padrões conhecidos pela solução forense. Os resultados desta etapa deverão ser certificados pelo perito criminal responsável e disponibilizados à equipe de investigação.
6) *Descoberta e apontamento de vínculos:* A descoberta e apontamento de vínculos entre alvos (intracasos e extracasos) serão executadas automaticamente, de acordo com os padrões conhecidos pela solução forense. Os resultados desta etapa deverão ser certificados pelo perito criminal responsável e disponibilizados à equipe de investigação.
7) *Reconhecimento de arquivos:* As análises de arquivos conhecidos serão executados automaticamente, de acordo com os padrões conhecidos pela solução forense. Os resultados desta etapa deverão ser validados posteriormente.

9. A Cognição da atividade de investigação policial.

"A investigação policial é, em última análise, uma paciente coleta de informações" [3]. O investigador, como agente cognoscente do processo investigatório de análise da informação, necessita conhecer dados referentes ao caso em concreto para que - após analisá-los, relacionando-os ao caso em apuração - possa atribuir a eles algum significado, conferindo-os condição de informação.

Posteriormente, de acordo com um contexto, considerando as experiências e percepções do agente cognoscente, a informação, depois de submetida a um processo de validação[5], é elevada à condição de conhecimento [14].

Segundo [14], "*o sujeito cognoscente passa a ser o elemento fundamental desse processo, qual seja, de transformar dados em informação e informação em conhecimento.*". Sobretudo, segundo [17], "*A informação dispersa não constitui inteligência. A partir da estruturação da informação é que a inteligência passa a existir*".

O método proposto promove a cognição na investigação criminal utilizando-se de mecanismos que fomentam a geração do conhecimento e inteligência no apuratório. A Fig. 11 demonstra, por intermédio das etapas de geração de conhecimento e inteligência, onde se inserem os componentes da solução proposta.

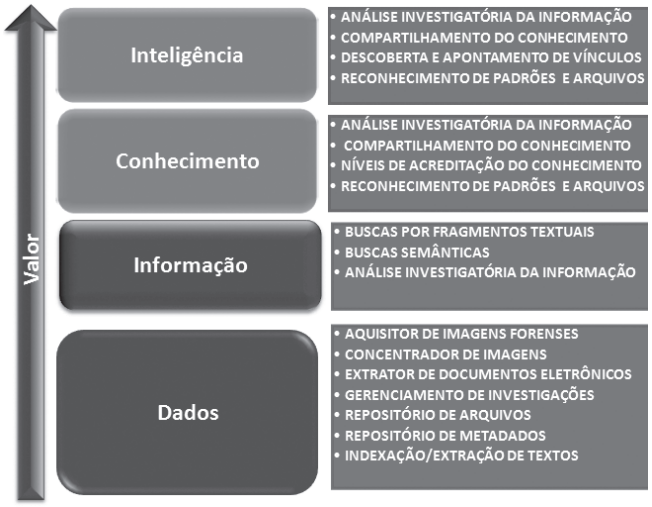

Figure 11. Etapas na geração de conhecimento e inteligência, adaptado de [17]

Para classificação em etapas de geração do conhecimento e inteligência, foram utilizados os conceitos abaixo:

1) *Dados :* Elemento da informação, "*uma seqüência de números e palavras, sob nenhum contexto específico*" [3].
2) *Informação: "Dados dotados de relevância e propósito. Elemento possuidor de significado, valor entendido por um sujeito cognoscente."* [14].
3) *Conhecimento: "Informação valiosa da mente humana. Inclui reflexão, síntese, contexto."* [14].
4) *Inteligência: "Informação e conhecimentos estruturados"* [15]. Dados, informação ou conhecimento que permitam alcançar outros elementos de informação simples ou complexos, como conexões (vínculos) entre delitos ou alvos [16], por exemplo.

10. Trabalhos Correlatos

No âmbito do Departamento de Polícia Federal, apesar da disponibilidade e uso de ferramentas forenses computacionais comerciais pela Perícia Criminal Federal, surgiram iniciativas que objetivam tornar célere o aporte de documentos eletrônicos na investigação criminal e mais eficiente o tratamento de grandes volumes de dados. As mais conhecidas foram denominadas AsAP – *assistente de análise pericial* e SARD – *sistema de acesso remoto de dados* [11].

A primeira iniciativa compreende uma ferramenta que automatiza alguns passos específicos da interação do perito com a ferramenta FTK - *Forensic Toolkit* da *AccessData Corp.* [10] para alcançar maior produtividade no processamento de evidências digitais.

A segunda é um conceito genérico, que resultou em múltiplas formas de operacionalização. Entende-se ser o provimento de acesso remoto ao conteúdo existente no material computacional arrecadado, por intermédio do acesso direto a imagens forenses ou partir de arquivos extraídos destes mesmos materiais. As soluções que observam este conceito permitem que investigadores busquem por arquivos

[5] Em relação à precisão, a completude, a confiabilidade, a relevância etc. Em certas situações estas validações, do contexto da persecução penal no Brasil, requerem apreciação de peritos criminais.

que aparentem relevância e, depois de encontrados, ao final do trabalho de buscas, os arquivos são apresentados por peritos oficiais em laudos criminais. Há operacionalizações deste conceito que consideram examinar minuciosamente o material computacional onde foram encontrados os arquivos considerados relevantes pelos investigadores [11].

É relevante mencionar a existência de duas outras iniciativas concebidas por Peritos Criminais Federais: o projeto de pesquisa denominado MADIK - *Multi-Agent Digital Investigation toolkit* [9] e o ferramental denominado *Mobius Forensic Toolkit* [12].

A iniciativa MADIK é um ferramental, baseado em agentes autônomos e inteligentes, para automatizar os exames periciais. Ele se pauta em "*obter maior eficiência na realização dos exames periciais, com aumento da utilização de recursos computacionais ociosos, redução no tempo despendido e melhor aproveitamento da especialidade dos peritos na realização de exames mais complexos. O sistema também visa fornecer mecanismos de retenção e reutilização do conhecimento obtido de casos anteriores, que podem auxiliar os peritos menos experientes em seu trabalho e futuramente pode permitir a aplicação de técnicas de mineração de dados e descoberta de conhecimento.*" [9].

A iniciativa *Mobius Forensic Toolkit* compreende um *Framework* forense que gerencia casos e itens de casos, provendo uma interface abstrata para o desenvolvimento de extensões [12]. Tal ferramenta está relacionada essencialmente ao processo pericial de produção da prova digital.

Além das iniciativas mencionadas, é relevante enfatizar a existência das ferramentas comerciais EnCase da *Guidance Software*, *Inc*. [13] e FTK da *AccessData Corp.* [10]. Também tais ferramentas comerciais operam sob uma ótica diversa daquela comumente utilizada para o processo investigatório de análise de informações, mesmo se utilizadas em observância ao conceito SARD ou por múltiplos examinadores em um mesmo caso. Tais ferramentas não possuem características que as especializem no processo investigatório de análise da informação, estando relacionadas essencialmente ao processo pericial de produção da prova digital.

11. Experimentos e Resultados

Um ferramental forense foi desenvolvido para servir como prova dos conceitos aqui apresentados. Diversas operações policiais conduzidas no Estado da Bahia e do Pará fizeram uso deste ferramental experimental.

Dentre às investigações conduzidas no Estado da Bahia duas serão citadas:

- Na operação A, que trata de desvio de verba pública, 258 discos rígidos arrecadados tiveram o conteúdo disponibilizado no ferramental em 2 meses;
- Na operação B, que trata de exploração de jogos de azar, 50 discos rígidos arrecadados tiveram o conteúdo disponibilizado no ferramental em 1 mês.

Dentre às investigações conduzidas no Estado da Pará três serão citadas:

- Na primeira operação, em documento oficial enviado à Justiça Federal, o chefe da investigação se referiu ao ferramental e aos resultados obtidos por seu uso, da seguinte forma*: "... um verdadeiro* turning point*, uma verdadeira quebra de paradigma em termos de investigações policiais que envolvam apreensões de mídias computacionais e suas respectivas análises (e nos dias atuais isso quase sempre ocorre) ..."* [5].
- Na segunda operação foram arrecadados 41 discos rígidos e outras mídias menores, totalizando, aproximadamente, 8 terabytes de capacidade. Processados os dados em aproximadamente 1 mês, os documentos eletrônicos foram disponibilizados à equipe de investigação. As análises apontaram para a existência de fraudes na concessão de benefícios. O conjunto probatório foi montado com provas de diversas naturezas jurídicas, incluindo documentais e periciais. Enfatizam-se as diligências posteriores que puderam ser realizadas em virtude do conhecimento adquirido com interpretação conjunta das provas. Adquiridos novos dados, outros exames periciais puderam ser realizados. Os exames demonstraram divergências entre detalhes de benefícios e outros dados oficiais.
- Na terceira operação, o chefe das investigações, apresentando palestra em seminário interno da Polícia Federal no Estado do Pará, referiu-se ao método da seguinte forma: "Este procedimento tornou mais célere e eficiente a procura por evidências e a materialização destas evidências nos laudos periciais, proporcionando, de forma inédita, a apresentação do relatório final de uma Operação com 31 indiciados em pouco mais de 02 meses, já com todas as perícias realizadas e o material apreendido já restituído. Desta forma, resta confirmado, na prática, o sucesso desta nova metodologia de trabalho.". [6].

A operação havia arrecadado 57 discos rígidos e outras mídias menores, totalizando, aproximadamente, 4 terabytes. A estimativa inicial era a conclusão dos exames em mais de seis meses. Proposto e aceito o método, os trabalhos periciais foram concluídos em duas semanas.

12. Conclusões

A solução apresentada expande e torna ágil o processo investigatório de análise da informação, fomentando a cognição na investigação criminal em estrita observância aos princípios da cadeia de custódia, ao mesmo tempo em que contribui para preservar o valor probatório da prova resultante.

O método proposto sistematiza o processo de análises e contribui para que os investigadores atinjam de forma célere o objetivo que justificou a arrecadação de equipamentos computacionais: a formação do conhecimento sobre o fato investigado e a instrução da investigação criminal. A análise

investigatória da informação digital poderá ser amplamente realizada no contexto da investigação, a partir de documentos tradicionais e eletrônicos de forma simultânea, utilizando-se de um só método de trabalho. Prover amplos meios para que a equipe de investigação faça suas próprias análises é permitir que estas sejam tão minuciosas e extensas quanto for exigido pelas características do fato e da conduta em apuração.

13. Trabalhos Futuros

O ferramental desenvolvido como uma prova de conceitos, em sua forma atual, já oferece funcionalidades substanciais. Para torná-lo ainda mais poderoso e aumentar o escopo de validação dos conceitos, pretende-se:

- Permitir que o componente de análises investigatória interaja, simultaneamente, com vários componentes de mineração de dados, cada qual contendo uma fração dos documentos eletrônicos de interesse, correspondendo a um particionamento do caso numa determinada perspectiva da investigação. Essa evolução será útil nas operações deflagradas em âmbito nacional, com diligências em vários estados e com trabalhos periciais de extração de dados realizados no próprio estado em que o material foi arrecadado.
- Operacionalizar os módulos de reconhecimento de padrões e descoberta e apresentação de vínculos. Essa evolução será útil para ampliar a aquisição de conhecimento e inteligência na investigação criminal. Tais recursos trarão melhoria na eficiência e na efetividade do processo de análise, utilizando-se de algoritmos de mineração de dados para revelar conexões, dados e informações que seriam indetectáveis ou dificilmente percebidas somente por uma análise e observação humana.

Referências

[1] Mariath, C. R. (2009). Investigação criminal e sua necessária releitura. Jus Navigandi, Teresina, ano 15, n. 2599 , p. 4-7 Disponível em: <http://jus.uol.com.br/revista/texto/17185>. Acesso em: 7 dez. 2010.

[2] Departamento de Polícia Federal. (2008). Manual de Gestão de Planejamento Operacional . Brasília-DF: Academia Nacional de Policia. p. 73-79.

[3] Departamento de Polícia Federal. (2009). Investigação policial criminal. Brasília: Academia Nacional de Polícia - Dos Anjos, Alessandro Barbosa Diógenes; Mariath, Carlos Roberto; Soares, Jeferson Severo; Luz, Paulo Sérgio; da Silveira, Pehkx Jones Gomes; Santana, Renato Menezes e da Silveira, Sérgio Luiz Queiroz Sampaio. p 9-42.

[4] INC/DITEC. (2010). Relatório estatístico das atividades do sistema nacional de criminalística. Brasília. DF: Departamento de Polícia Federal - Diretoria Técnico Científica. p. 25-29.

[5] Documento Oficial que compõem Inquérito Policial (2010), de lavra do Delegado de Polícia Federal Welder Oliveira de Almeida, Superintendência de Polícia Federal no Estado do Pará.

[6] Um método prático e rápido, integrando busca e materialização da prova cibernética (2009), Seminário de Integração – Delegados, Procuradores, Magistrados e Peritos Criminais, Superintendência de Polícia Federal no Estado do Pará.

[7] Manzano, Luíz Fernando de Moraes. (2011). Prova Pericial: admissibilidade e assunção da prova científica e técnica no processo brasileiro, editora Atlas, São Paulo. p 12-22.

[8] Pinheiro, Patrícia. Peck. (2008). Direito Digital 2 ed. São Paulo: Saraiva. p. 249-250.

[9] Hoelz, Bruno Werneck Pinto (2009) MADIK: Uma Abordagem Multiagente para o Exame Pericial de Sistemas Computacionais, Brasília – UnB. P 83-111.

[10] Access Data Corp. FTK 3.x Disponivel em: <http://accessdata.com/downloads/media/Configuring%20Distributed%20Processing%20with%20FTK%203.pdf >. Acessado em 12 jul. 2011.

[11] SEPINF/DITEC – Serviço de Perícias em informática, Ferramentas de Análise Pericial. Disponível em: <https://sepinf.ditec.dpf.gov.br/wiki/Ferramentas> Acessado em 12 jul. 2011.

[12] Mobius Forensic Toolkit Disponivel em: <http://savannah.nongnu.org/projects/mobiusft>. Acessado em 12 jul. 2011.

[13] EnCase Forensic Disponivel em: < http://www.guidancesoftware.com>. Acessado em 12 jul. 2011.

[14] Da Silva, Heide Miranda. Gestão do Conhecimento e Inteligência Competitiva em Organizações: Uma Abordagem Conceitual. p 85–92 Disponivel em: <http:// http://www2.marilia.unesp.br/revistas/index.php/ric/article/viewFile/157/144 > Acessado em 04 set. 2011.

[15] Nokaka, I.; Takeuchi, H. (1997) Criação de conhecimento na empresa: como as empresas japonesas geram a dinâmica da inovação. Rio de Janeiro : Campus, p 635. 1997.

[16] Ferro Júnior, Celso Moreira; . Lima Dantas, George Felipe de. A descoberta e a análise de vínculos na complexidade da investigação criminal moderna. p. 12, Disponivel em: < http://www.trgroup.com.br/pdf/White%20Paper%20CGU-UNODC%20051020090537.pdf> Acessado em 04 set. 2011.

[17] Tarapanoff, Kira, Araújo Júnior, Rogério Henrique de and Cormier, Patricia Marie Jeanne. Sociedade da informação e inteligência em unidades de informação. Ci. Inf., Brasília, v. 29, n. 3, p. 91-100, set./dez. 2000. Disponivel em: <http www.scielo.br/pdf/ci/v29n3/a09v29n3.pdf> Acessado em 04 set. 2011.

[18] Simson L. Garfinkel (2010). Digital forensics research: The next 10 years. Digital investigation 7, p. S64 - S73, Disponivel em: < http:// www.dfrws.org/2010/proceedings/2010-308.pdf> Acessado em 04 set. 2011.

[19] Daniel Ayers (2009). A second generation computer forensic analysis system. Digital investigation 6, p. S34 - S42, Disponivel em: < http://www.dfrws.org/2009/proceedings/p34-ayers.pdf> Acessado em 04 set. 2011.

[20] Beebe , Nicole L. (2009). Digital Forensics Research: The Good, the Bad, and the Unaddressed p. 7-13 (23-29) Disponivel em: < http://www.springerlink.com/content/v162t5230472k767/> Acessado em 06 set. 2011.

[21] Ferro Júnior, Celso Moreira. Inteligência Organizacional: Identificação das bases doutrinárias para a investigação criminal. Conteudo Juridico, Brasilia-DF: 16 set. 2008. Disponivel em: <http://www.conteudojuridico.com.br/?artigos&ver=2.21050>. Acesso em: 13 set. 2011.

[22] Logicube Corp. Disponível em: http://www.logicube.com Acessado em: 16 set. 2011.