UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

METODOLOGIA E ARQUITETURA PARA SISTEMATIZAÇÃO DO PROCESSO INVESTIGATÓRIO DE ANÁLISE DA INFORMAÇÃO DIGITAL

LEVI ROBERTO COSTA

ORIENTADOR: HÉLVIO PEREIRA PEIXOTO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

ÁREA DE CONCENTRAÇÃO INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: PPGENE.DM - 109/2012

BRASÍLIA / DF: FEVEREIRO/2012

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

METODOLOGIA E ARQUITETURA PARA SISTEMATIZAÇÃO DO PROCESSO INVESTIGATÓRIO DE ANÁLISE DA INFORMAÇÃO DIGITAL

LEVI ROBERTO COSTA

DISSERTAÇÃO DE MESTRADO PROFISSIONALIZANTE SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

Hélvio Pereira Peixoto, Doutor, DITEC/DPF
(Orientador)

Flávio Elias Gomes de Deus, Doutor, ENE/UNB
(Examinador Interno)

Rodrigo Bonifacio de Almeida, Doutor, CIC/UNB
(Examinador Externo)

DATA: BRASÍLIA/DF, 14 DE FEVEREIRO DE 2012.

FICHA CATALOGRÁFICA

COSTA, LEVI ROBERTO
Metodologia e Arquitetura para Sistematização do Processo Investigatório de Análise da Informação Digital [Distrito Federal] 2012.
xv, 102p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2012).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

Palavras-chave: forense computacional; investigação digital; documentos eletrônicos; automatização.

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

COSTA, L. R. (2012). Metodologia e Arquitetura para Sistematização do Processo Investigatório de Análise da Informação Digital. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM - 109/2012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 102p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Levi Roberto Costa

TÍTULO DA DISSERTAÇÃO: Metodologia e Arquitetura para Sistematização do Processo Investigatório de Análise da Informação Digital.

GRAU: Mestre ANO: 2012

Levi Roberto Costa
Av. Vice-Presidente José Alencar, 1500, bloco 7, apto 1501, Barra da Tijuca, CEP 22775 033 – Rio de Janeiro – RJ – Brasil

À minha esposa Suzana. Amor, não poderia descrever a moção que me toma ao registrar estas palavras. Sem a sua ajuda, eu não teria alcançado tal objetivo.

A meus filhos Lívia, Lucas e Luana. “Pra frente. Juntos!”. Eram estas as palavras de incentivo proferidas por meu pai sempre que eu completava um estágio acadêmico ou profissional. Ao dedicar este trabalho a vocês, meus filhos, eu não encontro outra forma de demonstrar meu compromisso senão repetindo estas mesmas palavras: “Pra frente. Juntos!”.

A meus pais Dermeval e Leny e a meus irmãos Suerli, Jorge, Solange, Sonia, Selma e Ubiratan. Eu os amo profundamente. Todos os momentos que vivemos juntos são um privilégio concedido por Deus.

Amados pais, eu sigo o caminho da dignidade, da luta e da fé que sempre buscaram ensinar-me.

Amados irmãos, juntos, a vida pode nos vergar, mas jamais romperá a resistência que a união familiar nos conferiu.

AGRADECIMENTOS

A Deus.

A meu grande amigo e orientador, Dr. Hélvio Pereira Peixoto, pelo constante apoio, incentivo, paciência e dedicação essenciais para o desenvolvimento deste trabalho. Sua sabedoria e ampla visão foram importantes motivações durante essa jornada.

A meu mestre e irmão, Jorge Roberto Costa, pelas primeiras tutelas e por todas as demais em todos os estágios da minha vida profissional e pessoal. Não há como expressar toda a gratidão e a admiração que sinto.

Aos Peritos Criminais Federais Luiz Eduardo Marinho Gusmão, Georger Rommel Ferreira de Araújo, Osvaldo Dalben Junior e Daniel Pacheco Politano. Presentes da vida! Suas sugestões foram importantes para este trabalho. Obrigado por tudo.

Ao fiel amigo e companheiro inseparável, Fábio Inácio da Silva, Tenente-Coronel da Polícia Militar do Estado do Rio de Janeiro, por todo apoio, amizade e incentivo para o desenvolvimento deste trabalho.

Aos colegas e professores do curso de Mestrado por tudo que passamos juntos.

Aos Peritos Criminais Federais do grupo de peritos em informática do Setor Técnico-Científico da Superintendência de Polícia Federal nos Estado do Rio de Janeiro. Especialmente, ao PCF Jonathas da Silva Ferreira, Engenheiro da Computação e Bacharel em Direito, pelas inúmeras lições no campo do Direito e da Perícia Criminal.

Aos Delegados de Polícia Federal Welder Oliveira de Almeida e Lucimar Sobral Neto por acreditarem nesta proposta e por serem os primeiros a adotá-la em investigações policiais.

Ao Perito Criminal Federal Marcos Aurélio Silva de Oliveira, um pioneiro da "análise remota de dados", por todos os exemplos.

Ao Perito Criminal Federal Nicolau Tolentino Bogoevich Neto, "*in memoriam*". Companheiro, você tinha razão! Eu deveria ter seguido os seus conselhos.

Aos Peritos Criminais Federais André Morum e Rogério Dourado, por acreditarem na proposta e defendê-la nos Setores Técnico-Científicos em que atuam.

Aos Peritos Criminais Federais, Clênio Guimarães Belluco e João Pinto Rosa, Diretor Técnico-Científico substituto e Diretor do Instituto Nacional de Criminalística substituto, respectivamente, pelo incentivo e apoio.

Ao Superintendente de Polícia Federal no Estado do Pará, Manoel Fernando Abaddi, pelo incentivo e autorização para minha participação no curso de Mestrado.

Aos Peritos Criminais Federais José Osmar Campos da Silva e Jorge Cley de Oliveira Rosa, ex-chefes em substituição do Setor Técnico-Científico da Superintendência de Polícia Federal no Estado do Pará, pelas lições no campo da criminalística e pela amizade.

Aos Peritos Criminais Federais Patrícia Maria Souza da Costa, Ricardo Hamid Saikali e Luis Carlos de Almeida Serpa, respectivamente, chefa do Setor Técnico-Científico da Superintendência de Polícia Federal no Estado do Rio de Janeiro, chefe do Núcleo de Criminalística e chefe substituto do Núcleo de Criminalística, pelo apoio recebido desde que cheguei ao Estado do Rio de Janeiro.

Ao Departamento de Polícia Federal, por intermédio do Diretor Técnico-Científico, Paulo Roberto Fagundes, e à Universidade de Brasília, por desenvolverem e apoiarem o projeto do Mestrado Profissional em Engenharia Elétrica com ênfase em Informática Forense e Segurança da Informação, no âmbito do qual esta pesquisa foi desenvolvida, e ao Ministério da Justiça, por fornecer os recursos financeiros necessários ao curso de Mestrado, por meio do Programa Nacional de Segurança Pública com Cidadania – PRONASCI.

Agradeço, especialmente, à minha amada esposa Suzana Brandt e a meus filhos Lívia, Lucas e Luana. Foram muitos os dias que passamos distantes durante esse projeto e muitas horas que deixamos de aproveitar para que eu pudesse superar os desafios e concluir este trabalho.

RESUMO

METODOLOGIA E ARQUITETURA PARA SISTEMATIZAÇÃO DO PROCESSO INVESTIGATÓRIO DE ANÁLISE DA INFORMAÇÃO DIGITAL

Autor: Levi Roberto Costa
Orientador: Hélvio Pereira Peixoto
Programa de Pós-graduação em Engenharia Elétrica
Brasília, fevereiro de 2012

Esta pesquisa propõe um instrumental que integra investigadores e peritos em torno da investigação digital, em conformidade com a segregação de papéis, atribuições e responsabilidades existentes na polícia judiciária brasileira. Ela apresenta uma metodologia e uma arquitetura para um ferramental forense especializado, que por um lado observam a investigação digital como espécie do gênero investigação policial, enquanto que, por outro, observam a investigação digital como espécie do gênero pericia criminal. Integrando-as em um mesmo processo de busca da prova de um crime. Desta abordagem resulta, de forma isenta e harmoniosa, tanto a prova documental, quanto a prova pericial. Cada qual estabelecida segundo suas próprias regras, exigências e particularidades.

A solução proposta permite lidar de maneira ágil com grandes volumes de dados e/ou dispositivos de armazenamento de dados computacionais, utilizando-se de uma infraestrutura de componentes computacionais autônomos e inteligentes, bases de dados, rede de comunicação, hardwares e pessoas para prover eficiência na apuração de delitos.

Para avaliar suas potencialidades, o instrumental foi posto em prática em investigações reais e de grande porte conduzidas pelo Departamento de Polícia Federal. Os resultados obtidos demonstraram redução no tempo médio de disponibilização de dados digitais ao apuratório e permitiram que as análises investigatórias permeassem a investigação policial criminal, possibilitando a exploração profunda do material computacional apreendido. Embora os resultados alcançados possam ser considerados promissores, há potencial para alcançar resultados ainda melhores.

ABSTRACT

METHODOLOGY AND ARCHITECTURE FOR SYSTEMATIZING THE INVESTIGATION OF DIGITAL INFORMATION

Author: Levi Roberto Costa
Supervisor: Hélvio Pereira Peixoto
Programa de Pós-graduação em Engenharia Elétrica
Brasília, February of 2012

Taking into consideration the responsibilities and the necessary segregation of investigators and forensic experts duties in the Brazilian judicial system, this work proposes a novel methodology and architecture for the whole digital investigation process. The proposed solution integrates in a single process the digital investigation process and the forensic investigation process. The harmonic integration of the criminal and forensic investigations, respecting their rules and particularities, creates a unique context where the documental and forensic evidences can be found, selected and later presented at a court of law.

Through a variety of simple, intelligent and autonomous computational components, connected through a network of computer and investigators/forensic experts, the proposed method and architecture can synergistically and effectively handle great volume of digital evidence retrieved from a variety of storage devices.

As a proof of concept, the method and the corresponding architecture were implemented in a prototype and tested on large data sets of real criminal investigations at the Brazilian Federal Police. The early results demonstrate a significant reduction at the processing time required to make the digital evidence available for analysis, allowing criminal investigators early access to the evidence and most important, a thorough and deeper search on the seized materials. Although one could consider the prototype's performance a significant improvement over traditional methods, the potential results could be much more significant with a more robust computational infrastructure.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

ANP – Academia Nacional de Polícia do Departamento de Polícia Federal.

DPF – Departamento de Polícia Federal.

DITEC – Diretoria Técnico-Científica do Departamento de Polícia Federal.

INC – Instituto Nacional de Criminalística da DITEC/DPF

CD – Compact Disk

AsAP – Ferramenta para automatização da interação com o FTK.

SARD – Sistema de acesso remoto de dados.

SEPINF – Setor de Perícias em Informática do INC/DITEC/DPF .

FTK – Ferramenta comercial de Informática Forense da AccessData.

Sleuthkit – Coleção de ferramentas de Informática Forense de código aberto.

Autopsy – Interface gráfica para o Sleuthkit.

Foremost – Ferramentas de Informática Forense de código aberto.

Scapel – Ferramentas de Informática Forense de código aberto.

EnCase – Ferramenta comercial de Informática Forense da Guidance Software.

AdLab – Versão de laboratório do software FTK

NAS – Network-Attached Storage

1. INTRODUÇÃO

Adquirir conhecimento oriundo de documentos eletrônicos[1] ganhou grande importância para a atividade policial no contexto da investigação criminal (ANP/DPF, 2008). Esta nova modalidade de documento vem substituindo gradualmente os documentos tradicionais[2]. Na Polícia Federal, por exemplo, a cada ano, mais de 6.000 discos rígidos e computadores são apreendidos em investigações policiais. O volume de dados contidos nos materiais seria da ordem de 720 terabytes, correspondendo, aproximadamente, a 36 vezes o tamanho da maior biblioteca do mundo (INC/DITEC, 2010) (INC/DITEC, 2011) (INC/DITEC, 2012).

Embora esse grande volume de dados possa conter inúmeros documentos de vital importância para resolução de delitos, os investigadores[3] se deparam com obstáculos para livremente obtê-los[4], reuni-los[5] e analisá-los[6] em um processo de análise da informação[7] - tal como fariam no caso de uma caderneta de anotações ou de um extrato bancário (ANP/DPF, 2008).

A investigação digital é realizada quase que exclusivamente por peritos criminais, enquanto que os investigadores – amplos conhecedores de detalhes relevantes sobre alvos e fatos referentes às investigações – acabam afastados de dados e informações que poderiam ser fundamentais ao apuratório. Tal situação criou óbices à produção da prova documental, contribuindo negativamente para elucidação de um crime.

[1] Documentos eletrônicos são representações binárias apostas em meio digital, produzidas para expressar idéias, conhecimento, etc.
[2] Documentos tradicionais são representações da escrita, de imagens ou de sons apostos em base material, produzido para expressar idéias, conhecimento, etc.
[3] De forma geral, um grupo composto por diferentes cargos policiais.
[4] Granjeá-los por meio de diligenciais policiais, utilizando-se de procedimentos minuciosos de busca e identificação.
[5] Conciliá-los em relação a determinadas premissas e suposições realizadas pelos investigadores no intento de se chegar à resolução de um crime.
[6] Analisá-los com base no que se conhece ou que se deseja conhecer em relação ao crime investigado.
[7] Obtenção, reunião e analise são etapas do processo de análise da informação a que são submetidos os documentos apreendidos em diligencias policiais (ANP/DPF, 2009).

1.1. PROBLEMA TRATADO

A natureza digital do documento eletrônico impôs certos cuidados para que seja mantido o valor probante da prova dele resultante. 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. Sua utilização na lide penal requer ações, por parte de peritos criminais, que afastem seu caráter dúbio, e assim possam alcançar a confiança dos magistrados (Pinheiro, 2008).

Tais características inerentes aos documentos eletrônicos contribuíram, no âmbito policial, para o surgimento de um processo diferenciado ao processo originalmente utilizado para a análise da informação tradicional, como aquela aposta em papel, por exemplo. Dando azo a coexistirem dois processos independentes e anacrônicos para análise da informação, representados na figura 1.1. Um para trabalhar com documentos tradicionais, conduzido por investigadores e outro para os documentos eletrônicos, conduzido por peritos criminais.

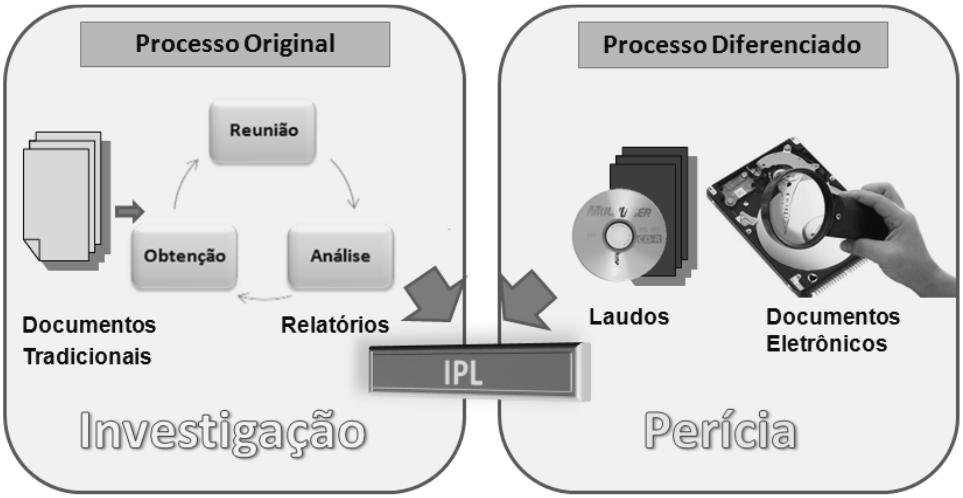

Figura 1.1 - Processo Original x Diferenciado

A situação atual é contraproducente e pouco eficiente, sobressaindo que:

1) Os processos original e diferenciado de análise da informação são independentes, pois não se intercomunicam obrigatoriamente. Além disso, são anacrônicos, uma vez os documentos tradicionais podem ser analisados tão logo sejam organizadas as equipes de análise, enquanto que os documentos

eletrônicos requerem um processamento prévio do material computacional arrecadado (ANP/DPF, 2008).

Ou seja, enquanto que no processo original os investigadores iniciam as análises dos documentos tradicionais tão logo a equipe de análise se organize, no modelo diferenciado, primeiramente, os materiais computacionais apreendidos são enviados a peritos criminais. Caberá a estes profissionais apresentarem aos investigadores os documentos eletrônicos que possuam certas palavras-chave e/ou respondam determinados quesitos (inquirições) (ANP/DPF, 2008).

Em 2011, o tempo médio transcorrido entre uma requisição de perícias e seu completo atendimento era de 157 dias (INC/DITEC, 2012), o que corresponde ao lapso temporal que investigadores necessitarão aguardar pela conclusão do processo diferenciado de análise da informação digital, para só então conhecerem todos os documentos reunidos pelos peritos criminais;

2) Há situações em que informações relevantes à elucidação do delito encontram-se unicamente no conteúdo de arquivos eletrônicos (ANP/DPF, 2008);

3) Para desempenhar as tarefas de análise, algumas vezes, os materiais e os quesitos recebidos pelo perito serão o primeiro e único contato que este profissional terá com o investigatório antes de iniciar o trabalho requisitado. Caso os quesitos não contemplem com exatidão as características de apresentação dos documentos eletrônicos relevantes, há risco de que o trabalho pericial não apresente de pronto os elementos necessários à elucidação do fato ou da conduta investigada;

4) O processo diferenciado de análise sujeita a investigação policial criminal ao descarte prematuro de dados, fato descrito como um erro grosseiro e irremediável (ANP/DPF, 2009). Tal situação ocorre ao serem estabelecidos pelos investigadores os critérios para que os peritos criminais apresentem os documentos eletrônicos ao apuratório. Neste momento, como os investigadores não terão, a priori, acesso aos demais documentos existentes no material apreendido, também, de forma indireta, foram por eles definidas as regras que desprezarão os demais documentos.

O cenário apresentado contrasta, por exemplo, com o norte-americano, em que os policiais que executam a investigação analisam, livremente, tanto os documentos

tradicionais, quanto os eletrônicos. Entretanto, a adoção de modelos de processos e ferramentas concebidas para suportar a investigação policial criminal naquele país, ou em qualquer outro, não oferecerá solução adequada aos problemas mencionados, caso não contemplem particularidades da legislação pátria. No Brasil, no que concerne a prova de um crime, o modelo de persecução penal vigente atribui papéis distintos, embora complementares, a investigadores e peritos.

Face aos fatores elencados, quais sejam:

1) Lacuna entre investigação e perícia ocasionada pela adoção de processos distintos, independentes e anacrônicos, para análise da informação tradicional e eletrônica;
2) Ferramentas e modelos de processo de investigação de crimes digitais inadequados à legislação brasileira.
3) Crescimento ininterrupto do volume e da capacidade de armazenamento de dados do material a examinar;

Configura-se a necessidade de desenvolver uma metodologia, sustentada por uma base teórica sólida e materializado em um ferramental especializado, associado a técnicas e procedimentos apropriados, para que a polícia judiciária brasileira possa fazer frente aos desafios promovidos pela criminalidade moderna.

1.2. HIPÓTESE DE PESQUISA

É possível integrar os trabalhos de investigadores e peritos criminais em torno da aquisição da prova digital, cada qual realizando, a partir das mesmas fontes digitais, frações distintas da investigação digital: a análise da informação, no caso dos investigadores, e o exame pericial no caso dos peritos criminais?

1.3. JUSTIFICATIVA E RELEVÂNCIA

Investigar e prover alternativas que promovam melhorias na investigação policial criminal é contribuir para diminuição da impunidade e para o aumento do efeito dissuasório em relação à criminalidade. A existência de dois processos independentes e anacrônicos para análise da informação contribui negativamente para elucidação de crimes, requerendo atenção.

1.4. OBJETIVOS

O objetivo deste trabalho é integrar investigadores e peritos criminais em torno da investigação digital, abolindo o processo diferenciado de análise.

Para alcançar o objetivo primário, foram definidos os objetivos específicos, a saber:

1) Conceber e implementar uma metodologia que norteará a investigação digital, em conformidade com a segregação de papéis, atribuições e responsabilidades existentes na polícia judiciária brasileira;
2) Projetar e implementar uma arquitetura computacional, voltada à Informática Forense, que seja capaz de processar grandes volumes de dados. Tendo por finalidade tornar mais ágil a disponibilização de documentos eletrônicos ao apuratório, eliminando ou minorando o anacronismo entre as análises de documentos tradicionais e eletrônicos;
3) Projetar os meios para tornar possível que investigadores tenham ampla visão do caso investigado, e possam submeter ao processo de análise investigatória, simultaneamente, todo o documental obtido dos diversos materiais arrecadados, evitando conjecturas baseadas em frações isoladas do caso. Uma determinada prova de um crime pode estar segmentada em diversos materiais, o que pode ofuscar a visão de investigadores caso estes trabalhem em partes isoladas do material arrecadado.
4) Elaborar processos dinâmicos de buscas textuais (palavra-chave) que operem simultaneamente em todos os documentos de um mesmo caso, a fim de alcançar agilidade na localização de documentos relevantes, mesmo em grandes volumes de dados;
5) Permitir a análise de documentos eletrônicos permeando a investigação policial criminal, de forma colaborativa e geograficamente distribuída.

1.5. RESULTADOS ESPERADOS

Os principais resultados esperados incluem:

1) Contribuir, no âmbito do Departamento de Polícia Federal, para que se atinja o objetivo estratégico, estabelecido pelos administradores da Perícia Criminal

Federal, referente à produção de instrumentos que viabilizem a análise e correlação de um grande volume de dados digitais obtidos em investigações criminais (INC/DITEC, 2010) (INC/DITEC, 2011) (INC/DITEC, 2012);

2) Contribuir para ampliação da eficiência investigatória da instituição policial;
3) Resguardar a objetividade do perito, que não deve ser exposto ao contexto das premissas e suposições da investigação;
4) Favorecer a evolução do conhecimento em ciclo à medida que novas informações são analisadas pela equipe de investigação, subsidiando a cognição na atividade policial;
5) Contribuir para aumento da eficiência na produção de provas, para aumento dos índices de elucidação de crimes e para efetiva aplicação da justiça;
6) Contribuir para tornar mais rápida a devolução de materiais apreendidos que se mostrem irrelevantes ao apuratório.

1.6. MÉTODO DE TRABALHO

Para alcançar os objetivos propostos foram realizados os passos descritos a seguir:

1) Revisão da literatura relacionada à investigação policial, à pericia criminal e ao direito penal, que permitiu identificar os trabalhos relacionados e as possíveis soluções para o problema;
2) Para restabelecer a análise investigatória de documentos tradicionais e eletrônicos a um único processo de análise, foi concebida uma metodologia que norteará os trabalhos de peritos e investigadores.
3) Para oferecer o suporte a adoção da metodologia concebida, foi desenvolvida uma arquitetura para um ferramental forense especializado que instrumentará as tarefas de peritos e investigadores;
4) Com base na arquitetura proposta, foi construído um protótipo para o ferramental especializado;
5) A metodologia e o ferramental foram então submetidos à prova de conceitos e avaliados em investigações policiais reais.

1.7. ORGANIZAÇÃO DA DISSERTAÇÃO

Os capítulos seguintes desta Dissertação foram assim organizados: no Capítulo 2 está a fundamentação teórica necessária ao desenvolvimento das pesquisas. No Capítulo 3 são apresentados os instrumentos comumente utilizados na investigação digital. No Capítulo 4 é apresentada a proposta do trabalho e, finalmente, nos Capítulos 5 e 6 são expostos, respectivamente, as provas de conceitos em casos reais e as conclusões.

2. REVISÃO DE CONCEITOS

Neste Capítulo é apresentado o fundamento teórico necessário ao desenvolvimento da pesquisa. Como a investigação digital pode ser abordada de diferentes pontos de vista[8], torna-se indispensável enfatizar que este trabalho aborda o tema pelo enfoque policial. Em virtude disso, é relevante a compreensão de princípios relacionados à persecução penal no Brasil, apresentados na Seção 2.1; a prova no direito penal, discutida na Seção 2.2; o crime informático e a investigação policial criminal, abordados nos capítulos 2.3 e 2.4, respectivamente; a perícia criminal, abordada na Seção 2.5. Ao final das revisões, são realizadas considerações que seguem na Seção 2.6.

2.1. PERSECUÇÃO PENAL

Com o fim de coibir condutas especialmente lesivas, a lei estabelece fórmulas segundo as quais o poder punitivo do Estado habilita o seu exercício formal. Tais fórmulas são os tipos penais. Através de um juízo de tipicidade, há a valoração de uma conduta como típica ou atípica, conforme sua adequação, ou não, ao tipo penal (Zaffaroni, Batista, Alagia, & Slokar, 2010).

Ao ocorrer um fato supostamente delituoso, surge para o Estado um poder-dever de punir. Para fazer valer tal prerrogativa estatal, no entanto, é necessária a persecução penal que, no Brasil, é composta por duas fases: o inquérito policial e a ação penal (Távora & Antonni, 2009).

Ao tomar ciência de uma conduta aparentemente típica, a autoridade policial iniciará a apuração da infração penal formalizando a investigação policial criminal por meio de um inquérito policial. Nas palavras de Tourinho Filho, o inquérito é "*o conjunto de diligências realizadas pela Polícia Judiciária para a apuração de uma infração penal e sua autoria, a fim de que o titular da ação penal, possa ingressar em juízo*" (Tourinho Filho, 2009).

Tendo sido ingressado em juízo, tem-se início a ação penal, conceituada como "*o direito de se pedir ao Estado-Juiz a aplicação do Direito Penal objetivo. Ou o direito*

[8] Como avaliação de incidentes, operações militares de guerra cibernética, investigação de crimes, entre muitas outras aplicações. Cada qual possuindo contexto próprio, características e exigências particulares.

de se pedir ao Estado-Juiz uma decisão sobre um fato penalmente relevante" (Tourinho Filho, 2009).

No inquérito e na ação penal, é necessária uma reconstrução histórica dos fatos. Busca-se demonstrar o ocorrido a partir da apresentação de provas. Enquanto que as provas apresentadas no inquérito policial se destinam ao titular da ação penal para convencê-lo se o processo (ação penal) deve ou não ser deflagrado, na ação penal, o destinatário da prova é o julgador, que formará seu convencimento quanto ao direito de punir do Estado.

Algumas provas são de natural entendimento quando sua interpretação está ao domínio dos operadores do direito. Outras, no entanto, necessitam de conhecimento específico em determinada área do conhecimento ou da arte para que sejam compreendidas. Nesses casos, é necessário um exame procedido por pessoa que tenha tais conhecimentos ou habilidades: o perito oficial. A Perícia Criminal atua nas fases pré-processual e processual, da persecução penal. Do exame pericial resulta um documento denominado laudo pericial criminal (Manzano, 2011).

Nas palavras de Manzano "*o perito oficial é aquele investido na função mediante concurso público, promovido pela Polícia Judiciária – Federal ou Civil -, para atuar nos órgãos técnicos da chamada polícia científica*" (Manzano, 2011).

Manzano deixou de considerar em sua definição os peritos oficiais que atuam em órgãos autônomos e independentes da Polícia Judiciária. O que ocorre em alguns estados da federação, como o estado do Pará, por exemplo. Assim, mais adequada definição, salvo melhor juízo, seria: o perito oficial é o agente público investido legalmente com a atribuição de, em questões criminais que dependam de conhecimento especial, examinar vestígios originários de crime ou dirimir as questões de ordem técnica, científica ou artísticas, relevantes ao acertamento do fato e ao deslinde da causa.

Segundo a Lei 12030/2009 são peritos oficiais o perito criminal, o médico-legista e o odontolegista. Destes, apenas o perito criminal lida com os vestígios na cena de um crime.

2.2. PROVA NO DIREITO PENAL BRASILEIRO

Provar é levar ao conhecimento de outro algo que se conhece e que se dá por certo, em relação ao que se alega ou se diz (Tourinho Filho, 2009). O conceito de prova, segundo Tourinho Filho seria: "*os elementos produzidos pelas partes ou pelo próprio juiz visando a estabelecer, dentro do processo, a existência de certos fatos"* (Tourinho Filho, 2009).

Segundo Paulo Rangel, o sistema de apreciação das provas adotado no Brasil é o da livre convicção motivada ou livre convencimento. Neste sistema, o juiz é que aprecia as provas existentes nos autos, atribuindo valor a elas, de forma fundamentada. Não existe, assim, prévia definição de hierarquia entre as provas. Todas as provas oferecidas são fundamentalmente importantes para se estabelecer a verdade processual. (Rangel, 2003).

Este pesquisador ousa afirma que a prova resultante da apreciação de peritos oficiais, embora não seja a mais importante das provas, certamente é a mais confiável. Os peritos oficiais são chamados a atuar pelas partes ou pelo próprio magistrado, emitindo conclusões objetivas e isentas, sem intenção de condenar ou absolver, apenas esclarecer a verdade por intermédio da ciência (Espíndula, 2009).

Nas palavras de Luís Fernando de Moraes Manzano, "*Elemento de prova ou simplesmente prova é todo dado objetivo que se presta à confirmação ou negação de uma asserção a respeito de um fato que interessa a decisão da causa*" (Manzano, 2011).

Guilherme de Souza Nucci ensina que (Nucci, 2008):

> O termo prova origina-se do latim – probatio –, que significa ensaio, verificação, inspeção, exame, argumento, razão, aprovação ou confirmação. Dele deriva o verbo provar – probare –, significando ensaiar, verificar, examinar, reconhecer por experiência, aprovar, estar satisfeito com algo, persuadir alguém a alguma coisa ou demonstrar.

Provar, então, é buscar oferecer os elementos de prova para que o julgador se convença, através de seu raciocínio, de haver um estado de certeza que o torna convicto da existência ou inexistência de um fato. Leciona Júlio Fabbrini Mirabete que (Mirabete, 2008):

> Provar é produzir um estado de certeza, na consciência e mente do juiz, para sua convicção, a respeito da existência ou inexistência de um fato, ou da verdade ou falsidade de uma afirmação sobre uma situação de fato, que se considera de interesse para uma decisão judicial ou a solução de um processo.

Sustenta Manzano que "*A finalidade da prova é, em última análise, o convencimento do juiz acerca da sustentabilidade ou não de uma alegação*" (Manzano, 2011).

Sobressai por de acordo o que se entende por verdade no processo: a verdade processual. Verdade processual é aquilo que se demonstra a partir das provas transladadas para os autos do processo. Trata-se, então, de uma verdade, que irá se estabelecer, no processo, pelo oferecimento de provas, segundo as regras do próprio processo (Nucci, 2008). Leciona o professor Nucci que "*A verdade processual emerge durante a lide, podendo corresponder à realidade ou não, embora seja com base nela que o magistrado deve proferir sua decisão.*" (Nucci, 2008).

O professor Paulo Rangel leciona sobre verdade processual afirmando que se considera inexistente a verdade não demonstrada no rol de provas dos autos do processo (Rangel, 2003):

> A adoção do sistema do livre convencimento é expressão da vontade do legislador, que dá ao juiz liberdade de agir de acordo com as <u>provas</u> que se encontram nos autos, pois, se não estão nos autos, não existem no mundo.

Ela aduz ainda que (Rangel, 2003):

> A apreciação é da prova. Portanto, deve haver prova nos autos, seja para condenar, seja para absolver.

Segundo ensina Manzano, há no sistema jurídico pátrio uma exceção que, como não contraria, complementa os ensinamentos de Paulo Rangel. De acordo com Manzano, no tribunal do júri vigora o sistema da íntima convicção, visto serem sigilosas as votações, o que tornaria misto o sistema adotado pelo ordenamento jurídico pátrio (Manzano, 2011).

Segundo Julio Fabbrini Mirabete, o objeto de prova são os fatos, as circunstâncias, os acontecimentos que devem ser demonstrados no processo. O objeto de prova abrangerá "*não só o fato criminoso e sua autoria, como todas as circunstâncias objetivas e subjetivas que possam influir na responsabilidade penal e na fixação da pena ou na imposição da medida de segurança.*" (Mirabete, 2008).

As provas são obtidas de fontes de prova. Fontes de prova são coisas ou pessoas. Segundo Manzano, documentos são fontes de prova enquanto fora do processo, passando a elemento de prova uma vez que forem transladados a ele (Manzano, 2011).

Do que ensina Nucci se conclui que todas as provas, exceto as que contrariam o ordenamento jurídico, podem ser produzidas no processo, mesmo aquelas que não tenham sido previstas no Código do Processo Penal (Nucci, 2008).

Quanto às provas de origem digital, Patrícia Peck ressalta que há fragilidades que devem ser observadas (Pinheiro, 2008).

> Apesar do alto nível de precisão da computação forense, há uma fragilidade: a coleta das evidências. Coletar de forma errônea pode tornar ilícita ou inválida determinada prova. Também, ainda, existe a possibilidade de alguma prova ilícita contaminar as demais, teoria da árvore dos frutos envenenados, eliminando todas as chances no litígio judicial.

Patrícia Peck vai além quando afirma que (Pinheiro, 2008):

> Outro problema enfrentado pelas evidências digitais é a falta de confiança dos magistrados nesse tipo de prova. Logo, cabe ao perito retirar este caráter dúbio da evidência em um laudo pericial claro, e, como inexiste uma hierarquia de provas no Direito brasileiro, caberá ao juiz analisar e medir a importância das evidências.

Entre os meios de prova, a busca e apreensão, a documental e a pericial são essencialmente importantes para este trabalho, sem, contudo, abster-se da relevância dos demais.

2.2.1. Busca e Apreensão

A busca e apreensão decorrem da relativização de direitos individuais (Nucci, 2008). Objetiva permitir que o estado alcance as provas mantidas sob domínio de investigados, entre outros fins.

Guilherme de Souza Nucci ensina que (Nucci, 2008):

> busca significa o movimento desencadeado pelos agentes do estado para a investigação, descoberta e pesquisa de algo interessante para o processo penal, realizando-se em pessoas e lugares.

Quando citando Cleunice A. Valentim Bastos Pitombo, Nucci afirma que a autora conceitua busca como (Nucci, 2008):

> ato do procedimento persecutivo penal, restritivo de direito individual (inviolabilidade da intimidade, vida privada, domicílio e da integridade física e moral), consistente em procura, que pode ostentar-se na revista ou no varejamento, conforme a hipótese: de pessoa (vítima de crime, suspeito, indiciado, acusado, condenado, testemunha e perito), de semoventes, de coisas (objetos, papéis e documentos), bem como de vestígios (rastros, sinais e pistas) da infração.

Por sua vez, Nucci enfatiza que apreensão é medida assecuratória que toma algo de alguém ou de algum lugar, com finalidade de produzir prova ou preservar direitos (Nucci, 2008).

Novamente citando Cleunice A. Valentim Bastos Pitombo, Nucci apresenta o conceito de apreensão como sendo (Nucci, 2008):

> ato processual penal, subjetivamente complexo, de aposamento, remoção e guarda de coisas – objetos, papéis ou documentos –, de semoventes e de pessoas, "do poder de quem as detém"; tornando-as indisponíveis, ou colocando-as sob custódia, enquanto importarem a instrução criminal ou ao processo.

Tanto a busca quanto a apreensão são medidas de natureza jurídica mista, podendo ser vistas, individualmente, como meios assecuratórios, meio de prova ou ambos (Nucci, 2008). Por suas palavras, doutrina Nucci:

> Conforme o caso, a busca pode significar um ato preliminar à apreensão de produto do crime, razão pela qual se destina a devolução à vítima. Pode significar, ainda, um meio de prova, quando a autorização é dada pelo juiz para se proceder a uma perícia em determinado domicílio. A apreensão tem os mesmos ângulos. Pode representar a tomada de um bem para acautelar o direito de indenização da parte ofendida, como pode representar a apreensão da arma do delito para fazer prova.

Alessandro Barbosa Diógenes dos Anjos e outros ensinam que, em certas situações, os envolvidos com o crime investigado são os únicos detentores de informações acerca dos fatos. Nestas situações, obter as informações em posse dos envolvidos assume um caráter relevante à apuração do suposto ilícito penal. (ANP/DPF, 2009).

Entre as coisas arrecadadas comumente em uma investigação policial se encontram os computadores, mídias computacionais de armazenamento de dados, fotografias, extratos bancários, comprovantes de transferências financeiras, comprovantes de aplicações e de câmbio, notas-fiscais, declarações patrimoniais, agendas de contatos, diários pessoais, vestígios biológicos e tudo mais quando possa representar fonte de informações ao apuratório, requerendo uma análise investigatória minuciosa realizada com a finalidade de alcançar as informações necessárias à elucidação do delito.

2.2.2. Prova Documental

O professor Guilherme de Souza Nucci apresenta o conceito de documentos como sendo (Nucci, 2008):

> quaisquer escritos (papel ou de outra base material contendo a representação de palavras ou idéias através de sinais), instrumentos (documentos pré-constituídos para a formação de prova, como recibo, procurações, termos etc.) e papéis (de aplicação residual, vale dizer, excluídos os elementos anteriores – escritos e instrumentos – cuida-se da base constituída de matéria fibrosa, de origem vegetal, tratada e destinada à formação de folhas aptas a receber gráficos, desenhos).

Quanto à classificação, o professor Nucci ensina que documentos podem ser nominativos ou anônimos. Os nominativos seriam aqueles que possuem indicação de quem o produziu[9]. Por sua vez, os anônimos são aqueles que não identificam seu produtor. Nucci nos conduz a conhecer que uma fotografia "*retratando determinada situação importante para o desfecho de um processo pode ser juntada aos autos, mesmo que não se saiba quem a produziu.*". Complementa Nucci que "*Ainda, assim, é um documento.*" (Nucci, 2008).

[9] Documentos eletrônicos assinados digitalmente são considerados análogos aos documentos tradicionais assinados, visto que se pode verificar sua autoria, autenticidade e integridade.

Em um arrazoado sobre a importância do documento anônimo como prova, Nucci assevera que:

> Logicamente, um escrito anônimo terá de ser cuidadosamente avaliado pelo magistrado, visto não ter o mesmo valor do documento nominativo. Entretanto, o fato de não se saber quem o escreveu não o torna inútil, nem lhe retira o aspecto documental de uma idéia reduzida em base material. Imagine-se alguém que tenha presenciado um homicídio e, não desejando ser reconhecido, envia carta anônima à polícia; graças a isso, localiza-se o autor, que ampla e espontaneamente confessa seu ato. Torna-se importante fator de prova aquela carta, pois justifica o fato de o Estado-Investigação ter chegado a desvendar a autoria da infração penal, legitimando-a de alguma forma. Não se quer absolutamente dar a esse documento anônimo o mesmo valor que possui o nominativo, passível de confirmação, mas não deixa de ser, no contexto probatório, um elemento a mais para a avaliação judicial. Somente, não se deve excluí-lo do conjunto das provas, visto que ilícito não é.

Segundo Nucci, quanto à valoração e licitude do documento como efetivo meio de prova, deve-se observar certos requisitos (Nucci, 2008):

> Para que seja considerado efetivo meio de prova, ensina a doutrina dever ser o documento apresentado, no processo, por inteiro – sem fragmentações que possam comprometer o seu sentido -, livre de defeitos ou vícios – sem rasuras, borrões ou emendas, tornando-o suspeito e inteligível – compreensível por quem o visualiza.

Enfatizando os avanços tecnológicos, o professor Nucci aduz que o conceito de documento vem sendo amplificado. Segundo ele, vem ocorrendo uma substituição da estrutura material tradicional por outras inovadoras que, de forma similar aos documentos tradicionais, permitem a fixação de uma base de conhecimento e expressão de pensamentos, idéias ou manifestações de vontade ou pensamento do ser humano. Nucci assevera que "*são documentos, portanto: escritos, fotos, fitas de vídeo e som, desenhos, esquemas, gravuras, disquetes, CDs, entre outros*" (Nucci, 2008). Nucci também enfatiza em alusão as mensagens eletrônicas que:

> o e-mail deve ser considerado documento, baseado no critério ampliativo do conceito de documento, abrangendo outras bases suficientes para registrar pensamentos ou outra manifestação de vontade, pois está armazenado dentro de um computador, no disco rígido.

Interpretando os ensinamentos de Nucci, pode-se entender possível estender tais conceitos aos demais documentos eletrônicos produzidos com o objetivo similar de registrar pensamento ou outras manifestações da vontade.

Em 1995, observou Pollitt que a característica intangível dos documentos eletrônicos provocava um conflito de entendimento em um mundo acostumado a lidar com documentos tradicionais. Esse novo tipo de documento fez surgir alguns questionamentos que até então não suscitavam dúvidas (Pollitt, 1995). Questões como: O documento realmente existe? De onde ele vem ou como surgiu? O que representa a cadeia binária que o origina? O que garante sua autenticidade? Estaria o documento apresentado íntegro? Em 2012, estas questões ainda não estão bem claras para os leigos em informática, mesmo que pareçam óbvias para alguns iniciados em tecnologia.

2.2.3. Prova Pericial

Alberí Espíndula ensina que a prova pericial é um meio de prova que exige uma fundamentação técnica, científica ou artística, produzida por perito oficial. Difere nas provas subjetivas uma vez que aquelas despendem de testemunhos e interpretações de pessoas, estando sujeitas a erros de relato, falhas de interpretação e má-fé de intenções que podem distorcer os fatos. (Espíndula, 2009).

Ensina Luiz Fernando de Moraes Manzano que (Manzano, 2011):

> A característica fundamental da perícia como prova científica, e que a distingue dos demais meios de prova, é que ela se vale de um princípio científico aplicado por meio de técnica adequada, cujo conhecimento escapa, via de regra, ao domínio dos aplicadores do Direito, mas que é essencial ao acertamento do fato e ao deslinde da causa.

Manzano versa sobre a importância da prova pericial enfatizando que, quando a infração deixar vestígios, a prova da existência do fato, via de regra, é pericial. Segundo Manzano, "*há casos em que a convicção do juiz se assenta sobremaneira no parecer do pericial, sem que possa negá-lo, em razão de seu vistoso conteúdo técnico-científico.*". Ele é ainda mais incisivo quando afirma (Manzano, 2011):

> Com o desenvolvimento técnico e científico, e o advento do processo eletrônico, a prova pericial ganhou relevo. Há casos em que o acertamento do fato e decisão da causa é somente alcançável pela prova pericial, o que reveste esse meio de prova de importância crucial na busca da verdade processual.

Mazano assevera, citando anotação de Tornaghi, que o "*acertado seria retirar a perícia do capítulo das provas e situá-la em lugar autônomo, entre esta e a sentença.*" (Manzano, 2011).

Quanto à distinção entre as provas, ensina Manzano que prova pericial não se confunde com a prova documental. "*São coisas distintas e submetidas a disciplinas jurídicas diversas*". Versando sobre documentos ele afirma: "*Este, aliás, pode também ser submetido à perícia*" (Manzano, 2011). Logo, a prova pericial pode resultar de um mesmo documento, tradicional ou eletrônico, que deu origem a uma prova documental.

Em outras palavras, um documento, tradicional ou eletrônico, oferecido como prova documental difere da prova pericial obtida a partir do mesmo documento. Para exemplificar o afirmado, se anotações contábeis do tráfico de drogas apostas em papel tivessem sido oferecidas como meio de comprovação de um delito, delas resultariam a prova documental[10]. Destas mesmas anotações contábeis, poder-se-ia também resultar a prova pericial. Por exemplo, haveria de ser necessária a análise da integridade destas anotações quanto a possíveis adições, alterações, substituições ou eliminações de texto. Haveria, também, de ser necessária a verificação de sua autenticidade quanto ao punho escritor que a produziu ou que a subscreveu, além do próprio exame pericial contábil.

2.3. CRIME INFORMÁTICO

De acordo com Marco A. R. da Costa uma conceituação própria para crime informático seria "*toda a ação típica, antijurídica culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão.*".

Em seus estudos, Costa assevera que "*a natureza dos delitos de informática, a complexidade e, principalmente, a ausência de unanimidade dos doutrinadores, fazem a dificuldade de definir os crimes de informática*". Ele enfatiza a importância de se desenvolver o Direito Criminal da Informática. O autor utiliza-se de palavras tão significativas que uma referência a seu trabalho não dispensará a apresentação de sua própria expressão (Costa, 1997).

> O Direito Criminal da Informática deve ser desenvolvido com extrema rapidez e segurança, de modo a serem sistematizadas normas que atinjam os crimes

[10] Considerando que foram atendidas às exigências legais que regem este tipo de prova.

> empiricamente tipificados, que são cometidos com o emprego de computadores e sistemas, desenvolvendo proteção à privacidade, a instrumentalização da produção de provas, inclusive reciclando os conceitos de provas, principalmente aquelas provas técnicas.

Segundo Túlio Lima Vianna, os crimes informáticos são classificados por próprios, impróprios, mistos, mediatos ou indiretos (Vianna, 2003).

Os crimes informáticos próprios são aqueles que o bem tutelado é a inviolabilidade de dados ou sistemas computacionais. Os crimes impróprios são aqueles em que computadores são utilizados como instrumentos para perpetração de delito, sem que, no entanto, o bem tutelado seja a inviolabilidade de dados ou sistemas computacionais. Agregam-se à conceituação de crimes impróprios, os crimes que empregam o uso de computador como instrumento da perpetração do delito e os crimes cujo uso de computador se deu de forma meramente incidental (Couri, 2009), substituindo uma máquina de escrever, um fac-símile, uma pasta de documentos, um bloco de anotações ou uma agenda. Nas palavras de Túlio Lima Vianna "*a hipótese clássica de crimes informáticos impróprios são os crimes contra a honra – calúnia (art. 138 CP), difamação (art. 139 CP), injúria (art. 140 CP) – cometidos pelo simples envio de um email.*" (Vianna, 2003).

Por sua vez, os crimes informáticos mistos são aqueles crimes complexos[11] cuja norma busca tutelar, além da inviolabilidade da coisa digital, outro bem jurídico diverso. O autor afirma que "*São delitos derivados do acesso não autorizado a sistemas computacionais que ganharam status de delitos sui generis dada à importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.*" (Vianna, 2003).

Finalmente, os crimes informáticos mediatos ou indiretos são aqueles delitos (delito-fim) não informáticos que herdam a característica de outro delito (delito-meio) praticado para que se alcance a consumação do delito não informático (Vianna, 2003).

> Se alguém acessa sem autorização o sistema computacional de um banco e transfere indevidamente dinheiro para sua conta, estará cometendo dois delitos distintos: o acesso não autorizado a sistemas computacionais e o furto; o primeiro, crime informático, o segundo, patrimonial. O acesso não autorizado será executado como delito-meio para se poder executar o delito-fim que

[11] Representa o concurso de mais de um tipo penal.

> consiste na subtração da coisa alheia móvel. Desta forma, o agente só será punido pelo furto, aplicando-se ao caso o princípio da consunção.
>
> O crime-fim será classificado como informático mediato ou indireto quando, pela aplicação do principio da consunção, um crime-meio informático não for punido em razão da sua consumação.

Segundo Huebner e outros, o crime informático poderia ainda ser classificado de outra maneira, (Huebner, Bem, & Bem, 2008):

1) Crime centrado no computador: É o crime cujo alvo é o próprio computador, um sistema computacional, redes de computadores, dispositivos de armazenamento de dados. Isso pode ser visto como nova classe de crime cometido com o emprego de novas ferramentas;
2) Crimes auxiliados por computador: É o crime em que o computador foi instrumento para perpetração da conduta sem, contudo, ter sido estritamente necessário seu uso na prática delitiva. Um novo instrumento utilizado para praticar crimes comuns;
3) Crimes com o envolvimento incidental do computador: É o crime em que o computador foi utilizado de uma forma incidental à atividade criminosa em si, armazenando dados ligados à prática delitiva em substituição a outras formas de registro. Como uma planilha de contabilização dos recursos obtidos com a prática criminosa mantidos em computador em substituição de outros mantidos em papel.

Assevera Couri que "*o crime informático se distingue dos demais ante a peculiar presença do computador na prática delitiva*". Segundo ele, o computador pode ser envolvido na prática do delito cumprindo diferentes papéis (Couri, 2009).

Segundo Patrícia Peck, citando Robson Ferreira, os papéis do computador no delito seriam na forma de alvo, instrumento da perpetração do crime ou até mesmo um papel meramente incidental na prática delituosa: uma espécie de repositório onde a manifestação escrita se materializou por intermédio de documentos eletrônicos. Tais papéis dependeriam da maneira como o crime fora praticado, sobretudo, do próprio delito em si (Pinheiro, 2008).

Os papéis do computador no delito seriam assim descritos:

1) O computador como alvo do delito ocorre quando o próprio equipamento é o objeto do crime ou quando o sistema computacional, o sistema de arquivos ou um sistema de informação, por exemplo, são alvos da conduta delituosa (Couri, 2009). Como exemplo de crimes onde o computador é o alvo da conduta relaciona-se a destruição intencional ou modificação não autorizada de banco de dados (Couri, 2009).

2) O papel do computador como instrumento ocorre quando o equipamento computacional é utilizado para a perpetração de um delito, tal qual uma arma de fogo em um caso de homicídio (Couri, 2009). Segundo assevera Guilherme de Souza Nucci, os instrumentos da perpetração do crime "*são os objetos que servem de agente mecânico para a realização do crime*" (Nucci, 2008). Como exemplo de crimes em que o computador é o instrumento, pode-se relacionar as transferências de valores não autorizadas, através da internet; assim como o compartilhamento de imagens contendo pornografia infantil.

3) Por fim, um computador será incidentalmente envolvido no delito nas vezes em que o equipamento tenha sido um mero contentor dos elementos de informação sobre o delito. Não, propriamente, em um crime informático (Couri, 2009). Por analogia, como se fosse uma pasta de documentos, um caderno de notas, uma gaveta ou um arquivo onde se armazenam contratos ou outros "papéis". Sendo, simplesmente, um contentor daquilo possivelmente útil às investigações. Nestes casos, os "computadores" são meros suportes para os elementos de informação de natureza digital. Como as mensagens eletrônicas trocadas entre os partícipes do delito ou os documentos eletrônicos que registram informações relacionadas ao crime, como as planilhas, as fotografias, as gravações em vídeos, os contratos etc. Como exemplo de crimes em que o computador pode ser envolvido incidentalmente, pode-se relacionar as fraudes contábeis, as fraudes previdenciárias, os roubos, os furtos, as torturas etc. Em suma, qualquer crime em que alguma informação que orbita em torno do delito ou mesmo uma informação que aponta a existência do próprio crime tenha ficado registrada de alguma forma no computador.

Os conceitos apresentados por Couri e Patrícia Peck estão em consonância com o que leciona Huebner, que sugeriu uma classificação para os crimes informáticos, e são complementares ao que nos ensinou Túlio Lima Vianna, todos referenciados anteriormente.

2.4. INVESTIGAÇÃO POLICIAL CRIMINAL

De acordo com Luiz Flávio Gomes e Fábio Scliar, "*Investigação é atividade de busca da verdade acerca de determinado fato, é esforço para conhecimento de determinada coisa que está oculta*" (Gomes & Scliar, 2008).

Em uma investigação, procura-se tornar evidente o obscuro, preenchendo os vagos de informação, elaborando inquirições e perseguindo respostas que permitam concluir sob a ação delituosa tudo quanto seja necessário para fundamentar a investigação criminal.Tomando por base o que é ensinado na Academia Nacional de Polícia, "*Investigar um crime é, de fato, fazer perguntas e catalogar respostas, em uma seqüência lógica, buscando reconstituir toda a ação delituosa e apontar, com segurança, a sua autoria.*" (ANP/DPF, 2009).

De acordo com a professora Maria Carolina Opilhar (Opilhar, 2006), a investigação policial poderia ser conceituada como:

> A investigação policia é atividade de natureza sigilosa exercida por policial ou equipe de policiais determinada por autoridade competente que, utilizando metodologia e técnicas próprias, visa a obtenção de evidências, indícios e provas de materialidade e de autoria do crime.

Em outras palavras, Maria Carolina Opilhar leciona que a investigação policial criminal tem por objetivo alcançar, não só a prova documental ou pericial de um crime, mas também os indícios, que são espécies de circunstancias que possuam relação com o crime, baseando-se em probabilidades, por exemplo - para apontar sua provável autoria e/ou a sua possível dinâmica de perpetração.

De acordo com Adriano M. Barbosa, a investigação policial busca informações orientadas por indagações que, respondidas, conduzem à elucidação do delito investigado (Barbosa, 2011). Segundo ele:

> O investigador diante da situação-problema (crime) há de indagar sobre: (a) O que aconteceu; (b) Quem foi o autor do fato; (c) Quando tal fato se deu; (d) Onde ele aconteceu; (e) Por que ele veio à tona; (f) Como foi o ato criminoso praticado; e (g) Com quais instrumentos o seu autor levou a termo a sua perpetração.

Para alcançar respostas a tais indagações, faz-se necessário granjear os detalhes a cerca do próprio fato em apuração. É para alcançar esse objetivo que as diligências policiais são orientadas, servindo a investigação como um dos instrumentos que aportam dados, informações, conhecimento e inteligência no inquérito policial.

2.4.1. Análise da Informação

A análise da informação na investigação policial criminal pode ser definida por intermédio de um ciclo representado na figura 2.1.

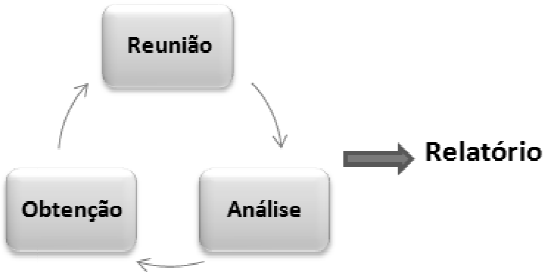

Figura 2.1 - Processo de análise (adaptado de DPF, 2009).

O processo tem por objetivo obter e aportar informações e conhecimento na investigação policial criminal, utilizando como veículos os relatórios de análise apresentados de forma sucessiva e complementar. Os relatórios de análise 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) (ANP/DPF, 2009).

A análise da informação não se resume a uma simples análise isolada de conteúdo de documentos, pois "*mesmo o mais simples dos casos demanda um exaustivo trabalho de*

busca, classificação e análise de informações das mais diversas fontes". (ANP/DPF, 2009). 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.

A complexidade dos delitos contemporâneos exige uma ampla integração dos meios de prova. Nesta linha, um investigador, agente cognoscente do processo de análise da informação, necessita reunir dados referentes ao caso em concreto para que - após analisá-los, relacionando-os com outros dados conhecidos - possa atribuir a eles algum significado, conferindo-os condição de informação (ANP/DPF, 2009).

Um processo de análise da informação deve permear a investigação policial criminal. Cada 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 possível dinâmica de perpetração (ANP/DPF, 2009).

2.5. PERÍCIA CRIMINAL

Segundo Adalberto José Q. T. de Camargo Aranha, desembargador aposentado do Tribunal de Justiça de São Paulo, "*A perícia é a lanterna que ilumina o caminho do juiz que, por não a ter quanto a um determinado fato, está na escuridão. A lente que corrige a visão que está deficiente pela falta de um conhecimento especial*" (Aranha, 1987).

De acordo com Luís Fernando de Moraes Manzano (Manzano, 2011):

> Perícia é um meio de prova técnica ou científica, que tem por objetivo a obtenção de certo conhecimento relevante para o acertamento do fato (elemento de prova), a partir de procedimento técnico realizado sobre pessoa ou coisa (fonte de prova). A conclusão do técnico ou profissional (conclusão probatória) é expressa num laudo (elemento de prova), que tem por finalidade (finalidade de prova) influir da persuasão racional do juiz, em seu processo cognitivo de valoração (valoração da prova).

Entre as definições clássicas de perícia criminal encontra-se o asseverado pelo Dr. C.J.A Mittermaier (Mittermaier, 1997): O doutrinador afirma que

> Tem lugar o exame de peritos sempre que se apresentarem na causa criminal questões importantes, cuja solução, para poder convencer o juiz, exija o exame de homens, que tenham conhecimentos e aptidões técnicas e especiais.

A perícia criminal poderá ser autorizada pela autoridade judiciária ou policial. Ressalvado o exame de corpo de delito, que não pode ser denegado quando a infração deixar vestígios, as demais perícias, se não necessárias ao esclarecimento da verdade, segundo o art. 184 do Código de Processo Penal Brasileiro, poderão ser indeferidas pela autoridade judiciária ou policial. O Código de Processo Penal Brasileiro em seu art. 158 determina que "*quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado*". Nestes termos, de sua falta pode resultar a nulidade processual. Contudo, o referido diploma legal não estabeleceu um conceito para corpo de delito. Citando Hélio Tornagui, Manzano fez conhecer que (Manzano, 2011):

> Corpo de delito é o conjunto de vestígios materiais deixados pelo crime. A expressão é de Farinácio, que distinguia a alma do delito (anima delicti), que é a malícia ou negligência do agente, e o corpo de delito, que é a materialidade do crime, aquilo que se vê, ouve, palpa, sente; aquilo que cai sob os sentidos; instrumentos; e o próprio crime; marcas, impressões, pegadas etc.

2.6. CONSIDERAÇÕES

Revisitando o conceito em torno do papel do computador no delito, combinando-o com os art. 158 e 175 do Código de Processo Penal Brasileiro, observa-se:

1) Quando o equipamento foi o alvo do delito – o próprio bem tutelado violado, o corpo de delito – seu exame pericial será indispensável;
2) Quando o computador foi o instrumento da perpetração da conduta delituosa um exame pericial que lhe verifique a eficiência para produzir os efeitos observados no delito será relevante. No artigo 175, o Código de Processo Penal Brasileiro estabelece que "*serão sujeitos a exame os instrumentos empregados para a prática da infração, a fim de se lhes verificar a natureza e a eficiência*". Segundo Nucci, verificar a "n*atureza significa estabelecer a espécie e a*

qualidade" do instrumento. Por sua vez, verificar a "e*ficiência quer dizer a verificação de sua força ou eficácia para produzir determinado resultado*". Nucci menciona ser plausível a hipótese de crime impossível, quanto se constata que a arma, em tese, utilizada para cometê-lo pode ser inapta para este fim. (Nucci, 2008);

3) Quando o computador teve um papel meramente incidental em um crime (armazenando documentos eletrônicos possivelmente relacionados a um caso em apuração), tem-se o objetivo inicial de alcançar tais documentos eletrônicos, assegurando sua procedência, autenticidade e integridade, a fim de que posteriormente se proceda à minuciosa análise de conteúdo destes documentos, cotejando-os com outras provas (ANP/DPF, 2008);

4) Um computador pode ao mesmo tempo cumprir mais de um papel no delito.

Para representar a análise da informação digital e o estudo de eventos, de rastros deixados por criminosos e dos efeitos ocorridos em um ambiente computacional ou provocados a partir dele, na literatura em inglês, é comum encontrar os termos *digital investigation, computer forensics, forensic computer science,* além de outros. Entretanto, do contexto da apuração de crimes no Brasil, o conceito que envolve o termo *digital investigation* é mais abrangente que os conceitos de perícia criminal e investigação policial criminal, vistos de forma isolada.

Segundo *Brian Carrier,* o conceito de *digital investigation* seria (Carrier, 2005):

> *A digital investigation is a process where we develop and test hypotheses that answer questions about digital events. This is done using the scientific method where we develop a hypothesis using evidence that we find and then test the hypothesis by looking for additional evidence that shows the hypothesis is impossible.*

Palmer conceituou *forensic computer science* da seguinte forma (Palmer, 2001):

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

Freiling e *Schwittay* conceituaram *computer forensic* como (Freiling & Schwittay, 2007):

> *Computer Forensics is a scientific discipline which is concerned with the collection, analysis and interpretation of digital data connected to a computer security incident; it is sometimes also called digital forensics. Since any device, data or other resource subject to a forensic examination may be subsequently used as evidence in a court of law, Computer Forensics puts special emphasis on the correct treatment of potential evidence to prevent it from being altered or tampered with.*

Em razão do que se discutiu neste Capítulo acerca de meios de prova, fragilidade da prova digital[12], papel do computador no delito, crime informático, busca pela produção de provas admissíveis em juízo e segregação de papéis existentes entre investigadores e peritos criminais, o conceito de *digital investigation* só é suficientemente compatível com a reunião dos conceitos de análise da informação e pericia criminal. Por conseguinte, requer uma integração de esforços entre peritos criminais e investigadores na busca pela elucidação dos fatos investigados.

Além do mais, no Direito Penal brasileiro, o meio de prova documental não se confunde com o meio de prova pericial. Conforme ensinou Manzano, referenciado na Seção 2.2.3, são coisas distintas e submetidas a disciplinas jurídicas diversas.

Conjuntamente, os conceitos apresentados neste capítulo e o problema de pesquisa, permitem expor que a forma como atualmente é desempenhada a análise da informação digital no Brasil, acarreta:

1. O afastamento dos investigadores de parte do principal insumo de seu trabalho: a informação em formato digital. Na medida em que estes não explorarem profundamente o material computacional arrecadado, documentos relevantes ao apuratório poderão não estar sendo percebidos, prejudicando a eficiência da investigação policial criminal;

[12] Em virtude de não serem tangíveis requerem procedimentos para adequada coleta e preservação (Pinheiro, 2008). Além de meios que assegurem, posteriormente, a sua integridade, autenticidade e procedência para que alçassem a confiança do magistrado em um processo legal (ANP/DPF, 2008).

2. Centralização, no perito criminal, do trabalho de busca e análise de documentos eletrônicos, donde resulta a prova documental, e do trabalho de condução de exames periciais, propriamente dito, donde resulta a prova pericial.

O Capítulo 3 discorre sobre os modelos de processo que foram propostos para a investigação digital no contexto da apuração de crimes, bem como ferramentas utilizadas para esse fim.

3. TRABALHOS RELACIONADOS

Este Capítulo apresenta diversas propostas concebidas para instrumentar as investigações que envolvem a aquisição de provas de origem digital. Na Seção 3.1 são apresentadas as principais características de diversos modelos de processo utilizados em investigações digitais[13]. Na Seção 3.2 são apresentadas diversas ferramentas empregadas no desempenho deste trabalho.

3.1. MODELOS DE PROCESSOS FORENSES

De forma geral, a concepção de um modelo de processos está relacionada ao seu emprego. Cada proposta tende a possuir características que atendam certas particularidades ou dirijam certo modo de trabalho. No segmento policial, por exemplo, as exigências legais e outros fatores são significativos.

3.1.1. Pollitt – 1995

Segundo *Pollitt*, para que os documentos eletrônicos alcancem admissibilidade em juízo, bases sólidas precisam ser estabelecidas, dúvidas precisam ser dirimidas e devem ser afastadas quaisquer inseguranças existentes. O pesquisador enfatiza que a cadeia digital que compõe o documento precisa passar por um processo de aquisição e conversão para só então dar origem a um formato inteligível. Somente depois deste momento é que um avaliador, após identificar algo possivelmente relacionado ao apuratório, julgará se a informação contida no documento identificado é relevante (Pollitt, 1995).

Para alcançar os objetivos pretendidos, *Pollitt* propôs um framework composto de quatro passos, representado na figura 3.1 (Pollitt, 1995).

Figura 3.1 – Modelo forense computacional (adaptado de Pollitt, 1995).

[13] Tradução literal do termo em inglês *digital investigation*.

O modelo de *Pollitt* representa as ações básicas em um processo forense e foi estruturado da seguinte forma (Pollitt, 1995):

1) A fase de aquisição tem por objetivo alcançar as provas digitais, utilizando-se de recursos que devem obedecer às regras definidas pela Lei;

2) A fase de identificação tem por objetivo converter a cadeia binária que dá origem ao documento para um formato que seja compreensível para o leigo;

3) A fase de avaliação tem por objetivo determinar se a informação contida no documento é relevante;

4) A fase de admissão tem por objetivo a apresentação da prova.

3.1.2. Palmer – 2001

De acordo com *Palmer*, os participantes do *First Digital Forensic Research Workshop*, conferência ocorrida no ano de 2001, conceberam um modelo de processo genérico e aplicável a grande parte das investigações envolvendo sistemas digitais e redes de computadores (Palmer, 2001). Representado na figura 3.2, o modelo descrito por *Palmer* é composto por 7 fases, em que as principais foram denominadas por preservação, coleta, exame e análise (Palmer, 2001).

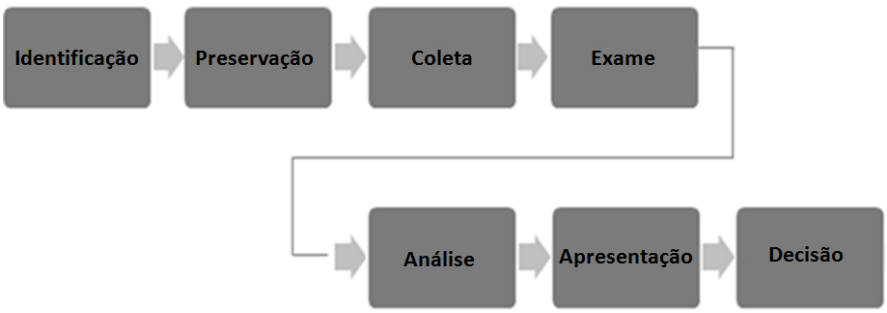

Figura 3.2 - Modelo forense computacional (adaptado de Palmer, 2001).

O modelo foi estruturado da seguinte forma (Palmer, 2001):

1) A fase de identificação consiste da detecção do evento ou crime, monitoramentos de eventos e auditoria de fatos;

2) A fase de preservação consiste da gestão do caso, cadeia de custódia[14], geração de imagens forenses;

3) A fase de coleta consiste da obtenção da autorização legal, do uso de técnicas de recuperação, preservação, adoção de software e hardwares apropriados, utilização de métodos confiáveis, técnicas de recuperação etc.;

4) A fase de exame consiste da preservação do material a examinar, na aplicação de técnicas de filtragem e pesquisas, na descoberta de dados ocultos, etc.;

5) A fase de análise consiste da busca pela descoberta da prova do evento ou crime;

6) A fase de apresentação consiste da documentação dos trabalhos e formalização da prova;

7) A fase de decisão consiste da avaliação final dos trabalhos investigatórios.

3.1.3. Reith, Carr e Gunsch – 2002

Reith, Carr e Gunsch propuseram um modelo, representado na figura 3.3, baseado na proposta descrita por *Palmer*, em 2001. Os pesquisadores teriam também utilizado como base de sua proposta um conjunto de regras utilizado pela Polícia Federal Americana para tratar a cena de um crime (Reith, Carr, & Gunsch, 2002).

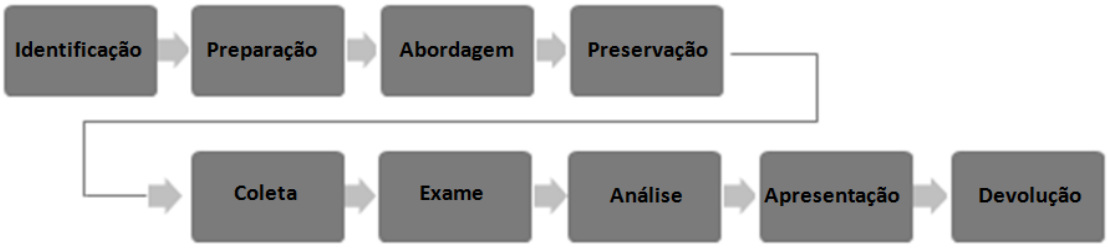

Figura 3.3 - Modelo forense computacional (adaptado de Reith, Carr e Gunsch, 2002).

Os pesquisadores sugeriram a necessidade de um primeiro passo, que denominaram por "Identificação", para classificar o delito ou incidente investigado, argumentando que tal visão é significativa, pois impacta os demais passos dos trabalhos (Reith, Carr, & Gunsch, 2002). O segundo passo envolveria a preparação dos trabalhos investigatórios. Ele aborda as autorizações legais para afastar direitos individuais, como mandados de

[14] Em síntese, a cadeia de custódia representa um registro cronológico que objetiva documentar os acontecimentos relacionados as evidencias, desde sua coleta até sua apresentação em juízo. Visa a idoneidade da prova.

busca e apreensão e autorizações para interceptações, tenso sido denominado "Preparação" (Reith, Carr, & Gunsch, 2002).

Após a conclusão dos passos de identificação e preparação, dá-se início ao passo de elaboração de estratégias para abordagem. Nesse ponto objetiva-se maximizar a coleta de provas, minimizando os impactos à vítima. Na sequencia, tem-se a preservação do estado das coisas (local e evidências) e a coleta, sugerindo a orientação deste modelo a um trabalho em local de crime. As demais fases são a execução de exames para identificação das evidências, a análise das evidências identificadas, apresentação das conclusões dos exames e devolução do material examinado aos respectivos proprietários. Em relação ao passo de análise das evidências identificadas, os autores sugerem que talvez sejam necessárias várias iterações para alcançar conclusões em relação aos fatos investigados. Concluem que nesse ponto, outras pessoas poderiam participar dos trabalhos, pois a exigência de uma elevada competência técnica teria sido afastada (Reith, Carr, & Gunsch, 2002).

3.1.4. Carrier e Spafford – 2003

Adotando por premissa que cada computador no delito é uma cena do crime em si, o modelo forense proposto por *Carrier* e *Spafford*, em 2003, representado na figura 3.4, aplica os conceitos alicerçados das perícias em locais de crime para oferecer uma alternativa de abordagem em investigações criminais. Os pesquisadores fazem menção à teoria de *Locard*[15], afirmando que condutas que se utilizam de computadores deixarão rastros perceptíveis aos investigadores (Carrier & Spafford, 2003).

Figura 3.4 - Modelo forense computacional (adaptado de Carrier e Spafford, 2003).

[15] Em síntese, qualquer pessoa que entre em um local de crime deixa algo novo na cena. E, ao retirar-se, leva algo que lá estava, mesmo que não tenha esta intenção.

Por exemplo, numa cena de crime, os cabelos, as fibras de roupas, o sangue, o suor do criminoso etc. são frequentemente utilizados por peritos criminais para obter informações relevantes à apuração do delito. De acordo com os pesquisadores, no caso de computadores, rastros como dados em memória, arquivos temporários, registros de eventos, entre outros, serão resultantes da conduta delitiva no ambiente computacional.

O modelo proposto por *Carrier* e *Spafford* foi estruturado da seguinte forma (Carrier & Spafford, 2003):

1) A fase de prontidão tem por objetivo alcançar uma infraestrutura capaz de suportar a investigação. Segundo os autores, tanto as provas de origem digital quanto outras provas podem ser perdidas se não forem coletadas adequadamente.

2) A fase de implantação tem por objetivo fornecer os meios para que o crime ou incidente seja identificado. Esta fase representa o início da investigação, propriamente dita.

3) O objetivo da fase de investigação da cena de crime[16], incluindo a cena de crime digital[17], é coletar e analisar os vestígios[18] e reconstituir as ações que aconteceram durante o incidente.

4) A fase de investigação da cena de crime digital se inicia quando dispositivos computacionais são coletados na cena do crime ou quando comunicações telemáticas relacionadas ao delito são interceptadas. Esta fase aborda um computador como uma cena do crime onde vestígios digitais devem ser procurados. Os pesquisadores enfatizam que a condução dessa fase deveria ser realizada por alguém tecnicamente capacitado, especialista em ferramentas e técnicas forenses.

[16] Em síntese, é todo local onde tenha ocorrido um crime.
[17] Em síntese, é um local relativo a computadores ou sítios de internet, por exemplo, onde tenha ocorrido um crime.
[18] Em síntese, são marcas, sinais de ações provocadas por alguém ou sinais de algo que aconteceu.

3.1.5. Ciardhuáin – 2004

O pesquisador *Ciardhuáin* publicou, no ano de 2004, um modelo composto de 13 fases, conforme representado na figura 3.5 (Ciardhuain, 2004).

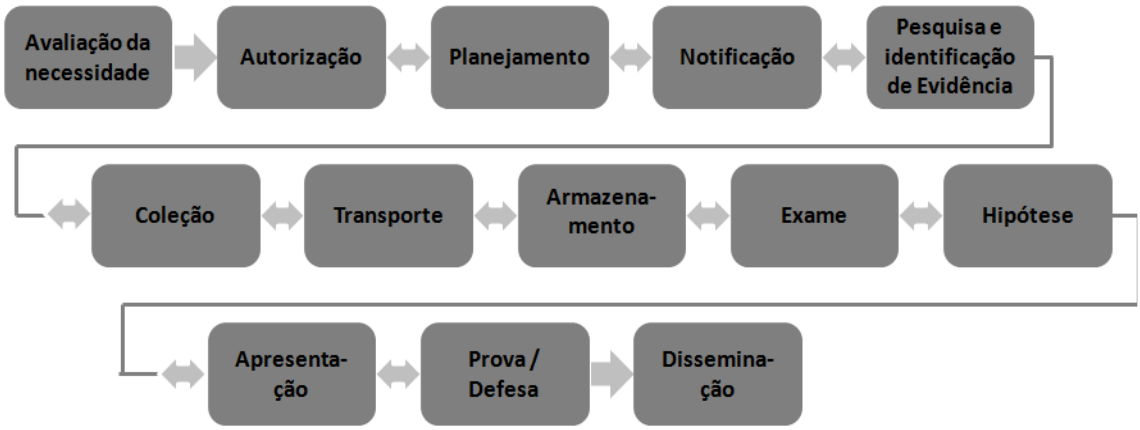

Figura 3.5 - Modelo forense computacional (adaptado de *Ciardhuáin,* 2004).

O modelo proposto foi estruturado da seguinte forma (Ciardhuain, 2004):

1) A fase de avaliação da necessidade tem por objetivo alcançar a convicção que a investigação é necessária. O pesquisador afirma que esta consciência é normalmente criada por eventos externos a organização.

2) A fase de autorização tem por objetivo alcançar a permissão necessária ao início dos trabalhos investigatórios.

3) A fase de planejamento tem por objetivo definir as estratégias a serem seguidas para condução das investigações, que podem sofre influencias internar e externas a organização responsável pelas apurações. De forma externa a organização responsável pelas investigações, os trabalhos são fortemente influenciados por regulamentos e legislações. Internamente, são influenciados por experiências anteriores, políticas da própria organização.

4) A fase de notificação tem por objetivo tornar conhecido que a investigação será realizada. O autor menciona que esta fase não se aplicaria a algumas investigações, onde o efeito surpresa é necessário para evitar destruição de provas.

5) A fase de pesquisa e identificação de evidência tem por objetivo a localização de fontes de provas, como o computador utilizado para perpetração da prática investigada.

6) A fase de coleção tem por objetivo alcançar os vestígios de forma que sejam analisados e preservados. Segundo o autor, esta atividade é de relevância para a investigação. Erros ou práticas equivocadas podem comprometer a validade da prova.

7) A fase de transporte tem por objetivo transladar os vestígios colidos para um local adequado e seguro a realização dos exames. Ë importante assegurar que o translado não afetará a integridade da prova.

8) A fase de armazenamento tem por objetivo a guarda dos vestígios, para os casos em que os exames não se iniciem imediatamente.

9) A fase de exame vai envolver a aplicação de técnicas apropriadas para alcançar e interpretar a prova.

10) A fase de hipótese tem por objetivo buscar elementos para demonstrar o que ocorreu, com base nos vestígios.

11) A fase de apresentação tem por objetivo oferecer as conclusões da investigação.

12) A fase de prova / defesa tem por objetivo que os investigadores comprovem a validade de sua hipótese, defendendo-a de ataques e criticas. Hipóteses que não se possa sustentar podem resultar em retrocesso nas investigações.

13) A atividade final do modelo é a disseminação de informações. Algumas informações podem ser disponibilizadas apenas para organização, enquanto outras informações podem requerer uma divulgação mais ampla.

3.1.6. Beebe e Clark – 2004

Os pesquisadores *Beebe* e *Clark* publicaram, no ano de 2004, um modelo composto de fases, subfases, princípios e objetivos. O primeiro nível do modelo foi organizado em 6 fases, conforme representado na figura 3.6. O trabalho resultou em um modelo forense hierárquico que observou pontos positivos de outros modelos e os harmonizou com suas

próprias idéias, de sorte a simplificar a complexidade de um processo investigatório (Beebe & Clark, 2004).

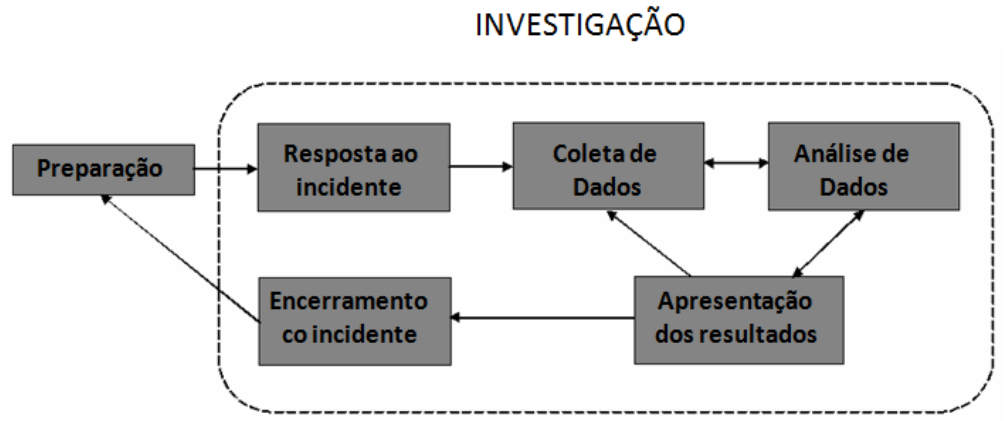

Figura 3.6 - Modelo forense computacional (adaptado de Beebe e Clark, 2004).

O modelo proposto foi estruturado da seguinte forma (Beebe & Clark, 2004):

1) A fase de preparação inclui as medidas tomadas para maximizar a oportunidade de se alcançar os vestígios.

2) A fase de resposta ao incidente tem por objetivo detectar, validar, avaliar e determinar uma estratégia de resposta para a suspeita de incidente de segurança.

3) A fase de coleta de dados tem por objetivo coletar os vestígios digitais em consonância com a estratégia definida na fase anterior.

4) A fase de análise de dados tem por objetivo confirmar ou refutar as alegações relacionadas à atividade suspeita.

5) A fase de apresentação tem por objetivo comunicar os resultados alcançados durante as investigações.

6) A fase de encerramento tem por objetivo registrar o encerramento das investigações e tomar ações que preservem o conhecimento adquirido para uso em experiências futuras.

3.1.7. Kent, Chevalier, Grance e Dang – 2006

Os pesquisadores *Kent*, *Chevalier*, *Grance* e *Dang* propuseram, no ano de 2006, um modelo forense composto de 4 fases (Kent, Chevalier, Grance, & Dang, 2006), conforme representado na figura 3.7.

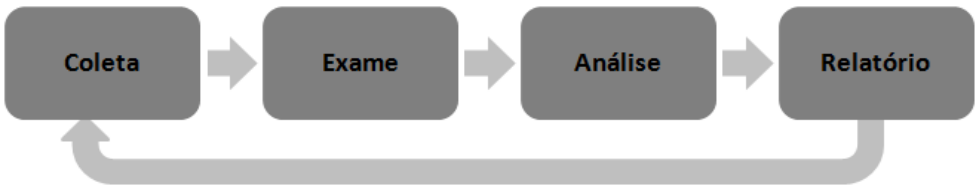

Figura 3.7 – Modelo Forense Computacional (adaptado de Kent, Chevalier, Grance e Dang, 2006).

O modelo proposto foi estruturado da seguinte forma:

1) Na fase de coleta os materiais referentes a um evento específico são identificados, rotulados, registrados e recolhidos, preservando-os em relação a sua integridade;

2) Na fase de exame as ferramentas forenses e técnicas adequadas são empregadas para identificar e extrair dados dos materiais coletados;

3) A fase de análise envolve a avaliação dos resultados obtidos na fase de exame para alcançar informações relacionadas aos fatos e alvos;

4) A fase de relatório tem por objetivo explicitar os resultados dos exames.

3.1.8. Kohn, Eloff e Olivier – 2006

Os pesquisadores *Kohn*, *Eloff* e *Olivier* propuseram, no ano de 2006, um modelo forense composto de 3 estágio. O modelo estabelece que as atividades forenses estejam atentas aos requisitos legais, para que estabeleçam provas válidas em juízo (Kohn, Eloff, & Oliver, 2006).

A figura 3.8 apresenta a ordem em que os estágios foram estruturados.

Figura 3.8 – Modelo Forense Computacional (adaptado de Kohn, Eloff e Olivier, 2006).

O modelo proposto foi organizado da seguinte forma (Kohn, Eloff, & Oliver, 2006):

1) O estágio de preparação da investigação deve observar as políticas e os procedimentos a serem empregados em investigações, o treinamento de pessoal, o reaproveitamento de experiências anteriores, a definição de estratégias de abordagem etc.;

2) O estágio de investigação deve considerar recolher computadores envolvidos com os fatos investigados, transportar as provas para um ambiente seguro, examiná-las usando as ferramentas adequadas, analisar o produto do exame para determinar o significado e o valor dos vestígios encontrados;

3) O estágio final da investigação forense deve incluir uma etapa de apresentação dos resultados da investigação.

3.1.9. Aspectos Relacionados ao Emprego dos Modelos

Os modelos de processo propostos em países estrangeiros não observam a segregação de papéis existentes entre investigadores e peritos criminais, no modelo de persecução penal no Brasil. Ao adotá-los, concorre-se para dificultar que seja alcançado um maior aprofundamento na análise do possível material probatório de origem digital, contribuindo para acarretar os problemas apresentados na Seção 1.1.

3.2. FERRAMENTAS FORENSES

Diversas ferramentas são comumente utilizadas no campo da investigação digital. Algumas delas são ferramentas comerciais e outras são iniciativas não comerciais, fortemente voltadas à extração de evidências de um ambiente computacional.

Em relação às ferramentas concebidas no Departamento de Polícia Federal, surgiram iniciativas que objetivam tornar célere a análise de documentos eletrônicos 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 (SEPINF/DITEC, 2011).

A primeira iniciativa compreende uma ferramenta que automatiza alguns passos específicos da interação do perito criminal com a ferramenta FTK - *Forensic Toolkit* da *AccessData,* para alcançar maior produtividade no processamento de dispositivos de armazenamento de dados computacionais (SEPINF/DITEC, 2011). A segunda é um conceito genérico. Entende-se ser o provimento de acesso remoto ao conteúdo do material computacional apreendido pela equipe de investigação.

Em relação às iniciativas não comerciais, é relevante mencionar a existência das ferramentas denominadas *SleuthKit/Autopsy Forensic Browser, Foremost* e *Scalpel.*

O *SleuthKit* é uma coleção de ferramentas de linha de comando que permitem investigar o sistema de arquivos de dispositivos de armazenamento de dados computacionais. Por sua vez, a ferramenta *Autopsy Forensic Browser* é uma interface gráfica para o *SleuthKit* (SleuthKit/Autopsy, 2011).

A ferramenta *Foremost* é um programa de linha de comando para recuperar arquivos de dispositivos de armazenamento de dados computacionais com base em seus cabeçalhos, rodapés e estruturas internas (Foremost, 2011).

A ferramenta *Scapel,* assim como o *Foremost,* é um programa de linha de comando para recuperar arquivos de dispositivos de armazenamento de dados computacionais com base em seus cabeçalhos, rodapés e estruturas internas (Scalpel, 2011).

No que tange às iniciativas comerciais, é relevante enfatizar a existência das ferramentas *EnCase* da *Guidance Software, Inc*. (EnCase Forensic, 2011) e *FTK* da *AccessData Corp*. (Access Data, 2011).

Em síntese, o FTK é uma ferramenta que integra um grande numero de funcionalidades aplicáveis à investigação digital, a maior parte delas dedicada a análise de dispositivos de armazenamento de dados computacionais. Segundo seus desenvolvedores, é reconhecida em todo o mundo como o padrão em *software* de computação forense. As

versões mais recentes incluem processamento distribuído, análise colaborativa, gerenciamento centralizado de casos e outros recursos projetados com o objetivo de tornar mais ágil a investigação digital.

A ferramenta Encase é descrita por seus idealizadores como uma solução forense completa e poderosa, utilizada para analisar uma variedade de dispositivos computacionais. A ferramenta inclui funções de aquisição de dados, recuperação de arquivos, pesquisa e análise de dados, além de outras funcionalidades (EnCase Forensic, 2011).

3.2.1. Aspectos Relacionados ao Emprego das Ferramentas

As ferramentas forenses apresentadas carecem de características que as especializem no processo investigatório de análise da informação, abordado no Capítulo 2, Seção 2.4.1. Elas tampouco suportam dimensões básicas e fundamentais àquele processo de análise, como, por exemplo, locais das apreensões, alvos, equipe responsável pela diligência policial e outros dados relevantes à cognição na atividade policial, principalmente no caso de investigações complexas, envolvendo múltiplos alvos e ações perpetradas em diferentes localizações, por exemplo.

Além do mais, corroboram os administradores da Pericia Criminal Federal, que as ferramentas não oferecem recursos capazes de trabalhar, de forma eficiente os mais de 6.000 discos rígidos e computadores arrecadados anualmente em diversas investigações policiais (INC/DITEC, 2010) (INC/DITEC, 2011).

3.2.2. Uma Nova Geração de Ferramentas

Segundo Nicole Beebe, uma nova geração de ferramentas forense deve ser capaz de oferecer respostas mais eficientes para os novos desafios da computação forense na atualidade. Entre os desafios frequentemente mencionados estão o tratamento com grandes volumes de dados, as grandes quantidades de mídias de armazenamento de dados comumente envolvidas em processos investigatórios e a frequente expansão da capacidade de armazenamento das mídias computacionais (Beebe N. L., 2009).

Na ótica de Beebe, uma alternativa para oferecer respostas ao grande volume de dados é a adoção de métodos seletivos de coleta. Outras soluções sugeridas para tornar mais eficiente o tratamento com grandes volumes de informação incluem processamento

analítico distribuído, processos de buscas baseados em mineração de dados, análise colaborativa geograficamente distribuída e classificação de arquivos para facilitar o processo de análise.

A pesquisadora enfatiza ainda que as abordagens computacionais atuais para busca, recuperação e análise isolada de evidências digitais são simplistas e fortemente dependentes do esforço de um investigador. Ela afirma também que as novas ferramentas devem prover-se de 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 (Beebe N. L., 2009).

Segundo Simson L. Garfinkel, 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 a concepção de soluções que adotem arquiteturas modulares, modelos alternativos de análise, processamento paralelo e recursos de colaboração e automatização de processos, entre outros pontos (Garfinkel, 2010).

Na visão de Daniel Ayers, 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, para originar a construção de uma solução modular com entradas e saídas claramente definidas (Ayers, 2009).

3.3. CONSIDERAÇÕES

Este Capítulo apresentou modelos de processo e ferramentas aplicáveis à investigação digital, pontuando suas limitações. Tais modelos de processo e ferramentas forenses, mesmo quando desenvolvidos observando requisitos de um ou mais países, naturalmente podem deixar de observar particularidades existentes em outros. No caso

especifico do Brasil, os modelos e as ferramentas possuem limitações que restringem sua aplicação na polícia judiciária brasileira, não oferecendo uma solução adequada à investigação digital no Brasil, causando o afastamento de investigadores do possível material probatório ou limitando seu acesso a eles.

O Capítulo também abordou os trabalhos de *Beebe* (Beebe N. L., 2009), *Garfinkel* (Garfinkel, 2010) *e Ayers* (Ayers, 2009), acerca de uma nova geração de ferramentas forenses. Os referidos pesquisadores influenciaram positivamente este trabalho, à medida que os seus conceitos lançaram desafios que foram enfrentados durante os estudos.

O Capítulo 4 discorre sobre a proposta desta pesquisa, apresentando a metodologia e a arquitetura do ferramental. Ambos concebidos para oferecer resposta ao problema de pesquisa apresentado na Seção 1.1, do Capítulo 1.

4. PROPOSTA DO TRABALHO

Neste Capítulo é apresentada a proposta desta pesquisa, com foco na sistematização e instrumentação dos trabalhos periciais e de análise da informação digital, para tornar mais ágil e eficiente a apuração de crimes. A Seção 4.1 apresenta a metodologia proposta, enquanto que a Seção 4.2 descreve a arquitetura para o instrumental especializado.

4.1. METODOLOGIA PROPOSTA

As investigações policiais criminais contemporâneas se deparam com um grande desafio: desenvolver de forma ágil o conhecimento que conduza à elucidação de crimes, tanto a partir dos elementos de provas e de informação tradicionais, quanto a partir das novas e numerosas fontes de informação eletrônica. A natureza dinâmica do cometimento de crimes, a ubiquidade de computadores, a estruturação das organizações criminosas, a transnacionalidade ou interestadualidade do delito tornam esta uma tarefa ainda mais complexa.

Antes de propor procedimentos e instrumentos, é relevante revisar que no Brasil, conforme apresentado no Capítulo 3, a investigação policial é um trabalho em equipe, multidisciplinar por natureza, que envolve peritos criminais e investigadores, formalizada pelo inquérito policial, uma fase pré-processual da persecução penal. O conceito de crime informático enfatiza três classificações: crime centrado no computador, crimes auxiliados por computador, crimes com o envolvimento incidental do computador. Ainda, conceitua-se a investigação policial como uma atividade que busca estabelecer a verdade acerca de um fato, num esforço para conhecer determinada coisa que está oculta, oferecendo provas admissíveis em juízo.

A metodologia proposta observa os requisitos abaixo:

1) Observar as fronteiras das atribuições de investigadores e de peritos criminais: criar os meios para que cada qual desempenhe de forma ampla e autônoma suas atribuições na investigação policial criminal;
2) Viabilizar que documentos tradicionais e eletrônicos sejam submetidos a um único processo de análise da informação;

3) Observar as exigências legais para admissibilidade em juízo da prova digital: prover os meios para que a prova digital seja apresentada, de tal sorte que possam ter verificada sua integridade, autenticidade e procedência;

4) Apresentar, de forma ágil, os documentos eletrônicos para viabilizar a realização das investigações: para conduzir investigações policiais, os investigadores, em certos casos, necessitam de informações que estão sob domínio dos próprios investigados. Nesses casos, diligências de busca e apreensão, devidamente autorizadas pela autoridade competente, são realizadas para que investigadores alcancem tais informações. No caso de informações em formato digital, intangíveis por natureza, contidas nos computadores apreendidos, faz-se necessário um procedimento eficaz para apresentar, de forma célere ao apuratório, os documentos eletrônicos produzidos pelo usuário do computador;

5) Viabilizar a análise da informação de forma colaborativa e geograficamente distribuída: a atividade de investigação é, via de regra, um trabalho multidisciplinar realizado em equipe. Investigadores que possuem os conhecimentos necessários à condução do processo investigatório de análise de informações muitas vezes estão geograficamente dispersos. Se, mesmo dispersos puderem colaborar em análises, a investigação policial será favorecida;

6) Viabilizar as análises que permeiem a investigação: um agente cognoscente depende da disponibilidade de dados e de experiências prévias para formar conhecimento. Dados que a princípio são irrelevantes podem se tornar fundamentais para elucidação do delito, em outro momento das investigações;

7) Evitar o descarte prematuro de dados: descartar dados considerados irrelevantes é condição irremediável, que compromete a formação posterior de conhecimento a partir dos dados descartados. Em um momento futuro das investigações podem vir a existir a condição que permitiria identificar a real relevância da informação descartada;

8) Viabilizar a triagem de materiais (identificação daqueles ligados ao delito dentre os demais arrecadados): otimizar o uso dos recursos humanos e materiais, minorando o esforço da Perícia pelo aumento da assertiva de quais materiais estão de fato relacionados ao crime em apuração;

9) Viabilizar a automatização de tarefas periciais e investigatórias: prover os meios para, por intermédio do emprego da tecnologia, tornar mais ágeis os trabalhos de peritos criminais e investigadores;

4.1.1. Visão Geral

O processo foi estruturado em 2 partições, 4 segmentos, 4 fases, 2 subfases e 18 atividades, conforme estruturado abaixo:

1) Partição: Investigadores
    a. Segmento: Planejamento
        - Atividade: Estratégia e Abordagem
    b. Segmento: Investigação
        i. Fase: Análise e cotejo
            - Atividade: Elaborar premissa
            - Atividade: Elaborar hipóteses
            - Atividade: Definir estratégias
            - Atividade: Obter os documentos eletrônicos (buscas)
            - Atividade: Reunir documentos
            - Atividade: Analisar (hipóteses, premissas, documentos)
            - Atividade: Elaborar relatórios de análise

2) Partição: Peritos Criminais

    c. Segmento: Apresentação de dados

        i. Fase: Extração de Dados

            - Atividade: Preparação em observância aos princípios da cadeia de custódia
            - Atividade: Aquisição
            - Atividade: Extração de documentos eletrônicos
            - Atividade: Montagem dos repositórios

        ii. Fase: Descoberta de Dados

            - Atividade: Reconhecimento por padrões
            - Atividade: Reconhecimento de vínculos
            - Atividade: Reconhecimento de artefatos

    d. Segmento: Exames Periciais

        i. Fase: Exame Pericial em Informática ou outro ramo do conhecimento científico

            - Subfase: Exame pericial em informática
                a. Atividade: Coleta
                b. Atividade: Exame
                c. Atividade: Formalização
            - Subfase: Exame pericial em outro ramo do conhecimento científico

A figura 4.1 representa o nível geral do processo proposto. As partições denominadas investigadores e peritos criminais delimitam a atuação de cada ator. Os segmentos planejamento, apresentação de dados, investigação e exames periciais delineiam o ponto em que cada ator participa do processo.

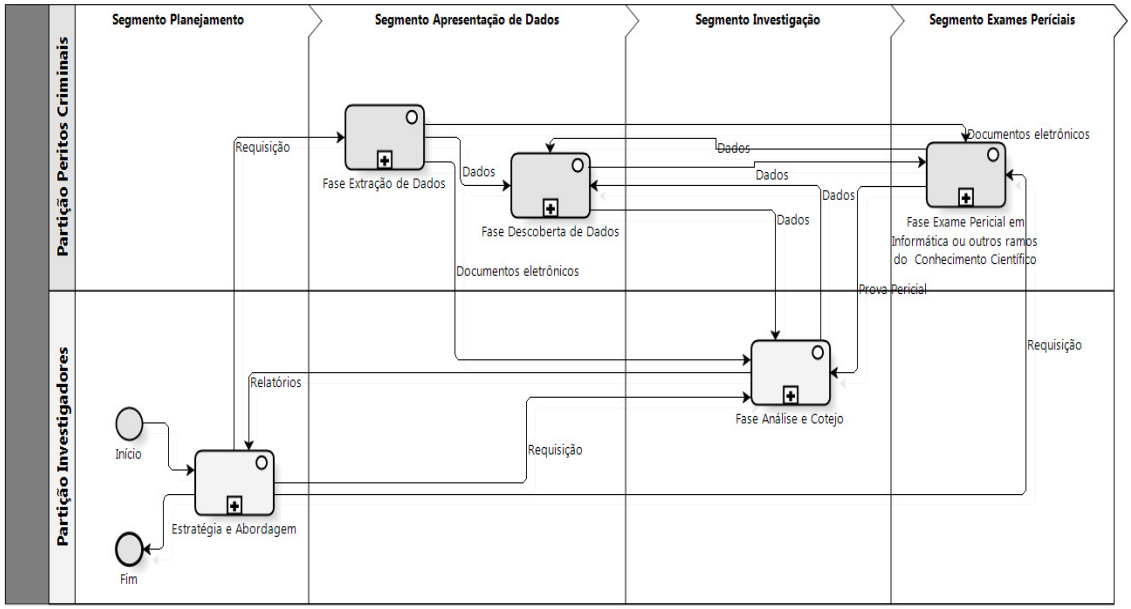

Figura 4.1 – Modelo Proposto

4.1.2. Segmento Planejamento

O segmento planejamento está a cargo de investigadores. Ele é composto da atividade denomina estratégia e abordagem. Foi concebido para permitir a coordenação da investigação policial criminal, estabelecendo a forma como serão organizados os trabalhos na apuração de um determinado delito. Alguns crimes podem requerer exclusivamente a análise da informação contida em documentos eletrônicos. Outros, exclusivamente a perícia nos materiais apreendidos. Ainda podem existir aqueles que requeiram as duas ações.

4.1.3. Segmento Apresentação de Dados

O segmento apresentação de dados está a cargo de peritos criminais. Foi concebido para apresentar ao apuratório os documentos e criar os elementos que permitirão assegurar verificações futuras da integridade, autenticidade e procedência destes documentos eletrônicos. Em conjunto com a cadeia de custódia, são fundamentais em contendas relacionadas à validade da prova digital ou ao repúdio desta em qualquer das etapas da persecução penal.

Para que os documentos eletrônicos possam ser apresentados para os investigadores, é necessário o envio formal do material apreendido a uma unidade de Perícia Oficial. No primeiro momento a unidade de pericia oficial procederá a descrição do material e sua preservação, o que permitirá a extração segura do conteúdo do material apreendido. Para desempenhar essa tarefa os peritos se utilizarão de conhecimento especializado sobre as fragilidades e os riscos associados às evidências digitais, valendo-se dos componentes do ferramental de uso típico da função pericial. Este trabalho visa a garantia da cadeia de custódia de provas, da procedência, da integridade e da autenticidade dos documentos eletrônicos repassados à equipe de investigação e à Justiça.

Num segundo momento, uma fase de descoberta de dados visará apoiar a identificação de documentos possivelmente relevantes ao apuratório. Para desempenhar essa tarefa os peritos interagirão com os componentes (agentes inteligentes) do ferramental. O produto desta fase é também disponibilizado para análise por investigadores. Este trabalho visa identificar subconjuntos de documentos, utilizando-se de técnicas e procedimentos automatizados, especializados em explorar grandes volumes de dados, procurando por arquivos que atendam a certos padrões, que possuam determinadas estruturas, que apresentem certas características, que possuam relacionamentos sistemáticos demonstrando possíveis ligações entre alvos (vínculos), entre outros possíveis.

As fases aqui descritas estão detalhadas nas subseções que seguem.

4.1.3.1. Fase de Extração de Dados

A fase de extração de dados é composta por quatro atividades, como apresentado na figura 4.2. Ela apresenta as ações de alto nível sugeridas para a execução do trabalho pericial que antecede os trabalhos de análise da informação.

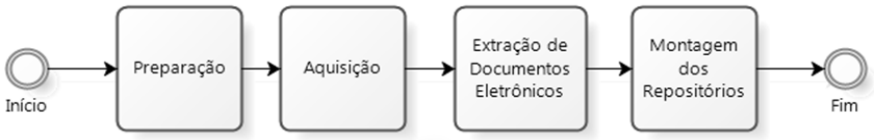

Figura 4.2 – Apresentação de dados ao apuratório

A fase é de responsabilidade de peritos criminais, ela estrutura os trabalhos de extração e disponibilização de documentos eletrônicos da seguinte forma:

1) Preparação: Objetiva reunir, caracterizar e organizar o processamento dos materiais que terão o conteúdo extraído. A tabela 4.1 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.1 - Preparação

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Materiais arrecadados • Requisição de disponibilização de dados • Auto de arrecadação • Priorização de alvos	• Análise minuciosa das características dos materiais • Análise da priorização definida	• Caracterização dos materiais • Mapa de Alvos x Materiais • Estratégias e ordem de priorização para processamento dos materiais arrecadados

2) Aquisição: Submeter os materiais aos procedimentos periciais de proteção e preservação para a realização de cópia forense. A tabela 4.2 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.2 - Aquisição

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Materiais arrecadados • Caracterização dos materiais • Mapa de Alvos x Materiais • Estratégias e ordem de priorização para processamento dos materiais arrecadados	• Componente Aquisitor	• Imagem forense (cópia bit-a-bit)

3) Extração de documentos eletrônicos: uma vez concluída a cópia forense de um dos materiais arrecadados, as extrações poderão ser iniciadas automaticamente. A tabela 4.3 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.3 - Extração

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Imagem forense • Caracterização dos materiais • Mapa de Alvos x Materiais • Estratégias e ordem de priorização para processamento dos materiais arrecadados	• Componente Extrator	• Documentos eletrônicos (artefatos) • Caracterização dos documentos eletrônicos extraídos (Metadados)

4) Montagem dos repositórios: As montagens de repositórios poderão ser executadas automaticamente logo após a conclusão das extrações. A tabela 4.4 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.4 - Montagem do Repositório

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Caracterização dos materiais • Mapa de Alvos x Materiais • Estratégias e ordem de priorização para processamento dos materiais arrecadados • Documentos eletrônicos (artefatos) • Caracterização dos documentos eletrônicos extraídos (Metadados)	• Componente montador	• Carga do repositório de arquivos • Carga do repositório central (metadados)

4.1.3.2. Fase de Descoberta de Dados

A fase de descoberta de dados é composta por três atividades, como apresentado na figura 4.3. Ela apresenta as ações de alto nível sugeridas para a execução de trabalhos que auxiliam na identificação de dados e informações relevantes para a análise investigatória da informação. Tem por objetivo processar grandes volumes de dados e permitir identificar padrões, vínculos e documentos que poderiam passar despercebidos pelos investigadores.

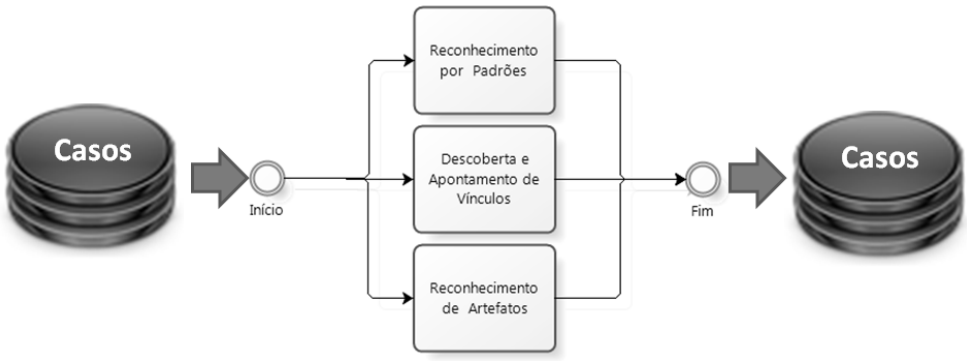

Figura 4.3 - Descoberta de Dados

A fase estrutura os trabalhos de descoberta de dados da seguinte forma:

1) Reconhecimento por padrões: As análises de padrões são concebidas para identificar artefatos que se enquadrem em certas características previamente definidas. Por exemplo: buscar por combinações de palavras-chave existentes em pontos determinados do artefato para identificar aqueles possivelmente relacionados a declarações de imposto de renda, balancetes ou balanços contábeis. A tabela 4.5 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.5 - Reconhecimento por padrões

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Documentos eletrônicos (artefatos) • Caracterização dos documentos eletrônicos extraídos (Metadados) • Parâmetros definidos	• Componente reconhecedor	• Relação de arquivos reconhecidos

2) Reconhecimento de vínculos: O reconhecimento de vínculos entre alvos (no mesmo caso e entre casos) é concebido para identificar possíveis ligações entre investigados. Por exemplo: uma mensagem eletrônica trocada entre pessoas, autoria de artefatos, artefatos reconhecidos como relacionados aos fatos investigados que existem idênticos em computadores de outros alvos. A tabela 4.6 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.6 - Reconhecimento de vínculos

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Documentos eletrônicos (artefatos) • Caracterização dos documentos eletrônicos extraídos (Metadados) • Caracterização dos materiais • Mapa de Alvos x Materiais • Dados conhecidos de alvos • Dados da investigação • Dados de artefatos relevantes identificados	• Componente Vinculador	• Relação de vínculos descobertos

3) Reconhecimento de arquivos: As análises de arquivos são concebidas para identificar artefatos previamente conhecidos, idênticos ou aproximados. Por exemplo: buscar por figuras conhecidas envolvendo crianças ou adolescentes em condições sexuais ou nus. A tabela 4.7 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.7 - Reconhecimento de arquivos

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Documentos eletrônicos (artefatos) • Caracterização dos documentos eletrônicos extraídos (Metadados) • Dados de artefatos conhecidos	• Componente reconhecedor	• Relação de arquivos reconhecidos

4.1.4. Segmento de Investigação

O segmento investigação está a cargo de investigadores e foi concebido para conferir os meios que permitirão a realização da análise da informação.

4.1.4.1. Fase de Análise e Cotejo

A fase de análise e cotejo é composta por sete atividades, como apresentado na figura 4.4.. Ela apresenta as ações de alto nível sugeridas para a execução do trabalho de análise da informação, acrescido de inovações para explicitar, dirigir e gerenciar as ações de análise e registro do conhecimento produzido durante a investigação policial.

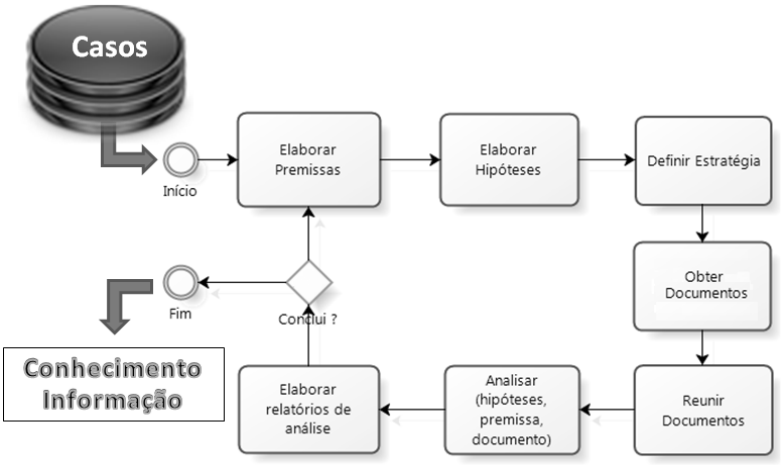

Figura 4.4 - Análise da informação

O procedimento de análise da informação digital estrutura as análises investigatórias da seguinte forma:

1) Elaborar premissas: Elaboram-se premissas que orientarão a investigação na busca por documentos que conduzam informações relevantes ao apuratório. As premissas irão antecipar, por deduções ou conjeturas, certas características da conduta investigada. Por exemplo: uma proposição do tipo "Tício participa da intermediação fraudulenta de benefícios previdenciários" ou "Tício gerencia os "laranjas" que participam do esquema." Irá orientar que se estabeleçam hipóteses que permitam encontrar documentos apontando para os fatos investigados. A tabela 4.8 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.8 - Elaborar premissas

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Dados conhecidos de alvos • Dados conhecidos da conduta investigada	• Componente de analisador	• Premissas da investigação

2) Elaborar hipóteses: Definem-se hipóteses, 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. A tabela 4.9 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.9 - Elaborar hipóteses

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Dados conhecidos de alvos • Dados conhecidos da conduta investigada • Premissas da investigação	• Componente analisador	• Hipóteses da investigação

3) Definir estratégias de buscas: Definem-se as estratégias de buscas a serem utilizadas. Por exemplo: buscas textuais, buscas semânticas, buscas em pastas ou buscas por fotografias, figuras ou outros arquivos gráficos. A tabela 4.10 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.10 - Definir estratégia de buscas

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Dados conhecidos de alvos • Dados conhecidos da conduta investigada • Premissas da investigação • Hipóteses da investigação • Mapa de Alvos x Materiais	• Componente analisador	• Estratégias de buscas definidas

4) Obter documentos: Procedem-se as buscas, utilizando-se das hipóteses, das premissas estabelecidas, dos termos de buscas e das técnicas escolhidas. Optando-se pelo uso do recurso de buscas textuais, os termos de pesquisa poderiam conter os seguintes fragmentos de texto:

   a. O endereço do sítio da previdência e dados da página de agendamento.
   b. Dados de laranjas conhecidos (Mércio) e endereço do sítio da previdência.
   c. O endereço de email de alvos.
   d. Dados conhecidos por intermédio de escutas telefônicas ou de oitivas relacionados ao Tício.

e. Dados obtidos de documentos tradicionais já analisados e considerados relevantes.
f. As palavras-chave “contrato”, “ Tício” e “Mércio”.

A tabela 4.11 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.11 - Obter Documentos

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Dados conhecidos de alvos • Dados conhecidos da conduta investigada • Premissas da investigação • Hipóteses da investigação • Mapa de Alvos x Materiais • Estratégias de buscas definidas	• Componente analisador • Componente minerador	• Documentos eletrônicos por analisar

5) Reunir os documentos: Organizam-se as análises de conteúdos dos resultados das buscas, estruturam-se as equipes de buscas e distribuem-se os trabalhos de análise entre os investigadores, de acordo com a técnica ou técnicas de busca escolhidas. Iniciam-se as análises dos resultados de buscas e/ou de contêineres de buscas em pasta ou buscas por fotografias ou outros arquivos em formato gráfico. Adicionam-se os documentos encontrados aos contêineres de hipóteses correspondentes. Documentam-se os conhecimentos adquiridos, retroalimentando o processo de buscas por documentos relevantes. A tabela 4.12 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.12 - Reunir os documentos

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Dados conhecidos de alvos • Dados conhecidos da conduta investigada • Premissas da investigação • Hipóteses da investigação • Mapa de Alvos x Materiais • Estratégias de buscas definidas • Documentos eletrônicos por analisar	• Componente analisador	• Documentos eletrônicos relevantes ao investigatório • Considerações do analista acerca do conhecimento adquirido com a análise do documento encontrado

6) Analisar (hipóteses, premissas e documentos): Analisa-se o conhecimento reunido nos contêineres de hipóteses, formando-se as conclusões possíveis. A tabela 4.13 relaciona suas principais entradas e saídas, além de relacionar as técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.13 - Analisar (hipóteses, premissas e documentos)

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Dados conhecidos de alvos • Dados conhecidos da conduta investigada • Premissas da investigação • Hipóteses da investigação • Mapa de Alvos x Materiais • Documentos eletrônicos relevantes ao investigatório • Considerações do analista acerca do conhecimento adquirido com a análise do documento encontrado	• Componente analisador	• Conclusões da investigação

7) Elaborar relatórios: Caso exista um conhecimento formado, elabora-se o relatório de análise para aportar os resultados do processo investigatório de análise na investigação criminal. Avalia-se se o conhecimento adquirido sugere a elaboração de novas premissas ou novas hipóteses, retomam-se as análises ou concluem-se 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.

   A tabela 4.14 relaciona suas principais entradas e saídas, além de relacionar as técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.14 - Elaborar relatórios

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Dados conhecidos de alvos • Dados conhecidos da conduta investigada • Premissas da investigação • Hipóteses da investigação • Mapa de Alvos x Materiais	• Componente analisador	• Relatórios de análise • Requisição de perícias • Triagem de materiais

• Documentos eletrônicos relevantes ao investigatório • Considerações do analista acerca do conhecimento adquirido com a análise de documentos encontrados • Conclusões da investigação		identificados como relacionados ao apuratório

4.1.5. Segmento de Exames Periciais

O segmento de exames periciais está a cargo de peritos criminais e foi concebido para atender a formalização da apresentação de documentos eletrônicos ao apuratório e a requisições de exames periciais elaborados por investigadores durante o andamento da investigação policial.

4.1.5.1. Fase de Exame Especializado

A fase de exame especializado representa os exames periciais em si. É relevante acrescentar que, com a adoção da metodologia proposta, os exames periciais, com base em informações e dados de origem digital, podem demandar, em conjunto com outros dados ou isoladamente, a requisição de exames periciais em informática ou mesmo em outro ramo do conhecimento científico, como contabilidade, por exemplo.

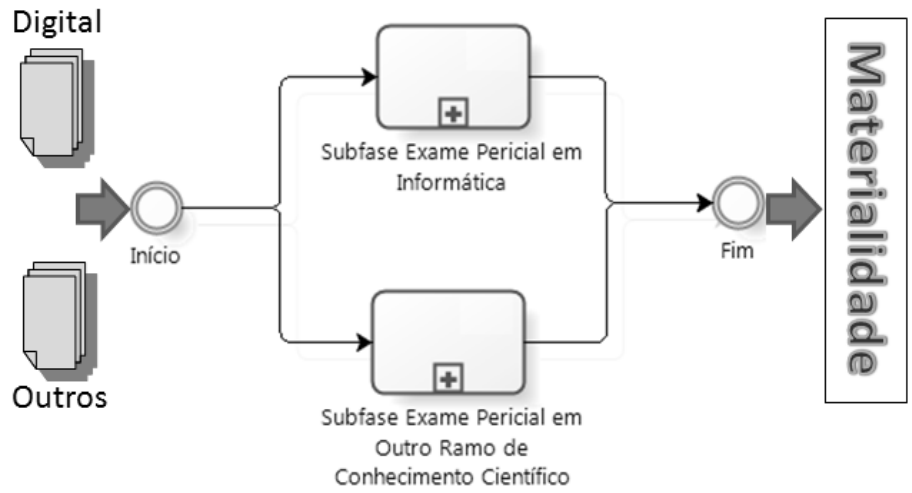

Figura 4.5 - Fase de exames especializados

4.1.5.1.1. A Subfase de Exame Pericial em Informática

A subfase de exame pericial em informática compreende o exame de um ou mais materiais arrecadados, visando responder as inquirições encaminhadas aos peritos

criminais. É composta por 3 atividades principais e apresenta as ações de alto nível sugeridas para a execução do trabalho de exame pericial em informática.

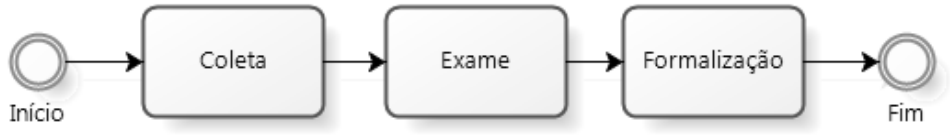

Figura 4.6 - Subfase de exame pericial em informática

O procedimento de exame pericial em informática estrutura os exames periciais da seguinte forma:

1) Coleta: compreende as ações de coleta de vestígios em si. Caso as imagens forenses não estejam mais disponíveis ao perito criminal ou caso este julgue adequado, nova imagem forense do material objeto do exame deverá ser providenciada pelo examinador. A tabela 4.15 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.15 - Coleta

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Materiais por examinar • Requisição de perícias • Auto de arrecadação • Dados conhecidos da investigação	• Componente aquisitor	• Vestígios coletados • Imagens Forenses • Certificação de integridade

2) Exame: compreende o estudo minucioso dos vestígios digitais coletados, a fim de responder as inquirições (quesitos) encaminhadas ao perito criminal. Esta subfase pode expandir-se em várias atividades de grande complexidade. A tabela 4.16 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.16 - Exame

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Materiais por examinar • Requisição de perícias • Auto de arrecadação • Imagem forense • Documentos eletrônicos	• Ferramentas forenses aplicáveis.	• Conclusões tecnocientíficas

relevantes • Dados conhecidos da investigação • Vestígios coletados		

3) Formalização: compreende a elaboração do documento formal (laudo pericial criminal) que conduz os resultados dos exames periciais. A tabela 4.17 relaciona suas principais entradas e saídas, além das técnicas e quais componentes da solução (ferramentas) serão utilizadas para sua execução.

Tabela 4.17 - Formalização

Principais Entradas	Ferramentas e Técnicas	Principais Saídas
• Materiais por examinar • Requisição de perícias • Auto de arrecadação • Imagem forense • Documentos eletrônicos relevantes • Dados conhecidos da investigação • Vestígios coletados • Conclusões tecnocientíficas	• Editores de texto e outras ferramentas aplicáveis	• Laudo Pericial Criminal • Novas diligências

4.1.5.1.2. A Subfase de Exame Pericial em Outro Ramo do Conhecimento

A subfase de exame pericial em outro ramo do conhecimento científico compreende o exame minucioso com base em informações e documentos encontrados nos materiais arrecadados. Visa atender as requisições de perícias de diversos ramos do conhecimento. Pode ser composta de diferentes atividades, dependendo do exame e do ramo em si. Uma abstração foi aqui abordada com o objetivo de enfatizar que dados ou informações em formato digital podem ser relevantes em exames de outro ramo do conhecimento. Como exemplo, os balancetes contáveis e razões de contas, que podem ser relevantes em perícias contábeis; fotografias que podem ser relevantes em perícias que visem identificar pessoas a partir de técnicas de reconhecimentos faciais; gravações de conversas que podem ser submetidas a procedimentos de identificação de locutor etc.

4.1.6. Aspectos relacionados à metodologia proposta

Do ponto de vista de peritos criminais, a metodologia proposta tem dois objetivos. O primeiro é orientar a extração de documentos eletrônicos existentes no material

apreendido, apresentando-os para que sejam analisados por investigadores. O segundo é orientar a realização de exames periciais requisitados, a fim de alcançar a prova pericial.

Do ponto de vista de investigadores, a metodologia proposta visa estruturar o processo de análise da informação[19], a partir dos documentos eletrônicos apresentados por peritos criminais.

A concepção da metodologia se baseou em:

1) No processo de análise da informação, apresentado na Seção 2.4.1;
2) Em pontos das propostas descritas por *Palmer*, em 2001 (Palmer, 2001) e por *Kohn*, *Eloff* e *Olivier*, no ano de 2006 (Kohn, Eloff, & Oliver, 2006), apresentadas na Seção 3.1;
3) Na experiência do pesquisador no desempenho de suas funções de Perito Criminal Federal no Departamento de Polícia Federal.

4.2. ARQUITETURA PARA O INSTRUMENTAL ESPECIALIZADO

Representado graficamente na figura 4.7, uma arquitetura foi concebida para nortear o desenvolvimento de um ferramental forense especializado, tanto na disponibilização de documentos eletrônicos ao apuratório, quanto no suporte ao processo de análise investigatória da informação, contribuindo para a busca pela excelência na produção de provas.

[19] O processo de análise da informação foi conceituado no Capítulo 2, Seção 2.4.1.

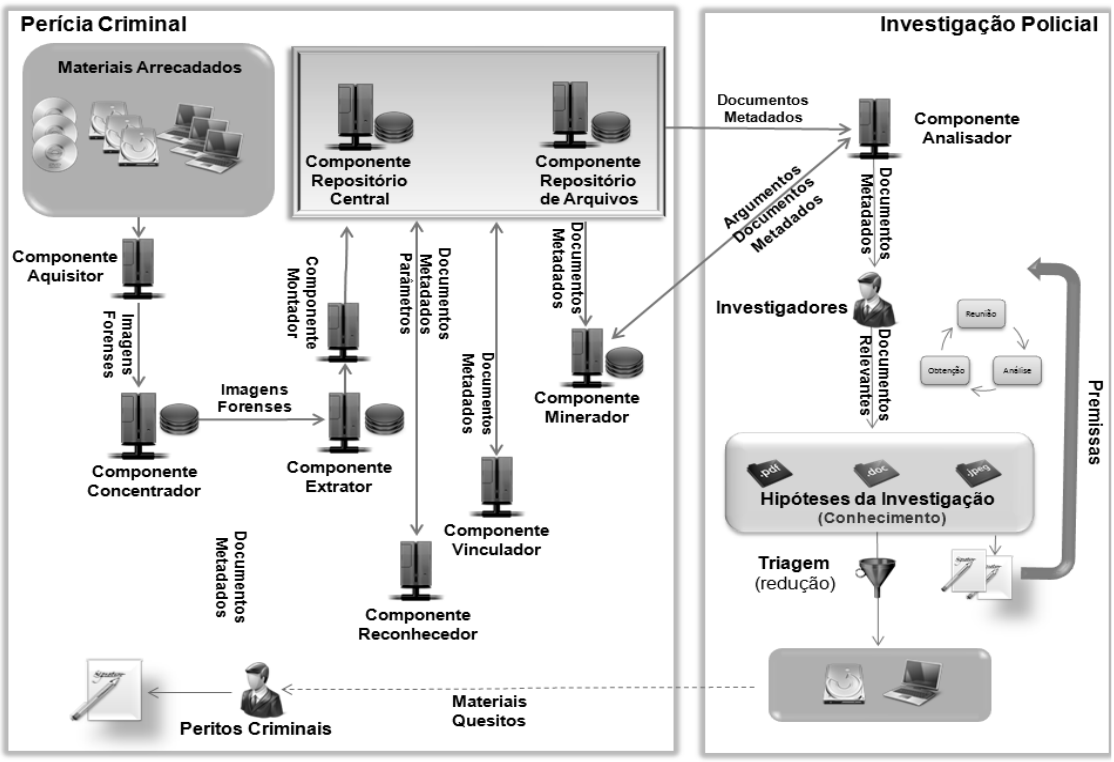

Figura 4.7 - Arquitetura Proposta

A proposta pode ser operacionalizada em um ferramental que considere características desejáveis em soluções para tratar problemas complexos e que envolvam grandes volumes de dados. Em particular, ela orienta o desenvolvimento de procedimentos e ferramentas que empreguem componentes[20] com as seguintes características:

1) 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.);

2) Análise investigatória colaborativa e geograficamente distribuída: a análise investigatória pode ser realizada no contexto da investigação criminal, por investigadores organizados em equipe de análise, composta, inclusive, por membros geograficamente distribuídos.

3) Componentes autônomos e especializados: visando paralelismo e eficiência, um conjunto de componentes (ou agentes)

[20] Entenda-se por componentes qualquer agente humano ou construído em software, hardware ou uma combinação deles, com um propósito ou conjunto de propósitos definidos.

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;

4) 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;

4.2.1. O Componente Aquisitor de cópias Forenses

Representado graficamente na figura 4.8, o componente aquisitor foi projetado para sistematizar e permitir a automatização da criação de cópias forenses. Ele opera de forma autônoma e assíncrona em relação aos demais componentes da solução.

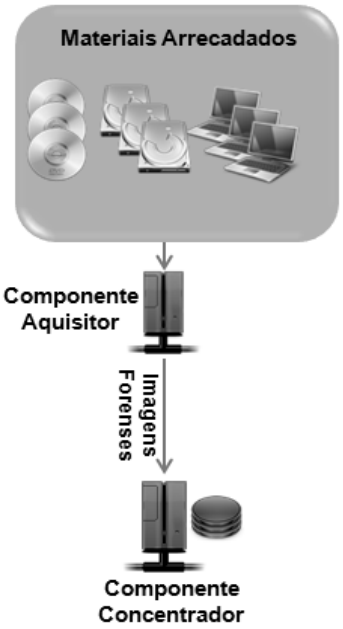

Figura 4.8 - Componente Aquisitor

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.

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 são capazes 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, por exemplo, está em dividir o grupo de dez aquisitores, utilizados no exemplo anterior, em 5 grupos compostos, cada um, por 2 aquisitores e 1 componente concentrador. Neste caso, distribui-se a E/S, a carga de transmissão de dados e de processamento entre os 5 componentes concentradores, 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, fundamentais à cadeia de custódia.

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.

4.2.2. O Componente Concentrador

Representado graficamente na figura 4.9, o componente concentrador fornece um repositório onde os componentes aquisitores armazenam as cópias forenses que serão posteriormente processadas por componentes extratores, podendo ser um simples servidor de arquivos, um NAS - *Network-Attached Storage,* um servidor de *storage* de alto desempenho e alta capacidade etc.

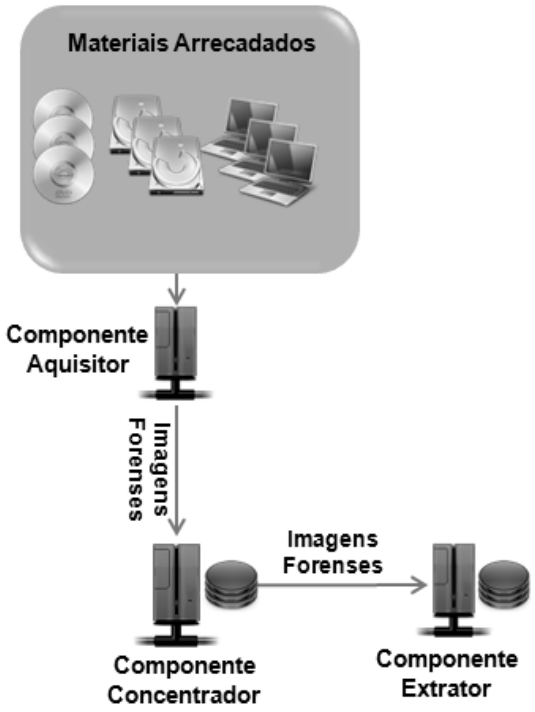

Figura 4.9 - Componente Concentrador

4.2.3. O Componente Autônomo Extrator de Documentos Eletrônicos

Representado graficamente na figura 4.10, o componente extrator trabalha de forma autônoma e assíncrona, extraindo documentos eletrônicos de imagens forenses armazenadas em um componente concentrador. Para que um componente extrator possa iniciar suas atividades, basta que uma nova imagem forense esteja disponível no concentrador.

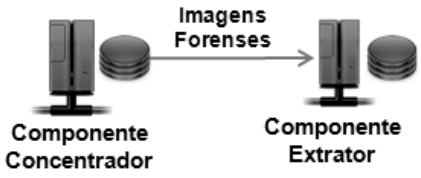

Figura 4.10 - Componente Extrator

Diversos componentes extratores podem trabalhar simultaneamente de forma independente. Quanto maior o número de componentes extratores, maior será a capacidade produtiva.

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. A seção 4.3.6 descreve o componente Minerador.

4.2.4. O Componente Autônomo Montador

Representado graficamente na figura 4.11, o componente montador trabalha de forma autônoma e assíncrona. Ele disponibiliza os documentos eletrônicos e demais metadados que serão utilizados pelos componentes minerador, reconhecedores e analisador. Para que um componente montador possa iniciar suas atividades, basta que uma extração tenha sido concluída pelo componente extrator. Diversos componentes montadores podem trabalhar simultaneamente de forma independente. Quanto maior o número de componentes montadores, maior será a capacidade produtiva.

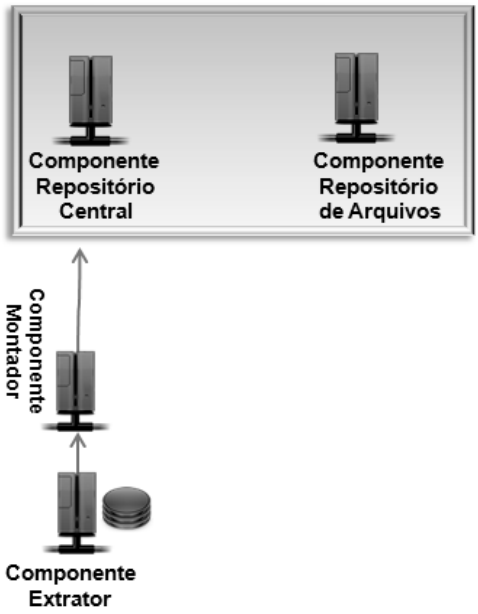

Figura 4.11 - Componente Montador

4.2.5. O Componente de Gerenciamento de Investigações

A solução proposta organiza investigações em casos, que são contêineres lógicos que agrupam diversos elementos. Os 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 membros de equipe de análise. 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) Metadados: São dados que descrevem um determinado documento eletrônico extraído de seu suporte, como por exemplo, nome, autor, e datas de criação e modificação;
4) Artefatos: Representam os documentos eletrônicos extraídos de materiais;
5) Premissas: São proposições que devem ser investigadas para alcançar uma conclusão. Premissas dão origem aos termos de buscas;

6) Termos de buscas: São palavras-chave ou conceitos utilizados para procurar artefatos eletrônicos;

7) Resultados de buscas: São contêineres lógicos que organizam os artefatos eletrônicos resultantes de pesquisas por fragmentos textuais;

8) Árvore de diretórios ou estrutura de pasta e subpastas: São contêineres lógicos que organizam os documentos eletrônicos resultantes de suportes;

9) Repositórios de arquivos em formato gráfico: São contêineres lógicos que organizam fotografias e outros arquivos gráficos, resultantes de suportes;

10) 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;

11) Dossiês: São contêineres lógicos que reúnem as diversas hipóteses de um caso.

4.2.6. O Componente de Mineração de Dados

Representado graficamente na figura 4.12, o componente de mineração de dados funciona de forma independente e assíncrona em relação ao demais componentes da solução.

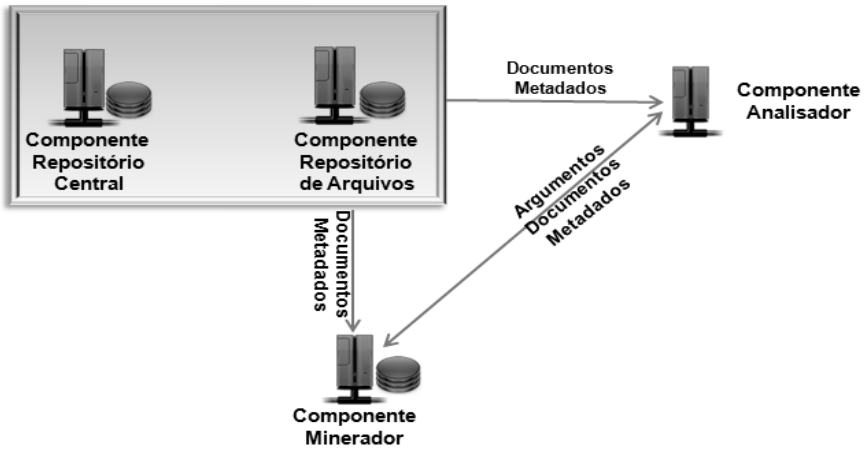

Figura 4.12 - Componente de Mineração de Dados.

A mineração de dados foi concebida para operar na retaguarda do ferramental e é composta 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 trabalhar 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 conjunto de banco de dados de índices, o que garante que as buscas de um caso não apresentem por resposta os documentos de outro caso.

O ferramental pode ser estruturado com diversos componentes de mineração de dados, para aumentar a capacidade de processamento, armazenamento de dados e distribuição de processos.

4.2.7. O Componente Vinculador

Representado graficamente na figura 4.13, o componente vinculador foi concebido para operar de forma independente e assíncrona em relação ao demais componentes da solução. 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. Assim, 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.*" (Ferro Júnior, 2008).

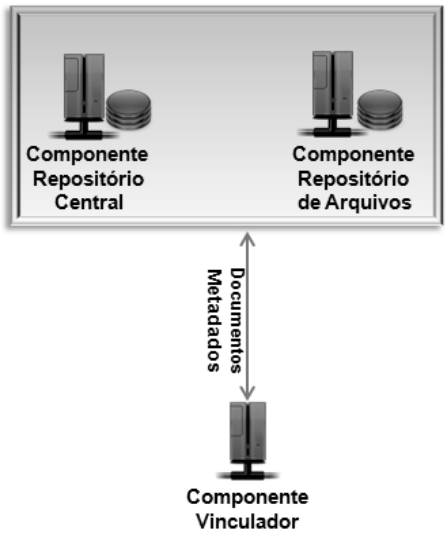

Figura 4.13 - Componente Vinculador

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

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.

4.2.8. O Componente Reconhecedor

Representado graficamente na figura 4.14, 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.

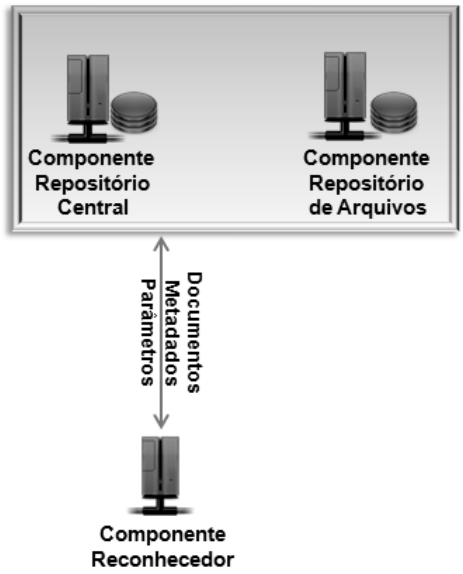

Figura 4.14 - Componente Reconhecedor

Um 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-chave em certas posições do texto, ou mesmo a partir de um banco de dados com assinaturas de arquivos conhecidos. Diversos componentes reconhecedores podem trabalhar de forma independente. Ampliando-se o número de componentes reconhecedores operando simultaneamente, poder-se-á ampliar a capacidade produtiva da solução.

4.2.9. O Componente Repositório de Arquivos

Representado graficamente na figura 4.15, o componente repositório de arquivos possui as seguintes funções essenciais:

1) Reunir os documentos eletrônicos extraídos de materiais arrecadados;
2) Prover um serviço de comunicação entre o componente repositório de arquivos e o componente de análise. Ele intermedia o acesso restrito aos

documentos eletrônicos de um caso. Somente investigadores membros da equipe de análise devem ter acesso aos documentos.

Figura 4.15 - Componente Repositório de Arquivos

4.2.10. O Componente Repositório Central

Representado graficamente na figura 4.16, o componente repositório central possui as seguintes funções essenciais:

1) Reunir os metadados de documentos eletrônicos de cada caso;
2) Reunir dados de auditoria de uso do ferramental;
3) Reunir relações de documentos eletrônicos resultantes de buscas por fragmentos textuais ou buscas semânticas;
4) Reunir dados de controle do ferramental (usuários investigadores, equipes de investigação, senhas e privilégios de acesso, etc.).

Figura 4.16 - Componente Repositório Central

4.2.11. O Componente de Análise Investigatória da Informação

Representado graficamente na figura 4.17, o componente de análise investigatória de informação foi concebido para permitir a integração e interação entre a perícia criminal e a investigação, minorando assim as diferenças apontadas no processo de análise da 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 subsidiar a cognição, a partir destas fontes de dados, na atividade policial.

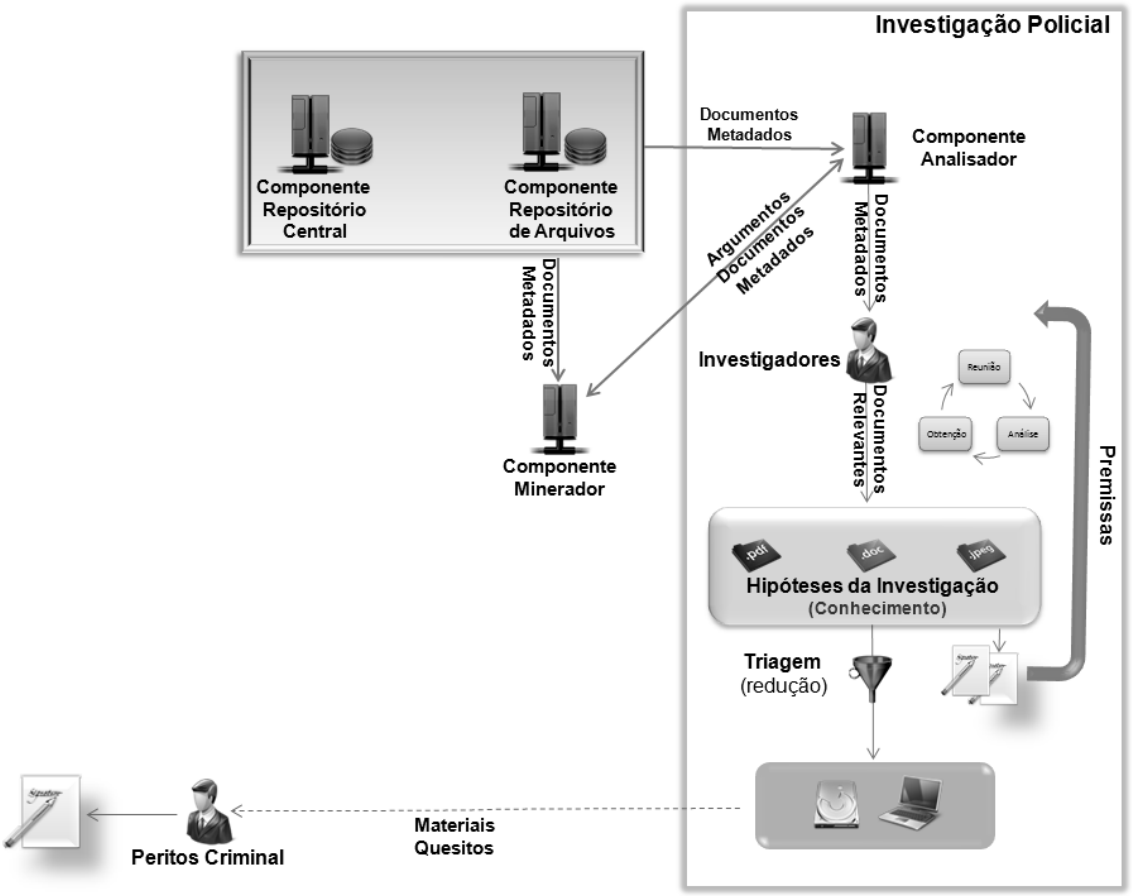

Figura 4.17 - Componente de Análise

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 documentos necessários estarão à disposição para início do ciclo de análises. As análises de documentos eletrônicos ou tradicionais poderão permear, conjuntamente, a investigação criminal pelo tempo necessário à condução do apuratório.

O componente de análises foi concebido para ser utilizado por meio de uma interface gráfica 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.

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 identificação de documentos relevantes, maximizando a geração de conhecimento no apuratório.

Durante as análises os investigadores poderão relacionar seus achados em contêineres lógicos de hipóteses, fazendo anotações que visem explicitar e compartilhar o conhecimento adquirido entre os membros de sua equipe de investigação. Dessa forma, o conhecimento tácito dos investigadores se transforma em conhecimento explícito do órgão policial, permitindo que novos investigadores possam estudar detidamente o atual estágio das análises investigatórias e, desta maneira, sejam integrados à equipe de investigação com rapidez e eficiência.

A qualquer tempo durante as análises investigatórias ou ao seu final, poder-se-á requisitar periciais criminais em razão das necessidades da persecução penal. A perícia requisitada pode ser de qualquer dos ramos do conhecimento científico, como contabilidade, informática, engenharia civil, engenharia elétrica etc.

4.2.12. Aspectos Relacionados à Arquitetura Proposta

A arquitetura proposta se propõe a orientar o preenchimento de uma lacuna deixada pelas ferramentas forenses no trato com a investigação digital, no Brasil, bem como introduzir um novo paradigma no desenvolvimento de ferramentas aplicadas à investigação policial criminal.

Seus principais recursos são:

1) Distribuição de processos: processos podem ser distribuídos por inúmeros componentes. Isto é, a solução pode trabalhar com diversos componentes dos tipos aquisitores, concentradores, extratores etc., de forma autônoma e simultânea, para maximizar a capacidade produtiva da solução;

2) Análise colaborativa e geograficamente distribuída permeando a investigação criminal: análises podem ser realizadas por diversos investigadores simultaneamente, mesmo se estiverem geograficamente

dispersos, entre diferentes delegacias, cidades, estados etc. Os documentos eletrônicos permanecem disponíveis para os analistas durante todo o ciclo da investigação policial, até sua conclusão;

3) Composição de força tarefas de análise entre instituições: as equipes de investigação não precisam estar compostas exclusivamente por investigadores do órgão policial. Outros profissionais, de outras instituições, podem trabalhar em conjunto com os investigadores policiais, compondo uma força tarefa.

4) Exportação e distribuição de caso para análise externa à instituição policial: após a geração de um caso, compreendendo a aquisição de imagens forenses e a extração de documentos eletrônicos, o componente de análise pode ser enviado para análise externa pelo Ministério Público, Judiciário ou outra instituição, como a Receita Federal ou o Instituto Nacional do Seguro Social;

5) Análise simultânea de múltiplos materiais: o componente de análise trabalha, simultaneamente, com os diversos materiais arrecadados durante a investigação, dispensando que os trabalhos de análise tenham que ser realizados material por material ou em pequenos grupos de materiais.

6) Arquitetura modular: decomposição de um problema complexo em parte mais simples - com entradas e saídas claramente definidas;

7) Gerenciamento centralizado de casos: embora vários investigadores possam trabalhar de forma colaborativa durante as análises investigatórias, o gerenciamento do caso estará centralizado;

8) Compartimentação sigilosa: os dados de uma investigação são restritos à equipe da investigação;

9) Automatização de tarefas: minimização da intervenção humana em tarefas passíveis de mecanização/automação;

10) Agendamento de processos: definição de processamentos em retaguarda, como indexação, análises de vínculos ou reconhecimento de padrões, por exemplo;

11) Disponibilização seletiva e ágil de dados para viabilizar a realização das investigações: extração e disponibilização de documentos tipicamente produzidos por usuários de um sistema computacional;

12) Processos de buscas baseados em mineração de dados: processos que revelem tendências para dados e informações que seriam indetectáveis ou dificilmente percebidas somente por uma análise e observação humana;

13) Classificação de arquivos para facilitar o processo de análise: estruturação de classes de arquivos, como documentos, planilhas, figuras etc.

O ferramental resultante, em razão de sua característica modular, poderá ser operacionalizado com tantos componentes quanto o apropriado para alcançar a eficiência necessária, dispondo ou não de um computador dedicado a cada componente. Este é um dos pontos fortes da arquitetura que lhe confere expansibilidade e versatilidade.

4.3. CONSIDERAÇÕES

A metodologia e arquitetura proposta permitem uma clara separação do que seja o trabalho de investigadores e peritos criminais na investigação digital, observando as peculiaridades da polícia judiciária brasileira. Juntas contribuem para que seja atingido, de forma mais célere, o objetivo que justificou a arrecadação de equipamentos computacionais: a formação do conhecimento sobre um fato investigado, a instrução da investigação criminal correspondente e a aquisição de provas, documentais e/ou periciais.

Este Capítulo descreveu o instrumental proposto para concretizar os objetivos desta dissertação. O Capítulo 5 apresenta os testes realizados em casos reais, bem como seus resultados.

5. PROVA DE CONCEITOS

Neste Capítulo é apresentado um protótipo desenvolvido com base na arquitetura proposta para o instrumental especializado. A metodologia proposta e o protótipo desenvolvido foram submetidos a teste em investigações policiais reais, visando verificar as potencialidades da solução e provar os conceitos apresentados nesta pesquisa. A Seção 5.1 apresenta um protótipo do ferramental proposto, enquanto que na Seção 5.2 são apresentados testes em casos reais. Por fim, são realizadas considerações que seguem na Seção 5.3.

5.1. PROTÓTIPO

O escopo de desenvolvimento do protótipo compreendeu os componentes descritos na arquitetura, exceto os componentes de reconhecimento, vinculação e a busca semântica do componente de mineração de dados. O ferramental resultante foi denominado Uiraçu[21].

5.1.1. Componentes Autônomos Aquisitor e Concentrador

Em síntese, o componente aquisitor automatiza a criação de cópias forenses de dispositivos de armazenamento de dados. Para armazenar tais cópias, um componente concentrador é utilizado, interconectado diretamente ao componente aquisitor, conforme descrito no Capítulo 4.

Representado pela figura 5.1, um conjunto compreendendo dois protótipos aquisitores e um concentrador foi capaz de, simultaneamente, realizar e armazenar 2 cópias forenses[22], a uma velocidade de processamento de até 2 gigabytes por minuto, com uma

[21] O Uiraçu é o nome indígena de uma grande ave de rapina, que impressiona por sua velocidade de voo, ferocidade e grande força. Também conhecida por Ave de Crista, Gavião-real ou, ainda, Harpia. A ave é capaz de caçar macacos, preguiças e outros animais de porte médios. Tal fabulosa ave está na lista de animais em extinção. Seu nome foi escolhido para batizar o protótipo, provas dos conceitos apresentados neste trabalho, em razão do local onde esta pesquisa foi iniciada: O estado do Pará, na região Amazônica brasileira.

[22] Os primeiros protótipos dos componentes aquisitor e concentrador trabalham com discos rígidos, em virtude deste tipo de dispositivo possuir maior significância em relação ao volume de documentos eletrônicos que armazenam.

autonomia que compreende o processamento, sem intervenções humanas, de até 10 discos rígidos[23] por ciclo de trabalho.

Figura 5.1 – Dois Aquisitores (esquerda) e um Concentrador

A tabela 5.1 apresenta a capacidade de processamento estimada para o conjunto de protótipos aquisitores e concentrador. Observa-se que, em razão da característica autônoma do componente de aquisição, a capacidade de armazenamento dos discos rígidos alvos do processo de cópia forense, mesmo quando variando entre 240 e 500GB, não comprometeriam a capacidade produtiva da solução de aquisição em um período de 24 horas[24].

Tabela 5.1 - Estimativa linear da capacidade de processamento (2 aquisitores)

Disco Rígido (gigabyte)	Produção de cópias por ciclo	Duração do processamento de um dispositivo (minutos)	Duração total do ciclo de processamento (horas)	Qtde. de intervenções durante às 8h do expediente de trabalho	Capacidade produtiva de cópias /dia	Capacidade produtiva de cópias / semana
120	10	60	5	2	20	100
240	10	120	10	1	10	50
320	10	160	14	1	10	50
400	10	200	17	1	10	50
500	10	250	21	1	10	50

[23] Um componente de aquisição (*hardware*) construído especificamente para está função poderia ser capaz de alcançar capacidade produtiva bem superior e maior autonomia de processamento.
[24] Considerando um pleno funcionamento dos materiais submetidos aos aquisitores.

5.1.2. Componente Autônomo Extrator

Em síntese, o componente extrator opera automaticamente a extração de documentos eletrônicos para as cópias forenses que encontrar disponíveis no componente concentrador, conforme descrito no Capítulo 4. A figura 5.2 exemplifica o componente em execução.

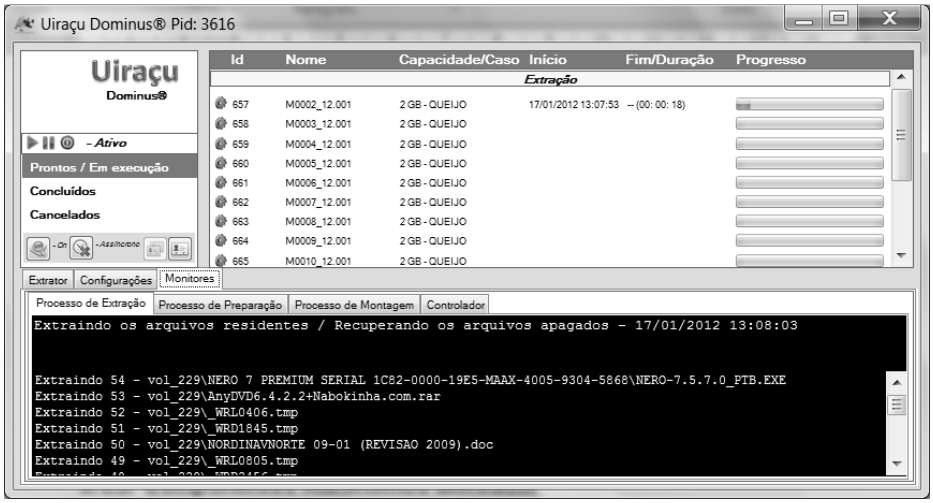

Figura 5.2 – Extrator

5.1.3. Componente Autônomo Montador

Em síntese, o componente montador opera automaticamente a montagem dos repositórios para os documentos eletrônicos extraídos de cópias forenses, conforme descrito no Capítulo 4. A figura 5.3 exemplifica o componente em execução.

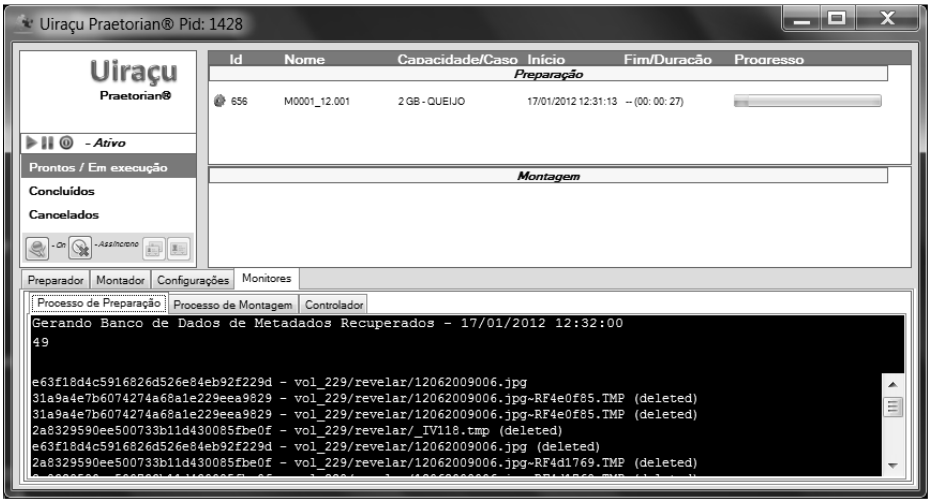

Figura 5.3 – Montador

5.1.4. Componente Análise Investigatória da Informação

Em síntese, o componente de análise investigatória da informação, disponibilizado através de uma interface gráfica em rede privada, permite que investigadores geograficamente dispersos, em cidades ou até estados diferentes, trabalhem de forma colaborativa, no mesmo caso, buscando e avaliando o conteúdo de documentos eletrônicos.

As principais funcionalidades deste componente são: buscas textuais, analisador de arquivos, simulador de sistema de arquivo, analisador de figuras, documentos digitalizados e fotografias digitais.

5.1.4.1. Buscas textuais

Em síntese, a funcionalidade de buscas textuais, representada na figura 5.4, opera simultaneamente em todos os documentos de um caso, utilizando-se de recursos providos pelos componentes mineradores e repositórios. Juntos, os componentes disponibilizam um serviço de busca que permite pesquisas em grandes volumes de dados[25], utilizando-se de critérios definidos pelos investigadores.

O resultado de cada pesquisa é persistido e permanece armazenado no instrumental por tempo indeterminado, compondo um conjunto de contêineres de buscas. Tais contêineres são compartilhados entre investigadores para que possam ter seus itens analisados de forma minuciosa, possibilitando a exploração profunda do material probatório.

Um contêiner de busca possui diversas dimensões que categorizam seus itens. Como, por exemplo:

1) Equipe: corresponde a identificação das equipes policiais que arrecadaram cada material;
2) Item: corresponde a identificação dos itens arrecadados;
3) Alvo: corresponde a identificação do alvo da busca e apreensão;

[25] O buscador *Google* da *Google Inc*., por exemplo, disponibiliza um serviço análogo que visa auxiliar na pesquisa de conteúdos na internet.

4) Arrecadação: corresponde a identificação do local das diligências policiais;

5) Categoria do documento: email, planilha, figura etc.;

6) Tipo do documento: docx, pptx, etc.

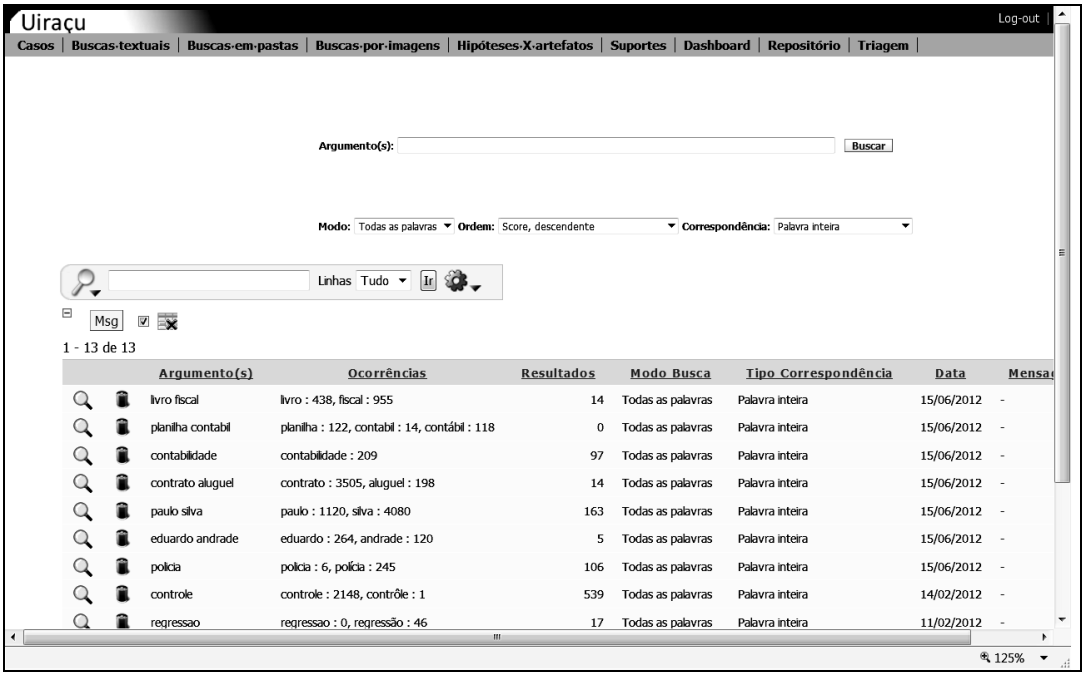

Figura 5.4 - Buscas Textuais

Cada documento eletrônico que compõe um contêiner de busca pode ser examinado sem que as fontes possam ser alteradas pelos examinadores. A figura 5.5 apresenta a interface de análise.

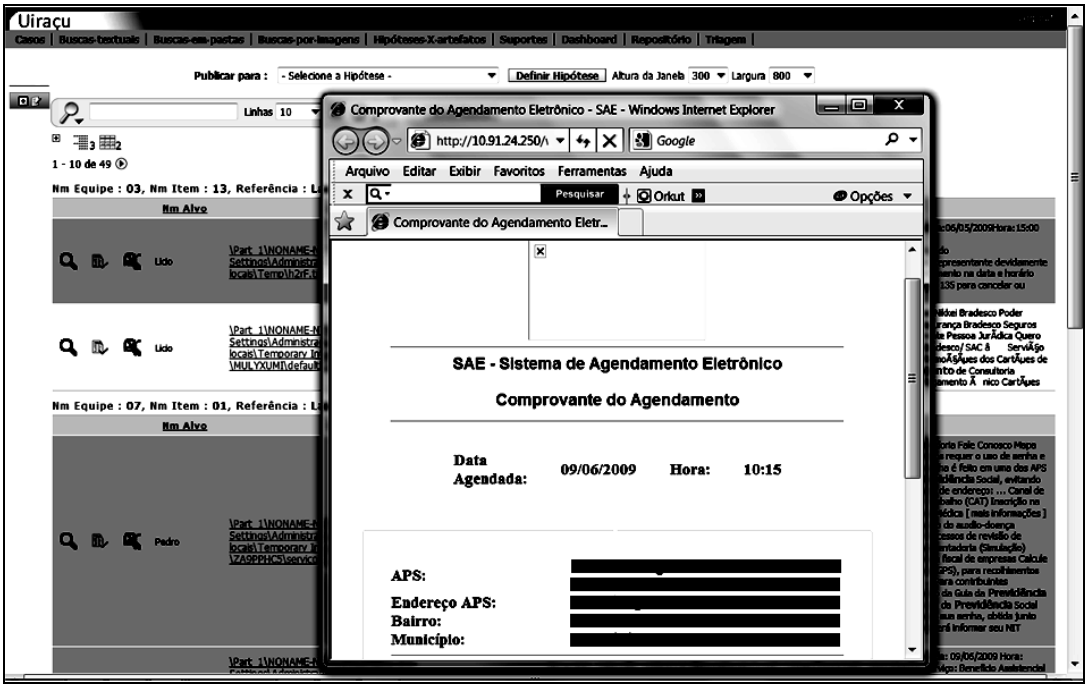

Figura 5.5 - Funcionalidade de Análise

5.1.3.2. Simulador de sistema de arquivos

A funcionalidade de simulação de sistema de arquivos, apresentada na figura 5.6, permite aos investigadores uma visão simulada do ambiente computacional onde residem os documentos eletrônicos obtidos pelo componente de extração. Tais documentos podem ser analisados de forma colaborativa geograficamente distribuída como se os investigadores estivem utilizando o ambiente computacional analisado.

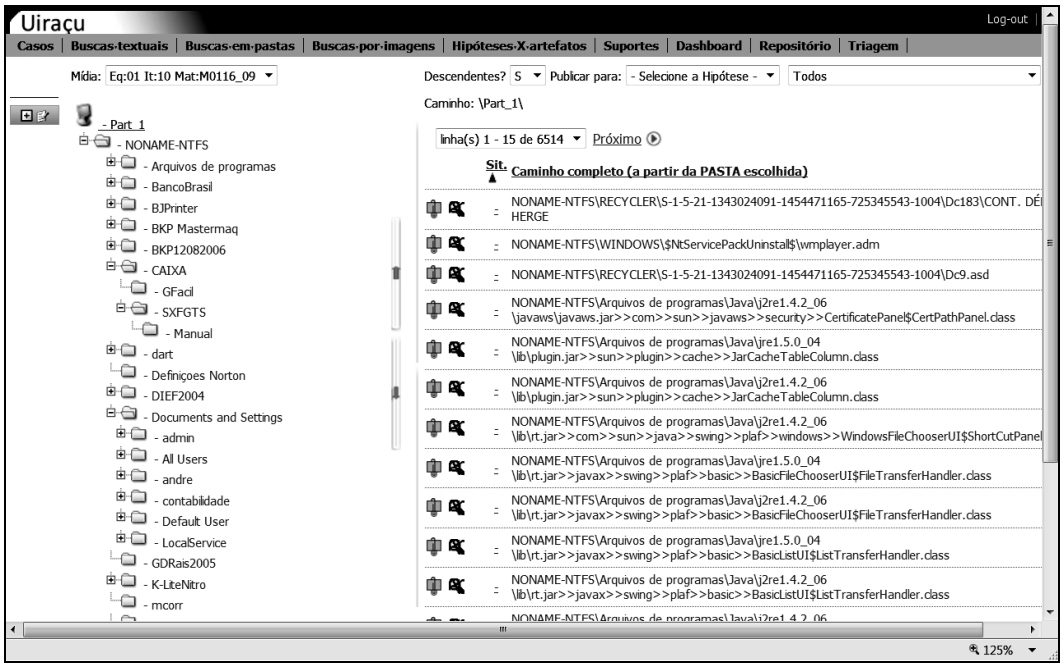

Figura 5.6 - Simulador do Sistema de Arquivos

5.1.3.3. Analisador de figuras e fotografias digitais

A funcionalidade de análise de figuras e fotografias digitais, apresentada na figura 5.7, permite explorar os arquivos em formato gráfico, utilizando-se de uma matriz de exibição configurável (linhas/colunas e filtros de exibição).

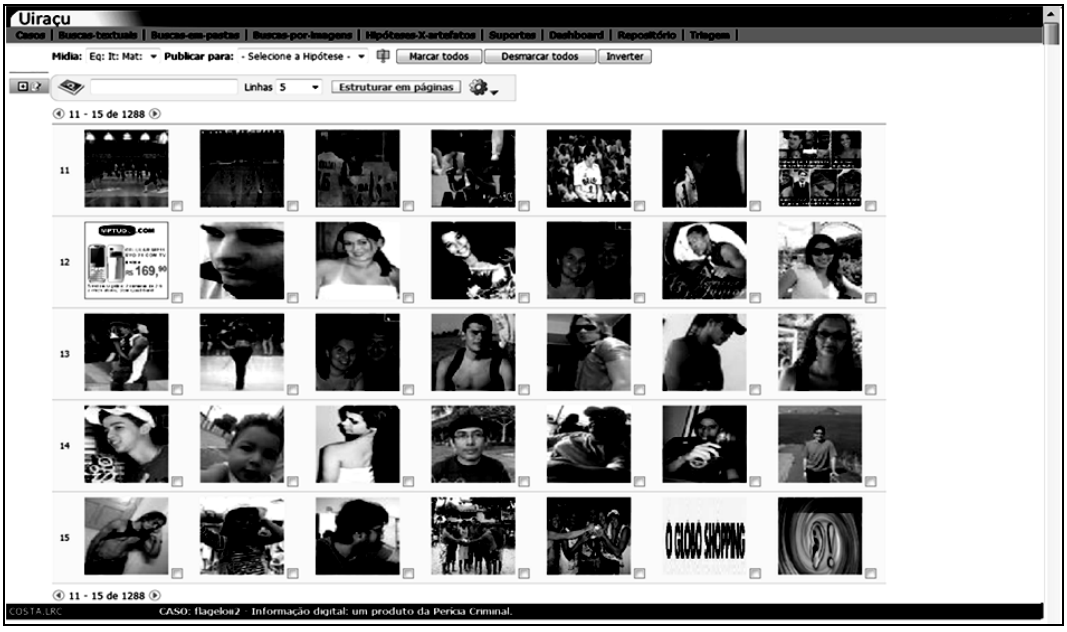

Figura 5.7 - Analisador de figuras e fotografias digitais

5.1.3.4. Demais Componentes

Os componentes de gerenciamento de investigações, repositório de arquivos, repositório central e minerador de dados, como descrito no Capítulo 4, operam na retaguarda do ferramental interagindo com os componentes montador e análise investigatória da informação. O protótipo do componente minerador de dados suporta diversos formatos de arquivos comumente produzidos por usuário. E, ainda, pode ser estendido, com relativa facilidade, para trabalhar com novos formatos de arquivos.

5.2. TESTES EM CASOS REAIS

Visando por a prova os conceitos concebidos na pesquisa e verificar as potencialidades da solução desenvolvida, o ferramental e a metodologia foram utilizados em investigações policiais reais e de grande porte, em duas Superintendências de Polícia Federal, nos estados da Bahia e do Pará.

Embora as configurações dos *hardwares* utilizados naquelas Superintendências de Polícia Federal sejam diferentes, a implementação da arquitetura é idêntica, contando com 3 equipamentos para operacionalizar a solução, estruturada com uma única instância de cada componente. A figura 5.8 apresenta o esquema posto em prática, uma abordagem minimalista dos recursos da arquitetura proposta.

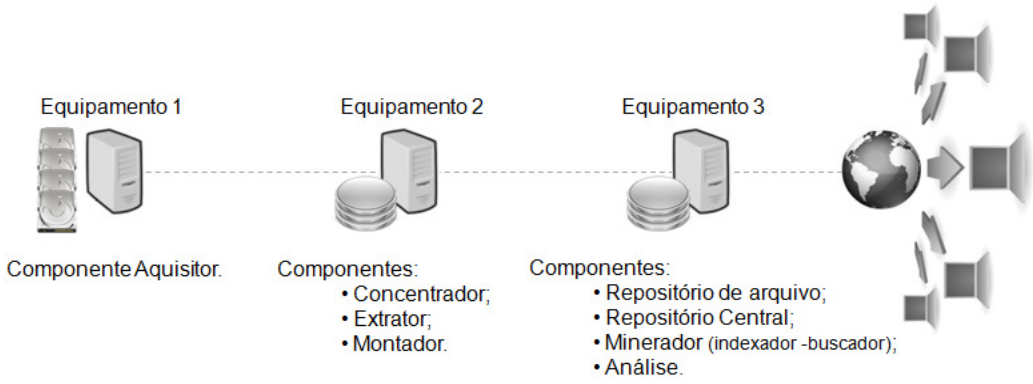

Figura 5.8- Esquema da configuração posta em prática para prova de conceitos.

5.2.1. Disponibilização de dados ao apuratório

Definida a estratégia e abordagem dos trabalhos investigatórios, etapa da metodologia correspondente ao segmento planejamento, descrito na Seção 4.1.2, os materiais arrecadados foram enviados a peritos criminais para que disponibilizassem os documentos eletrônicos, que seriam, posteriormente, explorados durante o processo de análise da informação.

Para disponibilizar os documentos fez-se uso da fase de extração de dados, do segmento de apresentação de dados da metodologia proposta, descrito na Seção 4.1.3.1. A etapa, prevista como atribuição de peritos criminais, serviu também para prover[26] meios[27] que tem por objetivo afastar quaisquer dúvidas que o magistrado, futuramente, possa ter, acerca da integridade e procedência de provas de origem eletrônica. Foram utilizados, também, os componentes aquisitor, concentrador, extrator e montador do ferramental forense especializado[28], visando automatizar certas frações dos trabalhos de peritos criminais.

Os documentos eletrônicos extraídos dos materiais processados foram disponibilizados para análise pelos investigadores a cada disco rígido processado. Mesmo antes de concluir todas as extrações de documentos, os investigadores já puderam ter acesso ao conteúdo dos materiais já processados. O caso, no entanto, só estaria completo após o processamento de todos os materiais.

Objetivando avaliar os resultados alcançados, os seguintes indicadores foram utilizados:

1) O tempo médio despendido para conclusão de Laudos que disponibilizam documentos eletrônicos ao apuratório: Para chegar a esse indicador conhecesse que, durante o ano de 2011, foram produzidos 9.130[29] Laudos, e que 180 peritos da área de Informática Forense estiveram em atividade neste período (INC/DITEC, 2012). O que resulta em uma produção média anual de 51 laudos por perito, cerca de 4 por

[26] Desde que tenha sido resguardada a manutenção adequada da cadeia de custódia, desde o momento de coleta das possíveis fontes de prova até que sejam trabalhadas pelo perito criminal.
[27] Por intermédio de documento técnico-científico, por exemplo.
[28] Em razão do natural aperfeiçoamento do instrumental, evoluções de componentes e da metodologia ocorreram entre as operações policiais, objetivando maximizar o resultado final da pesquisa.
[29] Estão agrupados nesta totalização, tantos os Laudos de apresentação de dados, quanto os demais, como aqueles referentes à pedofilia, fraudes bancárias e outros.

mês. Implicando que a cada 7 dias, aproximadamente, o exame de um disco rígido teria sido concluído;

2) O lapso temporal médio necessário à completa conclusão de uma requisição de perícias em informática: 157 dias[30] (INC/DITEC, 2012).

Tem-se, também, que a Diretoria Técnico-Científica do Departamento de Policia Federal publicou a Instrução de Serviço 008/2011-DITEC, de 23 de novembro de 2011, onde preestabeleceu indicadores de complexidade. Segundo os Administradores da Criminalística Federal "*O indicador de* "Complexidade" *das requisições corresponde ao tempo estimado, em dias corridos, para a realização dos exames e a elaboração do documento técnico-científico*" (DITEC/DPF, 2011). A tabela 5.2 apresenta tais indicadores.

Tabela 5.2 - Indicadores oficiais de complexidade (adaptado de DITEC/DPF, 2011).

Nível do indicador de complexidade	Tempo estimado para realização dos exames e confecção do laudo (em dias)
Nível I	$t \leq 0,5$
Nível II	$0,5 < t \leq 3$
Nível III	$3 < t \leq 7$
Nível IV	$7 < t \leq 14$
Nível V	$14 < t \leq 28$
Nível VI	$28 < t \leq 60$
Nível VII	$t > 60$

Cotejando tais indicadores com a duração média calculada para as perícias em Informática Forense – isto é, 7 dias –, poder-se-ia inferir que o nível III, exposto na tabela 5.2, apresenta compatibilidade com o lapso temporal necessário a conclusão deste tipo de exame pericial. Entretanto, como os dados calculados são aproximados serão utilizados para as aferições de desempenho:

1) O intervalo final referente ao nível III dos indicadores. Ou seja, 7 dias.

2) O intervalo final referente ao nível II dos indicadores. Ou seja, 3 dias.

3) O intervalo final referente ao nível I dos indicadores. Ou seja, 0,5 dia. O que representa, por exemplo, um lapso temporal comumente associado a exames preliminares de droga, em razão de sua simplicidade, alcançada

[30] Influi no cálculo deste lapso temporal, o tempo em que a requisição aguardará por atendimento em razão de possível indisponibilidade do efetivo pericial, que pode estar atendendo a outra requisição ou cumprindo missão policial, por exemplo.

em virtude de padronizações de métodos e utilização de reagentes previamente concebidos e preparados.

Os comparativos apresentados nas próximas Seções levam em consideração as seguintes premissas:

1) Os cálculos de esforço foram realizados com base na estimativa de produção de um único perito criminal, trabalhando com as ferramentas e os métodos em uso da instituição policial;
2) Somente um perito criminal foi responsável por trabalhar com a metodologia e o ferramental proposto.

Ressalte-se que os nomes de investigados e operações policiais não serão mencionados em razão da preservação do sigilo das investigações.

5.2.1.1. Operações policiais conduzidas na Bahia

No Estado da Bahia foram conduzidas três investigações policiais que utilizaram a metodologia e o instrumental especializado concebido nesta pesquisa. O resultado de cada teste segue conforme relacionado:

1) Na operação A, que investigou o desvio de verba pública, 258 discos rígidos arrecadados, totalizando aproximadamente 35 terabytes, tiveram o conteúdo disponibilizado pelo instrumental em 60 dias.
2) Na operação B, que investigou a exploração de jogos de azar, 50 discos rígidos arrecadados, totalizando aproximadamente 10 terabytes, tiveram o conteúdo disponibilizado pelo instrumental em 24 dias.
3) Na operação C, que também investigou a exploração de jogos de azar, 32 discos rígidos arrecadados, totalizando aproximadamente 5 terabytes, tiveram o conteúdo disponibilizado pelo instrumental em 9 dias.

Com base nos indicadores apresentado na tabela 5.2 e nos resultados alcançados como o uso do instrumental, é apresentado, na tabela 5.3, um comparativo de esforço para extração e disponibilização de documentos eletrônicos.

Tabela 5.3 - Comparativo de esforço para extração e disponibilização de documentos (Bahia).

Operação	Dimensão (terabytes)	Discos rígidos (qtde)	Esforço estimado Nível I (dias)	Esforço estimado Nível II (dias)	Esforço estimado Nível III (dias)	Esforço realizado (dias)	Proporção do esforço estimado nível I	Proporção do esforço estimado nível II	Proporção do esforço estimado nível III
A	35	258	129	774	1806	60	46,51%	7,75%	3,32%
B	10	50	25	150	350	24	96,00%	16,00%	6,86%
C	5	32	16	96	224	9	56,25%	9,38%	4,02%

A figura 5.9 demonstra graficamente o comparativo apresentado na tabela 5.3.

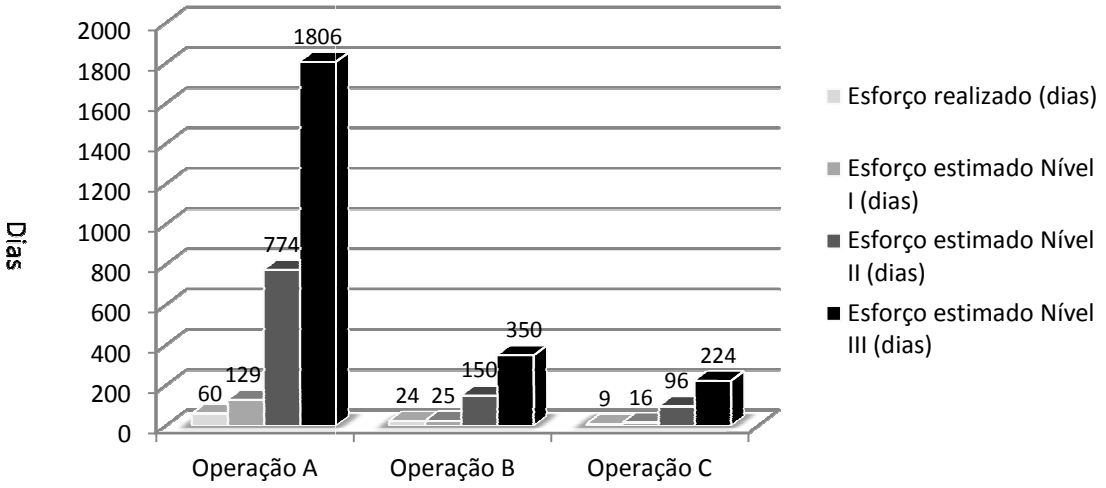

Figura 5.9 - Comparativo de esforço para disponibilização de dados.

5.2.1.2. Operações policiais conduzidas no Pará

No Estado do Pará foram conduzidas três investigações policiais que utilizaram a metodologia e o instrumental especializado concebido nesta pesquisa. O resultado de cada teste segue conforme relacionado:

1) Na operação D, que investigou o desvio de verba pública, 3 discos rígidos arrecadados, totalizando aproximadamente 0,3 terabytes, tiveram o conteúdo disponibilizado pelo instrumental em 1 dia.

2) Na operação E, que investigou crime previdenciário, 41 discos rígidos arrecadados, totalizando aproximadamente 8 terabytes, tiveram o conteúdo disponibilizado pelo instrumental em 27 dias.

3) Na operação F, que investigou o desvio de verba pública, 57 discos rígidos arrecadados, totalizando aproximadamente 4 terabytes, tiveram o conteúdo disponibilizado pelo instrumental em 12 dias.

Com base nos indicadores apresentado na tabela 5.2 e nos resultados alcançados como o uso do instrumental, é apresentado, na tabela 5.4, um comparativo de esforço para extração e disponibilização de documentos eletrônicos.

Tabela 5.4 - Comparativo de esforço para extração e disponibilização de dados (Pará).

Operação	Dimensão (terabytes)	Discos rígidos (qtde)	Esforço estimado nível I para um PCF (dias)	Esforço estimado nível II para um PCF (dias)	Esforço estimado nível III para um PCF (dias)	Esforço realizado com o instrumental por um PCF (dias)	Proporção do esforço realizado em relação ao nível I	Proporção do esforço realizado em relação ao nível II	Proporção do esforço realizado em relação ao nível III
D	0,3	3	1,5	9	10,5	1	66,67%	11,11%	9,52%
E	8	41	20,5	123	143,5	27	131,71%	21,95%	18,82%
F	4	57	28,5	171	199,5	12	42,11%	7,02%	6,02%

A figura 5.10 demonstra graficamente o comparativo apresentado na tabela 5.4.

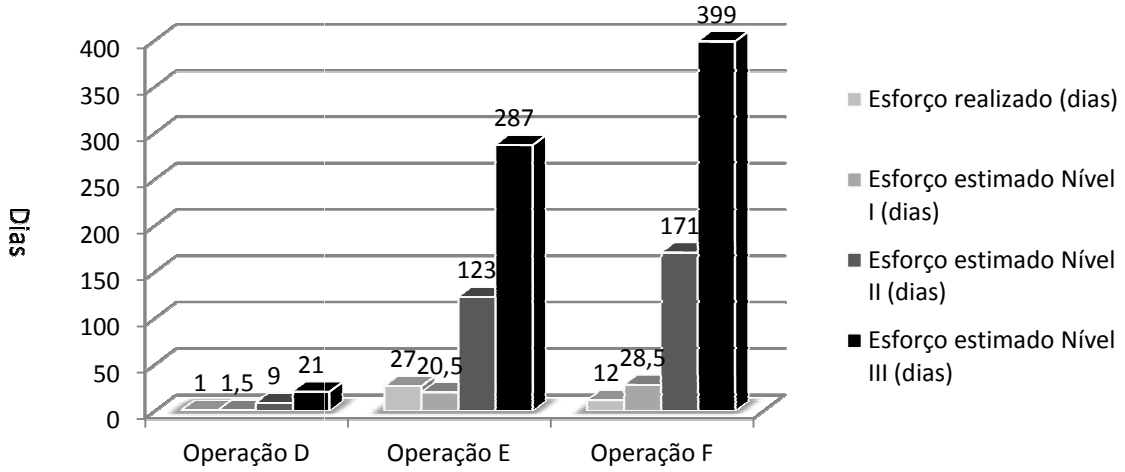

Figura 5.10 - Comparativo de esforço para disponibilização de dados.

5.2.1.3. Eficiência Produtiva Alcançada

A figura 5.11 apresenta a eficiência alcançada em cada uma das 6 operações conduzidas com uso da solução proposta.

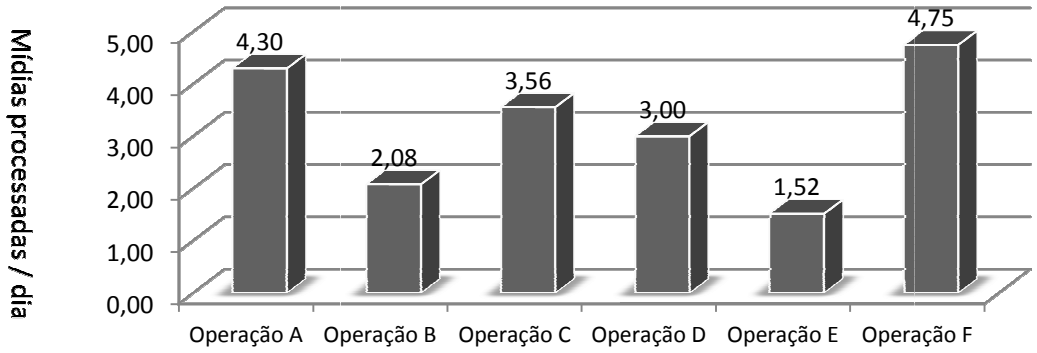

Figura 5.11 - Eficiência alcançada com o uso da solução proposta

Nas operações conduzidas com a solução proposta, as disponibilizações de dados aos apuratórios foram concluídas em um intervalo temporal inferior a 157 dias. Conforme representado na figura 5.12.

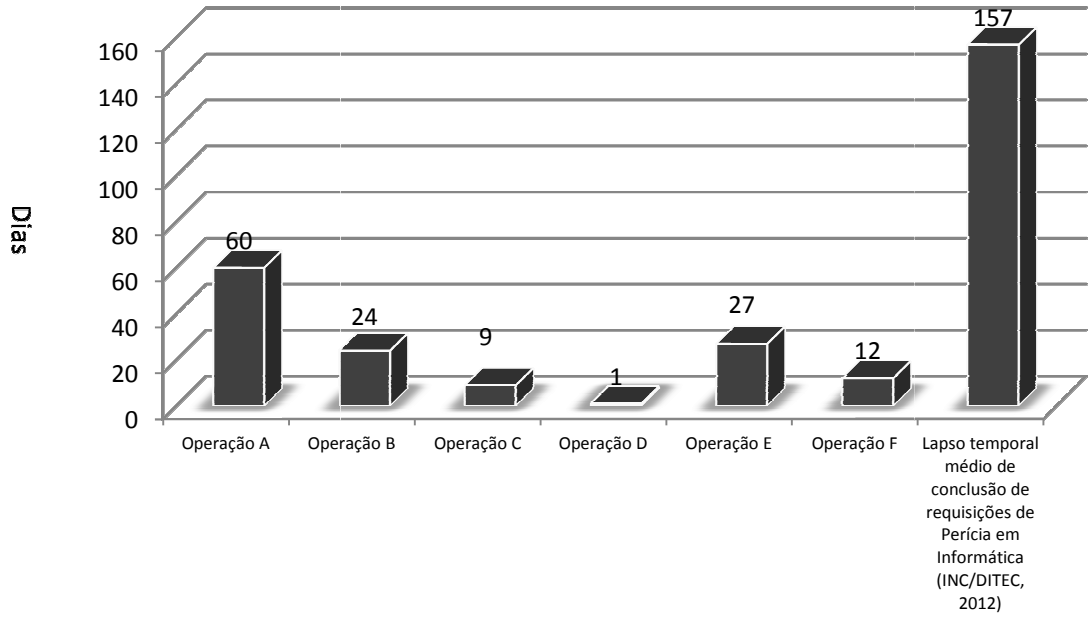

Figura 5.12 - Lapso temporal transcorrido

Mesmo a operação A, que arrecadou o maior número de materiais e contabilizou o maior volume de dados (257 mídias e 37 terabytes), durou 60 dias, tendo sido concluída

em 38% do tempo médio necessário ao completo atendimento de requisição de perícias em informática.

A figura 5.13 apresenta um comparativo entre o tempo médio consumido pela solução para completar as disponibilizações de documentos ao apuratório[31] e o tempo médio necessário ao completo atendimento de requisição de perícias em informática, no ano de 2011.

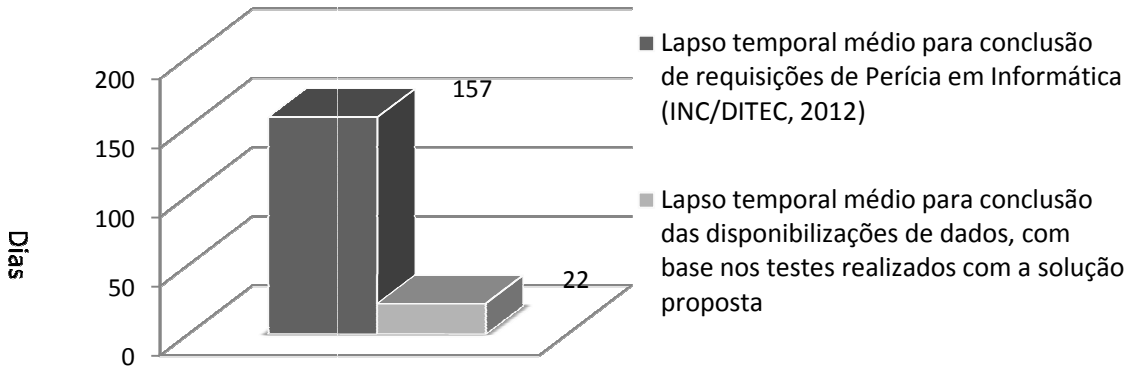

Figura 5.13 – Proporção de eficiência

5.2.1.4. Consumo de Espaço de Disco

A arquitetura proposta utiliza a estratégia de extrair, do material arrecadado, documentos comumente produzidos por usuário e disponibilizá-los em repositórios. A tabela 5.5 apresenta o espaço em disco efetivamente consumido pelo ferramental para reunir os documentos de cada operação policial. A tabela 5.5 apresenta dados de operações conduzidas na Bahia e no Pará.

Tabela 5.5 – Consumo de espaço em disco

Operação	Discos rígidos (qtde)	Dimensão[32] (terabytes)	Espaço efetivamente consumido no ferramental[33] (terabytes)	Proporção
A	258	35	0,1133	0,32%
B	50	10	0,0234	0,23%
C	32	5	0,0313	0,63%
D	3	0,3	0,0008	0,28%
E	41	8	0,0645	0,81%
F	57	4	0,0156	0,39%

[31] Considerando o tempo consumido em cada uma das seis operações onde a solução foi utilizada.
[32] Somatório das capacidades dos discos rígidos arrecadados.
[33]Espaço consumido no repositório de artefatos para armazenar os documentos eletrônicos extraídos dos materiais arrecadados em cada operação policial.

A figura 5.14 demonstra graficamente o comparativo apresentado na tabela 5.5.

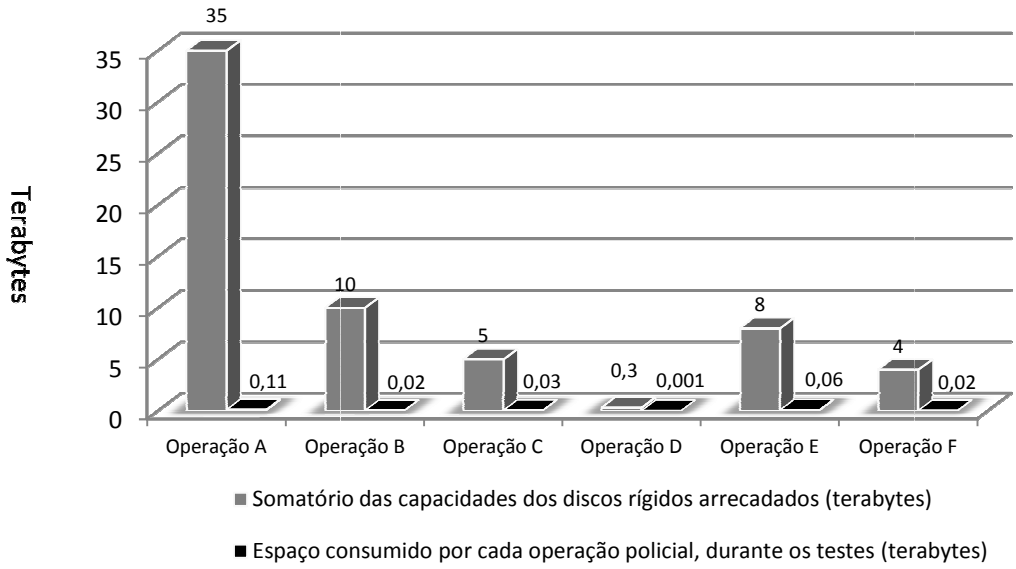

Figura 5.14 - Consumo de espaço em disco

O reduzido consumo de espaço em disco alcançado pela solução favorece que se possa gerenciar um grande número de operações policiais de grande porte simultaneamente. Esta característica também favorece que a análise da informação possa permear a investigação policial criminal, respeitando-se o tempo de cognição na atividade policial, sem impor ao ciclo de produção do conhecimento limites que não sejam inerentes à própria investigação. A análise da informação permeando a investigação é um dos requisitos apresentados no Capitulo 2 de revisão conceitual, especificamente, na Seção 2.4.1, que aborda a análise da informação na investigação policial criminal.

Fazendo uma extrapolação dos resultados obtidos nos teste realizados na Bahia, se existissem 20 operações policiais rigorosamente iguais à operação A, sendo conduzidas simultaneamente na instituição, por intermédio da solução proposta, seriam necessários, aproximadamente, 2,4 terabytes de espaço em disco para acomodar os documentos extraídos de todas elas. Por outro lado, se esse mesmo cenário fosse suportado por uma solução baseada em acesso direto as cópias forenses do material arrecadado, como o FTK ADLab, por exemplo, seria necessário uma configuração computacional com, aproximadamente, 700 terabytes de espaço em disco.

Embora, na visão deste pesquisador, a ferramenta concebida na pesquisa e a ferramenta FTK ADLab sejam ferramentas forenses de classe distintas[34], a figura 5.15 apresenta um comparativo de consumo de espaço entre elas.

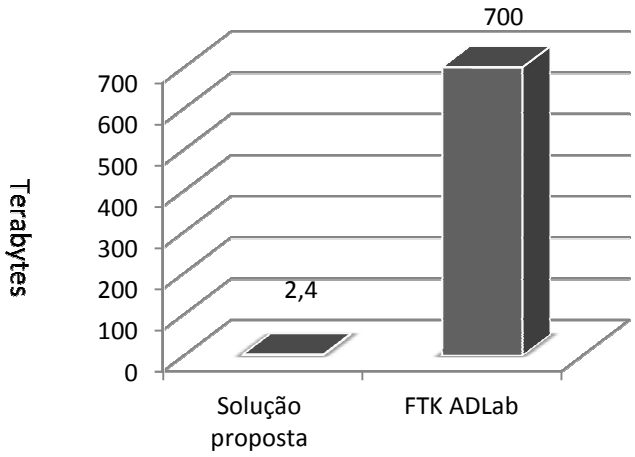

Figura 5.15 - Estimativas de consumo de espaço

O reduzido consumo de espaço em disco, confirmado pelos testes realizados, é especialmente relevante, à medida que demonstra ser possível reunir uma base histórica das operações, de forma a permitir por em prática os componentes mais avançados de mineração de dados do instrumental: o componente reconhecedor e o componente vinculador, descritos na Seção 4.1.3.2.

Revisitando os conceitos apresentados no capítulo 3, Seção 3.2.1, Nicole Beebe assevera que uma ferramenta com potencial de minerar dados seria capaz de permitir aos investigadores alcançarem níveis de informação sem precedentes (Beebe N. L., 2009).

5.2.1.5. Aspectos Relacionados à Eficiência Alcançada

A estratégia modular permite que cada componente especialista cuide de uma fração do problema denominado disponibilização de documentos eletrônicos. Cada módulo ou componente opera simultaneamente em relação aos demais, desde que tenha tarefa por

[34] Em síntese, a primeira é o protótipo de uma ferramenta especialista, tanto na disponibilização ágil de documentos eletrônicos, quanto no suporte ao processo de análise investigatória da informação, que inaugura uma nova classe de ferramentas forense voltadas a ajudar em investigações. Enquanto que, a segunda, é uma ferramenta forense orientada à tradicional identificação de evidências digitais, estendida por uma funcionalidade gráfica que permite acesso colaborativo aos arquivos existentes em uma ou mais mídias, em que pese a importância da referida ferramenta nos processos empregados em outros países.

cumprir. Para que dê início a uma nova tarefa, não requer intervenção humana, o faz de forma automática e assíncrona uns em relação aos outros. Ou seja, enquanto uma mídia esta sendo submetida ao processo de cópia forense, por exemplo, outra sofre extração, outra está em fase de montagem de dados, assim por diante.

A arquitetura da solução também a confere habilidade para lidar com grandes quantidades de mídias. A capacidade de automação da solução permite que, em um mesmo momento, lotes de mídias sejam oferecidos a processamento aos componentes aquisitores. Quanto maior o número de mídias processando simultaneamente, maior será a eficiência final, desde que, também, os demais componentes sejam dimensionados para atender ao volume de trabalho produzido.

Em outras palavras, os componentes da solução trabalham de forma modular, simultânea, autônoma e assíncrona uns em relação aos outros. O que representa um dos pontos fortes da proposta. Em virtude de sua arquitetura, o protótipo alcançou a capacidade produtiva apresentada na Seção 5.2.1.3. A figura 5.16 exemplifica didaticamente os componentes em funcionamento.

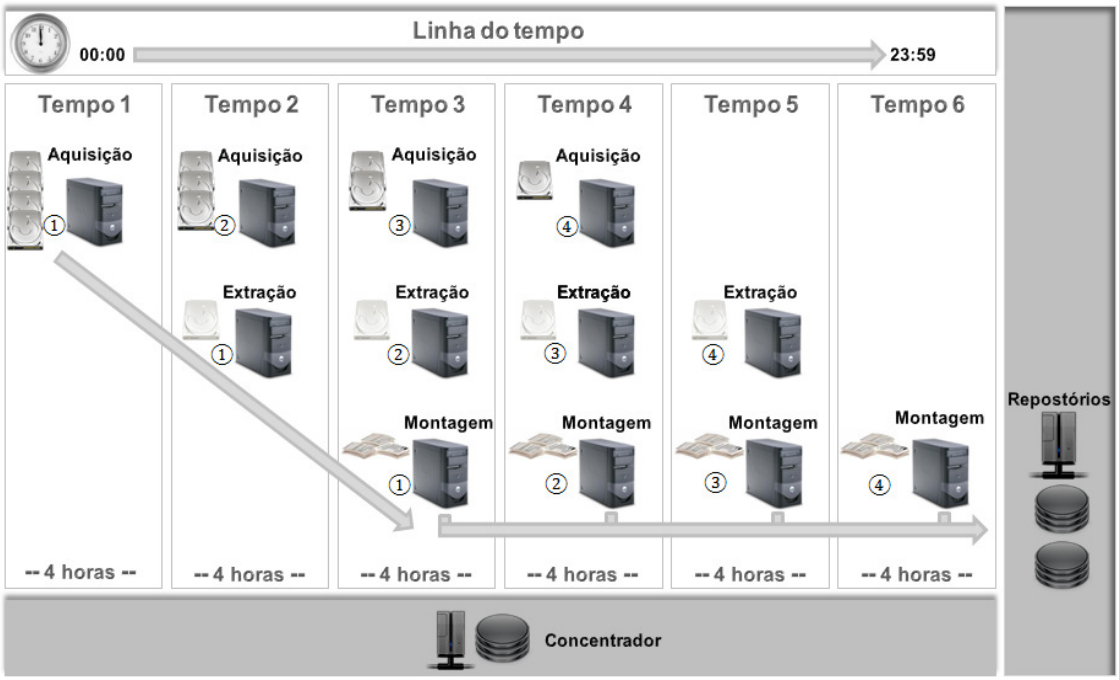

Figura 5.16 – Exemplificação de componentes em execução simultânea.

5.2.1.6. Expansibilidade e Versatilidade da Solução

A expansibilidade é outro ponto forte da solução proposta. O ferramental, concebido com base na arquitetura, está preparado para expandir sua capacidade produtiva - com a

adição de novas instâncias de componentes, operacionalizadas ou não em novos *hardwares* - para suportar um aumento de carga quando um maior poder de processamento for necessário. Por exemplo, a operacionalização exemplificada pela figura 5.17 seria capaz de expandir a eficiência alcançada por aquela apresentada na figura 5.8, que representou o esquema da configuração posta em prática para prova de conceitos. O modelo expandido é capaz de suportar o oferecimento simultâneo de até 40 discos rígidos. Tal modelo de operação é também versátil a ponto de permitir a desativação, temporária ou definitiva, de componentes e/ou de *hardware*, mantendo-se operacional[35].

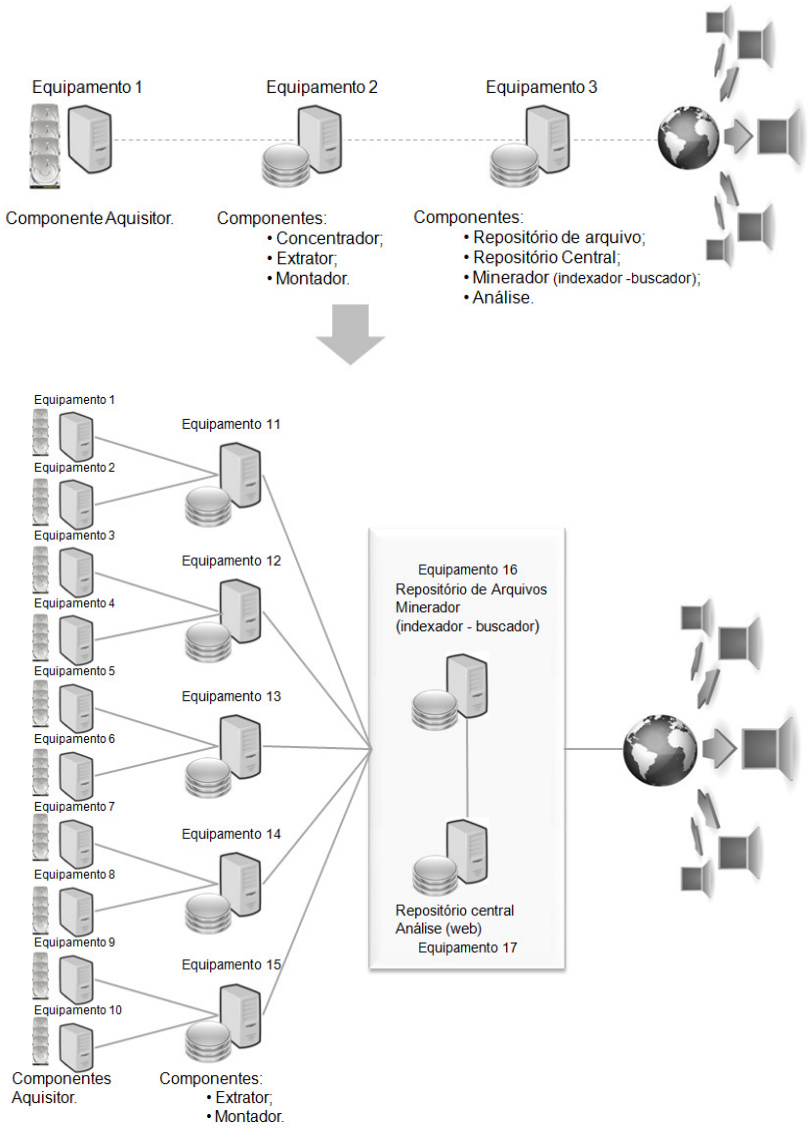

Figura 5.17 – Exemplo de configuração que demonstra a expansibilidade e versatilidade da configuração do ferramental.

[35] Desde que, pelo menos, uma instância de cada componente permaneça ativa, em um mesmo conjunto produtivo.

5.2.2. Análise investigatória da informação

Para analisar os documentos eletrônicos fez-se uso da fase de análise e cotejo, do segmento de investigação da metodologia proposta, descrito na Seção 4.1.4.1. A etapa, prevista como atribuição de investigadores, serviu para instrução da investigação policial criminal.

Por intermédio do uso do componente de análise, os investigadores puderam definir a estratégia de exploração do possível material probatório, organizando a atuação da equipe de investigadores. Por exemplo, a estratégia de organização dos trabalhos de análise pode levar em consideração os alvos investigados por cada policial ou mesmo suas especializações. Tal organização pode maximizar as chances de alcançar dados relevantes ao apuratório.

Uma vez organizados os trabalhos de análise, os investigadores exploraram os documentos eletrônicos submetendo buscas por palavras-chave, por exemplo, com base nas hipóteses investigatórias. As buscas tiveram como escopo simultaneamente todos os documentos disponibilizados na fase de extração de dados da metodologia proposta. A abordagem permitiu trabalhar eficientemente com grandes volumes de dados, funcionando a semelhança das ferramentas de buscas comumente utilizadas na internet. Com a diferença de que os *hits* permanecem disponíveis por tempo indeterminado, organizados em contêineres de buscas, a fim de que sejam avaliados profundamente e de forma colaborativa pela equipe de investigação.

A análise colaborativa e geograficamente distribuída permitiu que investigadores em salas, unidades policiais ou estados diferentes, por exemplo - compusessem uma mesma equipe de investigação, maximizando a força de análise.

Depois de avaliados, os documentos considerados relevantes pelos investigadores puderam ser adicionados a contêineres lógicos, que representaram as hipóteses da investigação. Os contêineres lógicos são compartilhados entre os investigadores de uma mesma equipe de análise. Todos puderam contribuir com a adição de outros documentos, posteriormente identificados durante o ciclo do processo de análise da informação. A eles também foi possibilitado registrar anotações que sustentassem teses, conjecturas, conclusões e outros dados que julgassem relevantes, retroalimentando a investigação.

Em síntese, os contêineres de hipótese serviram para reunir e compartilhar o conhecimento entre os membros de uma equipe de investigação, fomentando a cognição na atividade policial. Deles resultaram os relatórios de análise.

Em razão do curso das investigações, perícias em diferentes áreas do conhecimento foram requisitadas. Por exemplo, para verificar rastros que indicassem elaboração ou edição de determinados documentos em certos computadores[36], apontando indícios de autoria ou coautoria.

Por suas palavras, durante os testes, o delegado de policia federal Welder Almeida assim se referiu a experiência com a solução proposta (Almeida, 2010):

> Uma singela explanação acerca do sistema informatizado UIRAÇU se faz necessária, razão pela qual HÁ QUE SE COLACIONAR ao Feito o documento de apresentação desse novel instrumento de trabalho, 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 – é o *quod plerumque accidit*);

Acerca do nível de profundidade da exploração do possível material probatório, o delegado enfatizou (Almeida, 2010):

> Disponibilizado tal universo de arquivos pessoais por meio de aplicativo na intranet do DPF, obteve-se um mecanismo de busca automatizado (qual verdadeiro Google otimizado), cujas pesquisas, por parte dos investigadores que conhecem a fundo o caso concreto (e não dos peritos criminais, que conhecem a fundo as técnicas inerentes às suas especialidades); esses investigadores passaram, então, a realizar consultas, valendo-se de palavras-chave com relevância (no mais das vezes grande, alguma vezes pequena), tantas vezes quanto uma razoável duração do processo (algo constitucionalmente previsto) poderia permitir, e com isso se pode afirmar que as mídias computacionais foram vasculhadas a fundo, por meio de diversos critérios de pesquisa, e isso, certamente, é algo que dá muita segurança ao d. Magistrado Federal para decidir acerca do conjunto probatório amealhado com a apreensão de mídias computacionais;

[36] Verificando a existência de diferentes versões de um mesmo documento, em recurso de recuperação provido pelo ambiente computacional utilizado, por exemplo.

5.3. CONSIDERAÇÕES

Embora os resultados alcançados tenham sido promissores, há potencial para alcançar resultados muito melhores se for utilizada, de forma plena, a capacidade da solução proposta. Justifica enfatizar que os resultados positivos ora apresentados foram obtidos através de uma prova de conceitos. Há espaço para melhorias, algumas delas elencadas na Seção 6.3, que podem proporcionar resultados ainda mais positivos.

É valido acrescentar, extrapolando os objetivos da pesquisa, que os recursos de análise disponibilizados aos investigadores, para utilização durante a fase inquisitorial da persecução penal, podem ser franqueados ao titular da ação penal. Posteriormente, durante a fase processual, podem ser ainda estendidos ao magistrado e, também, a parte ré - em razão do direito ao Contraditório e à Ampla Defesa prevista pela legislação pátria[37]. Pode-se alcançar tal funcionalidade uma vez que o componente de análise e os demais que trabalham na retaguarda da solução podem ser operacionalizados por intermédio de ambiente computacional virtual[38] e receber a exportação de todos os documentos que compõem um determinado caso. Uma vez criado, o ambiente computacional virtual pode ser utilizado facilmente. O resumido consumo de espaço em disco necessário à solução contribui positivamente para tornar possível tal versatilidade operacional. Por exemplo, a operação A, conduzida na Bahia, acomodar-se-ia em um ambiente virtual de 150 gigabytes de tamanho total.

Este Capítulo trouxe os resultados da aplicação da prova de conceitos da metodologia e da arquitetura propostas aplicadas a casos reais. O Capítulo 6 apresenta as conclusões desta pesquisa e propõe trabalhos futuros.

[37] O Princípio do Contraditório e da Ampla Defesa é assegurado pelo artigo 5º, inciso LV da Constituição Federal.
[38] Simulação de um computador implementado através de software, que executa programas tal qual um computador real.

6. CONCLUSÕES

Neste Capítulo são apresentadas as conclusões da pesquisa. A Seção 6.1 apresenta as principais contribuições, enquanto que na Seção 6.2 são apresentadas as considerações finais. Por fim, são relacionados trabalhos futuros, que seguem na Seção 6.3.

6.1. PRINCIPAIS CONTRIBUIÇÕES

A principal contribuição do presente trabalho é que, diferentemente dos trabalhos apresentados anteriormente ou das soluções comerciais focadas sempre na ferramenta disponibilizada aos investigadores e peritos, o foco desta dissertação é uma metodologia e uma arquitetura que oferece os seguintes principais benefícios:

1) Tornar mais ágil a disponibilização de documentos eletrônicos ao apuratório;
2) Viabilizar e otimizar o trabalho de investigação a partir de dados em formato digital;
3) Resguardar a objetividade do perito, que não deve ser exposto ao contexto das hipóteses da investigação;
4) Viabilizar a análise de dados colaborativa e geograficamente distribuída, permeando a investigação policial criminal;
5) Favorecer a evolução do conhecimento em ciclo à medida que novas informações são analisadas pela equipe de investigação;
6) Tratar o grande volume de dados digitais sem exclusão de informação julgada irrelevante, visto que em outro momento das investigações essa informação pode vir a ser importante;
7) Viabilizar a construção de mecanismos automatizados de mineração de dados que auxiliem na identificação de dados relevantes a investigação policial criminal.

Com base neste trabalho, um artigo científico foi submetido à ICoFCS 2011 (*The Sixth International Conference on Forensic Computer Science*), tendo sido publicado nos

anais dessa conferência e apresentado no VIII Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber 2011).

6.2. CONSIDERAÇÕES FINAIS

Neste trabalho foram concebidas uma metodologia e uma arquitetura para sistematizar a análise investigatória da informação digital. Os resultados alcançados em investigações policiais reais confirmaram a hipótese de pesquisa, mostrando ser possível integrar os trabalhos de investigadores e peritos criminais em torno da investigação digital. A metodologia e a arquitetura proposta demonstraram eficiência e os resultados práticos alcançados mostram eficácia.

Cada qual estabelecida segundo suas próprias regras, exigências e particularidades, as provas resultantes do modo de trabalho proposto podem possuir:

- Um caráter de prova documental - quando transmitem ideias e pensamentos, por exemplo, apostos em um suporte digital;

- Um caráter de prova pericial – quando, por exemplo, apresentem os efeitos de condutas, por intermédio da técnica, da ciência ou da arte.

Em virtude da adoção desta proposta, a análise da informação poderá ser amplamente realizada no contexto da investigação, abolindo o método diferenciado de análise, podendo ser tão minuciosas e extensas quanto for exigido, em razão das características do fato e da conduta em apuração.

6.3. TRABALHOS FUTUROS

Há diversas possibilidades para trabalhos futuros. Eis algumas:

1) Permitir que o componente de análise 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.

2) 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;

3) Evoluir o componente de aquisição especializado em disco rígido e conceber aquisitores para outros tipos de mídia.

REFERÊNCIAS BIBLIOGRÁFICAS

Access Data. (2011). Fonte: *Access Data Corp*. FTK 3.x: Disponível em: <http://accessdata.com/downloads/media/Configuring *Distributed Processing with* FTK 03.pdf >. Acessado em julho/2011.

Almeida, D. W. (2010). Documento Oficial que compõe Inquérito Policial em curso. Belém do Pará, PA.

ANP/DPF. (2009). Investigação policial criminal. Brasília: Academia Nacional de Polícia.

ANP/DPF. (2008). Manual de Gestão de Planejamento Operacional. Brasília-DF: Academia Nacional de Polícia.

Aranha, A. Q. (1987). Da Prova no Processo Penal. Saraiva.

Ayers, D. (2009). A second generation computer forensic analysis system. digital investigation .

Barbosa, A. M. (24 de 02 de 2011). Ciclo do Esforço Investigativo criminal - CEIC. Acesso em outubro/2011, disponível em www.jurisway.org.br: http://www.jurisway.org.br/v2/dhall.asp?id_dh=5481

Beebe, N. L. (2009). Digital Forensics Research: The Good, the Bad, and the Unaddressed. San Antonio, Texas, Estados Unidos da América.

Beebe, N. L., & Clark, J. G. (2004). A Hierarchical, Objective-based Framework for the Digital Investigations Process.

Carrier, B. (2005). File System Forensic Analysis, Addison Wesley, ISBN: 0-321-26817-2.

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence .

Ciardhuain, S. O. (2004). An Extended Model of Cybercrime Investigations. . International Journal of Digital .

Costa, M. A. (1997). Crimes de Informática. Jus Navigandi , Disponível em: <http://jus.uol.com.br/revista/texto/1826>. Acesso em: junho/2011.

Couri, G. F. (2009). Crimes pela Internet. Escola da Magistratura do Estado do Rio de Janeiro - Revista da EMERJ , p. Disponível em : <http://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2009/direto_penal/direito_penal.html> Acessado em: junho/2010.

DITEC/DPF. (9 de Dezembro de 2011). Instrução de Serviço 008/2011-DITEC, de 23 de novembro de 2011. Boletim de serviço 235.

EnCase Forensic. (2011). Fonte: Disponível em: < http://www.guidancesoftware.com>. Acessado em julho/2011.

Espíndula, A. (2009). Sistema Judiciário, Sistema de Segurança Pública/Policial e Sistema Pericial. Acessado em julho/2011, disponível em http://www.espindula.com.br: http://www.espindula.com.br/conteudo.php?id=7

Ferro Júnior, C. M. (2008). Inteligência Organizacional: Identificação das bases doutrinárias para a investigação criminal. Acessado em setembro/2011, disponível em http://www.conteudojuridico.com.br/?artigos&ver=2.21050

Foremost. (2011). Fonte: foremost: Disponivel em: <http://foremost.sourceforge.net/>, Acessado em dezembro/2011

Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years . Digital investigation 7 , S64 - S73 Disponivel em: < http:// www.dfrws.org/2010/proceedings/2010-308.pdf> Acessado em seembro/2011.

Gomes, L. F., & Scliar, F. (2008). Investigação preliminar, polícia judiciária e autonomia. LFG, São Paulo , p. Disponível em: < http://www.lfg.com.br/public_html/article.php?story=20081020154145672>. Acesso em:7 dez. 2010.

Huebner, E., Bem, D., & Bem, O. (2008). Computer forensics - past, present and future. Journal of Information Science and Technology.

INC/DITEC. (2010). Relatório Estatístico das Atividade do Sistema Nacional de Crimilalística. Brasília. DF: Departamento de Polícia Federal - Diretoria Técnico Científica.

INC/DITEC. (2011). Relatório Estatístico das Atividade do Sistema Nacional de Crimilalística. Brasília. DF: Departamento de Polícia Federal - Diretoria Técnico Científica.

INC/DITEC. (2012). Relatório Estatístico das Atividade do Sistema Nacional de Crimilalística. Brasília. DF: Departamento de Polícia Federal - Diretoria Técnico Científica.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response , NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology.

Kohn, M., Eloff, J., & Oliver, M. (2006). Framework for a Digital Forenisc Investigation. Proceedings of Information Security South Africa (ISSA).

Manzano, L. F. (2011). Prova Pericial: Admissibilidade e Assunção da Prova Científica e Técnica no Processo Brasileiro. São Paulo: Atlas.

Mirabete, J. F. (2008). Processo Penal. 18ª ed. São Paulo: Atlas.

Mittermaier, C. (1997). Tratado da Prova em Matéria Criminal. 2ª ed. Tradução de Herbert Wützel Heinrich. Campinas: Bookseller.

Nucci, G. d. (2008). Manual de Processo Penal e Execução Penal 5ª ed. rev., atual. e ampl. 2 tir. São Paulo: Revista dos Tribunais.

Opilhar, M. C. (2006). Criminalística e Investigação : livro didático / Maria Carolina Milani. UNISULVIRTUAL - Universidade do Sul de Santa Catarina . Palhoça, Santa Catarina pp. 49-89.

Palmer, G. (2001). A Road map for Digital Forensic Research. Utica, New York: Disponível em <http://www.dfrws.org/2001/dfrws-rm-final.pdf>, Acessado em: outubro/2011.

Pinheiro, P. P. (2008). Direito Digital 2 ed. São Paulo: Saraiva.

Pollitt, M. (1995). Computer Forensics: an Approach to Evidence in Cyberspace. Proceeding of the National Information Systems Security Conference. 487-491. Baltimore, MD.

Rangel, P. (2003). Direito Processual Penal. Rio de Janeiro: LUMEN JURIS.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models International. Fonte: Disponível em: <http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf>, Acessado em outubro/2011.

Scalpel. (2011). Fonte: http://www.digitalforensicssolutions.com: Disponivel em: <http://www.digitalforensicssolutions.com/Scalpel/>, Acessado em: dezembro/2011

SEPINF/DITEC. (2011). – Serviço de Perícias em informática. Ferramentas de Análise Pericial. Disponível em: <https://sepinf.ditec.dpf.gov.br/wiki/Ferramentas> Acessado em julho/2011.

SleuthKit/Autopsy. (2011). Fonte: sleuthkit.org: Disponivel em: <www.sleuthkit.org>, Acessado em: dezembro/2011.

Távora, N., & Antonni, R. (2009). Curso de Direito Processual Penal. 3. ed. Salvador: Podivm.

Tourinho Filho, F. d. (2009). Processo penal. São Paulo: Saraiva: Saraiva.

Vianna, T. L. (2003). Fundamentos de Direito Penal Informático. Rio de Janeiro: Forense.

Zaffaroni, E. R., Batista, N., Alagia, A., & Slokar, A. (2010). Direito Penal Brasileiro: segundo volume – Teoria do Delito: introdução histórica e metodológica, ação e tipicidade. Rio de Janeiro: Revan.