ETAPAS DO PROCESSO DE COMPUTAÇÃO FORENSE: UMA REVISÃO

Adriano Gomes Sousa
Bacharel em Ciência da Computação pelo Centro Universitário da Bahia (FIB).
Especialista em Ciências Forenses IFAR/LS
E-mail: adrianosousa@gmail.com

Resumo
A palavra Forense está diretamente relacionada com o trabalho de investigação, o trabalho de descobrir informações que possam ser utilizadas em investigações criminais, civis, empresariais etc. Este artigo é um resumo, uma breve revisão sobre o processo de computação forense, explicando brevemente os principais aspectos, técnicas, e ferramentas utilizadas em cada etapa do processo computacional Forense. Por fim, são revisadas algumas políticas de segurança que podem melhorar os resultados da perícia forense em computadores e redes.
Descritores: Processo de Computação Forense; Etapas forenses; técnicas e ferramentas.

STAGES OF THE FORENSIC COMPUTATION PROCESS: A REVIEW

Abstract
Forensic word is directly related to the research work, work to discover information that can be used in criminal investigations, civil, business etc. This article is a summary, a brief review of the computer forensics process, briefly explaining the main aspects, techniques and tools used in each step of Forensic computational process. Finally, it reviewed the security policies that can improve the results of forensic expertise in computers and networks.
Keywords: Process forensics; forensic computing; technical measures and tools.

INTRODUÇÃO

A Computação forense é uma arte de descobrir e recuperar informações sobre um crime de tal forma a torná-lo admissíveis em tribunal (YASINCAC, MANZANO, 2001). Segundo DAN FARMER (2012), a Perícia Computacional Forense trata da captura e análise de evidências, tanto quanto possível e livres de estarem distorcidas ou tendenciosas, de tal forma, a reconstruir determinados dados ou o que aconteceu num sistema no passado. Através desses conceitos, é possível verificar a importância que a computação forense tem na busca da verdade dos fatos, sendo esse um motivo relevante para revisar suas etapas, seus aspectos, e aplicações.

METODOLOGIA

Nesta revisão, foram consultadas referências, todos os autores de livros com domínio pertinente ao assunto: computação forense e suas etapas. Por fim, foi revisto as políticas de segurança que ajudam no processo de perícia forense computacional.

REVISÃO DE LITERATURA

Segundo Eleutério e Machado (2011) Computação Forense é uma ciência que obtém, preserva e documenta evidências de dispositivos de armazenamento digital, como computadores, PDAs, câmeras digitais, telefones celulares e vários dispositivos de armazenamento de memória. Esses autores organizam a Computação Forense em 4 etapas principais: Coleta, Exame, Análise e Relatório.

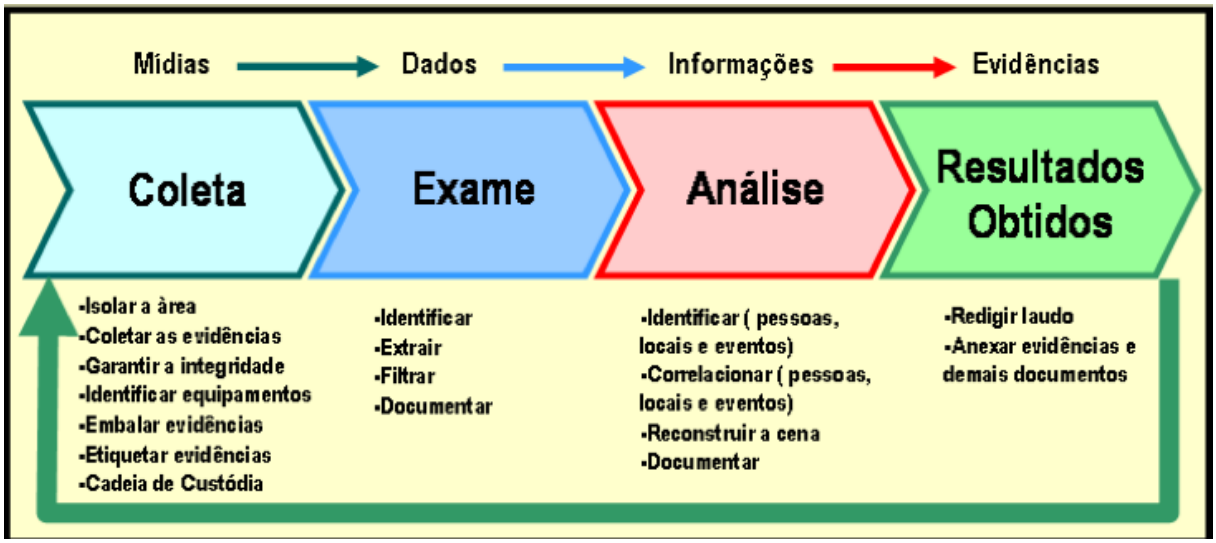

Figura 1. Etapas do processo de computação forense (Fonte: Adaptado de Kent et al, 2006)

a) **Coleta**: O objetivo da primeira etapa é identificar, isolar, etiquetar, registrar e coletar os dados e evidências físicas relacionadas com o incidente que está sendo investigado, enquanto estabelece e mantem a integridade das provas.

b) **Exame**: identificar e extrair as informações relevantes a partir dos dados coletados utilizando ferramentas e técnicas forenses adequadas.

c) **Análise**: Analisar os resultados do exame para gerar respostas úteis para as questões apresentadas nas fases anteriores.

d) **Relatório (Resultados)**: inclui encontrar relevância para o caso. Nessa etapa também é redigido o laudo pericial, o qual deve ter conclusão imparcial, clara e concisa; deve ter exposto os métodos utilizados na perícia, e deve ser de fácil interpretação por uma pessoa comum, de conhecimento médio.

Nos tópicos a seguir, serão apresentadas as principais ferramentas e técnicas utilizadas nas Etapas supracitadas.

- **Ferramentas e Técnicas utilizadas na Etapa de Coleta**

De acordo com Eleutério e Machado (2001), é fundamental que os dados contidos nos dispositivos (mídias digitais e dispositivos de armazenamento) e os dados voláteis (aqueles que constam na memória RAM ou trafegando em rede de

computadores), possíveis fontes de evidências digitais, permaneçam coletados e preservados corretamente, de maneira a garantir que não seja alterado.

Nessa fase de preservação e coleta que será possível buscar elementos (dados, mídias de armazenamento, entre outros) de maneira a consolidar uma base investigativa para as fases seguintes da perícia.

- ✓ **Sobre as Técnicas de Imagem e Espelhamento**

De maneira geral, os exames forenses devem ser efetuados em cima de duplicatas idênticas, as quais são obtidas dos materiais questionados originalmente apreendidos e submetidas a exames forenses. Dessa forma, deverão ser aplicadas ferramentas e técnicas que efetuem uma cópia fidedigna dos dados e mantenham a integridade do material apreendido (ELEUTÉRIO; MACHADO, 2011).

Imagem e Espelhamento são técnicas de duplicação/cópia utilizadas na fase de coleta. Essas técnicas, ao serem realizadas através de softwares e equipamentos forenses, garantem uma cópia fiel dos dados e consequentemente a preservação correta do material que foi apreendido (ELEUTÉRIO; MACHADO, 2011).

- ✓ **Ferramentas usadas para bloqueio de escrita e na duplicação forense**

Existem muitas ferramentas em hardware que ajudam na preservação dos dados no momento da realização da Imagem ou do Espelhamento. Entre eles, os destaques são os duplicadores forenses e os bloqueadores de escrita.

Segundo Eleutério e Machado (2001), Os equipamentos Espion Forensics e o Forensic Bridge Tableau são os mais utilizados para bloqueio de escrita em discos, já o software ICS Write Protect Card Reader é o mais utilizado para bloqueio de escrita em cartões de memória.

As principais vantagens na utilização de duplicadores forenses são: maior rapidez na duplicação dos dados; suporta muitas interfaces de discos; não precisar de computador para efetuar a interface entre os discos questionados. (ELEUTÉRIO; MACHADO, 2011).

- ✓ **Sistemas operacionais e programas utilizados para duplicação forense**

O uso de dispositivos de bloqueio de escrita ou duplicadores forenses não é obrigatório na etapa de coleta de dados. No entanto, a utilização desses dispositivos facilita o processo de duplicação de discos, como exemplo, segundo Eleutério e Machado (2011), a possibilidade do utilização de alguns programas específicos ou de sistemas operacionais que não entrem/acessem o equipamento de armazenamento questionado, garantindo a integridade.

O programa Norton Ghost da empresa Symantec é uma opção ao uso de duplicadores forenses e bloqueadores.

O software Forensic ToolKit (FTK) e o software Encase são soluções proprietárias compatíveis com o Windows. Ambas possuem diversas funcionalidades que possibilitam a realização de diversas técnicas para perícia forense computacional. Já como opções para Linux, o autor destaca a utilidade de alguns softwares para a etapa de preservação e coleta: DC3DD e Guymager, e destaca também os sistemas Linux CAINE e FDTK-Ubuntu para mesma finalidade. (ELEUTÉRIO; MACHADO, 2011).

- ✓ **Principais ferramentas/dispositivos utilizados para coleta de dados voláteis**

Segundo LILLARD et al (2010), a fase de coleta de evidências digitais para realizar uma perícia forense computacional é dividida em dois grupos, separados de acordo com a volatilidade dos dados: Grupo post-mortem, a coleta é realizada sobre fontes não voláteis, (que independam de energia para armazenar os dados) e grupo em vida (coleta live), nesse as informações digitais são coletadas em fontes voláteis(armazenagem temporária).

Segundo Eleutério e Machado (2001), os principais dispositivos fontes da coleta post-mortem são: CDs, DVDs, cartões de memória, Mídias de armazenamento, discos rígidos(HD).

Embora as atividades do tipo post-mortem sejam consideradas imensa maioria nos exames periciais, todavia, em alguns casos, é fundamental a coleta Live, por

exemplo, em situação que a evidência está em uma memória RAM do computador ou trafegando em uma rede de computadores.

A coleta do tipo live, quando realizada em redes de computadores, geralmente ocorre a captura de dados que trafegam pela entrada ou pela saída de tráfego de um computador ou de um ponto da rede.

Nesse sentido, segundo GALVÃO (2013), essa é a principal função dos softwares de Network Forensic Analysis Tools (NFAT), ou seja, a captura e análise de tráfego de rede, neste caso, voltado para parte forense**.**

Nessa categoria de software, segundo Galvão (2013), o programa TCPDUMP é o sniffer de rede mais conhecido e utilizado hoje em dia. Esse programa possui uma interface amigável e uma biblioteca libbcap, a qual possui infraestrutura flexível para captura de pacotes em redes de computadores.

Outro exemplo dessa categoria de software, o Wireshark é um famoso analisador de protocolo de rede e ainda possui a funcionalidade de captura de pacotes de redes. Ele coloca a placa de rede em modo promíscuo, possibilitando a um maior alcance da captura de pacotes, além das funcionalidades de exportar pacotes para uma posterior análise. O software Wireshark é Open Source e disponível para diversas plataformas.

- **Ferramentas e técnicas utilizadas na etapa de extração**

Depois de finalizada a etapa de coleta, a próxima etapa é extrair dados / informações relevantes para uma posterior análise. Nessa etapa, é extraído e avaliado o quê pode ser importante para a investigação. Nesse ponto, podem ser encontradas evidências inacessíveis, devido à proteção por senha, criptografia, ou prévia exclusão do dado. A seguir, será revisto importantes ferramentas e técnicas utilizadas na etapa de extração**.**

- ✓ **Recuperação de arquivos (Data Carving)**

De acordo com Eleutério e Machado (2001), Data Carving, que na computação refere-se à recuperação de arquivos apagados, é uma técnica realizada através da localização de assinaturas conhecidas (por exemplo, cabeçalhos que contêm a identificação do tipo de arquivo). Alguns softwares como Photorec e Ontrack Recovery podem realizar a recuperação de arquivos apagados de forma automática.

O programa Photorec é compatível com várias assinaturas, suporta vários sistemas de arquivos, além de ser software livre. Já o software Ontrack Recovery possui interface intuitiva e realiza a recuperação de diversos tipos de arquivos, seja com base na técnica de assinaturas, seja com base na estrutura do arquivo (ELEUTÉRIO; MACHADO, 2011).

Outro problema comum durante a fase de extração é o surgimento de programas e arquivos que precisam de senhas para serem extraídos. Dessa forma, segundo Eleutério e Machado (2001), as principais técnicas para solucionar esse problema são: Engenharia reversa, a engenharia social, ataques de força bruta.

De acordo com Pinheiro (2013), a engenharia reversa de um software é um processo de desmontagem e análise cujo principal objetivo é construir e analisar um modelo representativo em alto nível, para que assim o programa alvo possa ser estruturado e entendido.

Quando consegue entender a estrutura e o funcionamento de um programa, é possível localizar a parte que faz o processo de Login (autenticação), podendo alterar o software estaticamente ou dinamicamente, conseguindo assim ter acesso a parte protegida do software, e consequentemente a informação deseja pela perícia.

Engenharia social é um método de ataque, no qual alguém faz uso da persuasão, diversas vezes abusando da ingenuidade ou confiança do usuário, com a finalidade de obter informações que possam ser utilizadas no acesso não autorizado a computadores ou informações. (SOCIAL-ENGINEER, 2015).

Segundo Eleutério e Machado (2011), em um ambiente no qual os arquivos são protegidos por senha e os seus usuários são acessíveis da equipe de investigação, a

técnica de engenharia social pode ajudar neste processo de acesso as senhas, facilitando o trabalho pericial.

Já o Ataque de força bruta consiste em utilizar um dicionário de senhas, testando cada senha de forma automática, a fim de localizar uma possível senha dentro do dicionário utilizado. Um dos softwares mais utilizado para força bruta é ElcomSoft Password Recovery. (ELEUTÉRIO; MACHADO, 2011)

- ✓ **Utilização da técnica de Indexação de dados**

A indexação é uma técnica de organização/arrumação de dados. Essa técnica envolve a criação de estruturas de dados associados aos documentos de uma determinada coleção, de forma que possa ser acessado posteriormente com índices, gerando mais velocidade no acesso dessas informações.

Muitos softwares de computação forense trabalham com indexação de dados, dentre estes, destaca-se o FTK e o Encase. (BATTULA, 2000).

- **Ferramentas e técnicas utilizadas na etapa de análise**

De acordo com Almeida (2011), esta etapa consiste em examinar os dados/informações extraídos da etapa de extração, e em seguida identificar evidências digitais, verificando a relação com o fato apurado.

Após a identificação e avaliação das evidências encontradas no material questionado, é possível responder as perguntas feitas pela autoridade solicitante.

Dessa forma, é importante que o a autoridade solicitante busque sempre detalhar o quê procura, descrevendo no máximo de detalhes possível, ou seja, que mostre para a equipe pericial exatamente o quê deve ser buscado, para dessa forma, evitar desperdício de trabalho dos peritos. (ALMEIDA, 2011).

- ✓ **Análise de dados originados de dispositivos de armazenamento de dados**

Um disco rígido, nos padrões atuais de tamanho, por menor que seja esse tamanho, em geral, contem milhões de arquivos, todavia, analisar o conteúdo de todos esses arquivos pode consumir muito tempo, tornando o exame pericial inviável. (ELEUTÉRIO; MACHADO, 2011).

Nesse sentido, diversas ferramentas, técnicas e procedimentos podem ser usados para tornar a fase de na análise mais eficiente e viável.

Um bom exemplo de técnica de análise é o Known File Filter (KFF), que é um utilitário de banco de dados que compara valores hash conhecidos contra uma base de arquivos a ser analisada. Usando a KFF durante a etapa análise, pode-se: identificar imediatamente e ignorar 40 a 70 por cento dos arquivos; identificar imediatamente os tipos de arquivo pelo seu conteúdo (usando um hash que é baseado em dados e não nomes ou extensões de arquivos); localizar um arquivo específico de interesse à perícia, como em casos de imagens de pornografia infantil (ELEUTÉRIO; MACHADO, 2011).

Outra técnica muito eficiente e muito utilizada na etapa de análise é a busca por palavras-chave, sendo essa técnica disponível em muitos softwares de análise de arquivos. (ELEUTÉRIO; MACHADO, 2011).

Segundo Eleutério e Machado (2011), as ferramentas que são destaques na etapa de análise são os software Encase e o software Forensic Toolkit (FTK), pois eles além de serem uteis em todas as etapas do processo forense computacional, eles ainda têm diversas funcionalidades que são fundamentais para a etapa de analise, como: as buscas por palavra-chave, a navegação adequada pelos arquivos e pastas da base de dados, o KFF, entre outras.

Como exemplo de técnica de analise, Eleutério e Machado (2011) cita a virtualização como técnica viável para simular e entender as ações realizadas pelos usuários de um sistema emulado. Dentre os software de virtualização, os destaques são o WMware e o Virtual Box.

O WMware é um software proprietário que permite o processo de virtualização sem modificar os dados contidos nas duplicatas originadas da etapa de coleta, pois o VWware cria uma camada intermediária entre a duplicata analisada e a máquina virtual (ELEUTÉRIO; MACHADO, 2011).

Virtual Box é um software completo de virtualização, disponível em versões para empresas e para usuário individual. Ele é gratuito e com código fonte livre.

- ✓ **Breve perspectiva da Etapa de Análise em tráfego de rede**

De acordo com Junior e Moreira (2014), a análise forense de redes permite a união de informações sobre o tráfego e ajuda a responderaos quesitos feitos pela investigação. Ou seja, o principal é verificar eventuais dados / informações que possuam alguma relação com o incidente apurado, de maneira a elucidar o fato apurado.

O trafego de uma rede pode ser analisado em tempo real ou a partir de uma captura realizada anteriormente. Independente da forma de captura do pacote, para perícia, geralmente é importante saber a origem e destino do pacote, as portas, e principalmente o conteúdo completo dos pacotes suspeitos (GALVÃO 2013).

Segundo Galvão (2013), é fundamental saber o quê está sendo procurado, pois assim poderá ser aplicado corretamente os filtros na captura, conseguindo assim ter um resultado mais eficiente sobre a analise, tendo em vista a quantidade de informação/dados que geralmente trafegam em uma rede.

- ✓ **Breve perspectiva da Análise Forense em ambiente computacional virtualizado**

A análise forense do computador pode ser aplicada em ambiente virtual ou máquina virtual. Máquina virtual é um software que permite que o usuário crie um ou mais ambientes separados, cada um simulando seu próprio conjunto de hardware e software próprio. O objetivo principal da computação forense é realizado em quatro fases, que são: acessar, adquirir, analisar e relatar (ELEUTÉRIO 2011). Máquina virtual

simula alguns componentes básicos, uma vez que não foi criado para fornecer suporte completo para uma ampla gama de dispositivos de hardware. Quando aplicado computação forense em máquina virtual, algumas regras básicas devem ser seguidas, quais sejam: manipulação mínima da informação original; registrar qualquer alteração, agir em conformidade com as regras de prova; e não ultrapassar o seu nível de conhecimento.

- ✓ **Breve perspectiva da Análise Forense utilizando logs**

Forense digital é campo de investigação de crimes informáticos. O processo básico realizado é a coleta de provas, exame que evidencia, analise dessas provas e finalmente a confecção de relatórios. Um item importante a ser consideração são os arquivos que possuem as informações correspondentes ao usuário que fez a ação (Logs do sistema). Os arquivos de log estão em formato de texto para que eles possam ser lidos usando o bloco de notas ou qualquer editor de texto. Os arquivos de log consistem em informações como data, URL, nome da máquina, tempo, bytes de status e de referência. Estas informações agem como grande sucesso para Forense Digital. Arquivos de log são novamente divididos em diferentes tipos de análise. Os tipos são: dispositivo de registros de rede que é usado para executar a comunicação na rede; logs de firewall, usados para monitorar o tráfego de entrada e saída da rede; logs de Web Server, usados para manter os logs de acesso e relatórios de número de visitantes, vistas, páginas visitadas mais frequentes. De forma geral, os software ou sistemas operacionais mantêm arquivos de logs de todas as ações efetuadas pelos usuários.

- **Políticas de segurança para melhorar os resultados da perícia forense em computadores e redes.**

Políticas são introduzidas de forma que, com base em evidências encontradas durante a investigação forense, possa ser mais fácil identificar o tipo de crime cometido e sua autoria. Neste processo, as seis políticas abaixo são fundamentais (YASINCAC, MANZANO, 2001).

a) **Retenção de informação:** consiste de copiar e reter aplicação e arquivos de usuários locais e copiar e reter computador e atividade de rede logs, utilizando técnicas apropriadas que garantam a integridade, autenticidade.

b) **Planejando a resposta**: consiste no estabelecimento de uma equipe forense, estabelecendo um procedimento de resposta de intrusão e formalização do processo de investigação.

c) **Formação técnica**: isso inclui treinamento de equipe de resposta. Formação da equipe de investigação e de formação para todo o pessoal que utilizam computadores.

d) **Acelerar a investigação**: inclui nessa política a proibição da criptografia de arquivos pessoais, proibir software de trituração de arquivo. Recomenda-se indexação de dados.

e) **Prevenção de todas as atividades anônimas**: Exigir data, hora e usuário estampados nos arquivos, usando a autenticação rígida de usuário e mecanismos de controle de acesso rígidos, garantindo que toda atividade seja identificada.

f) **Proteger as provas**: exercer um controle rígido sobre o acesso administrativo das evidências. Criptografar arquivos de evidências e conexões, aplicando tecnologia de verificação de integridade forte.

Utilizando estas seis políticas, além de haver diminuição de crimes digitais, facilitará o processo investigativo da perícia computacional (YASINCAC, MANZANO, 2001).

CONSIDERAÇÕES FINAIS

Computação forense é a fonte para encontrar a evidência da cena do crime através das evidências digitais. Segundo a pesquisa de diversos autores, a computação forense é a busca da verdade nos vestígios computacionais. A equipe forense também

tem muitas ferramentas diferentes disponíveis para trabalhar em vários tipos de crimes. A equipe forense computacional trabalha em processo básico que inclui a identificação, coleta, preservação, análise e relatório. Este processo funciona de forma muito eficiente para investigação. E por fim, os autores consideram o melhor desempenho das técnicas de computação forense quando é apresentado por técnicas de análise forense ao vivo.

REFERÊNCIAS

ABDULLAH, M. **Advances in Computer Forensics**. IJCSNS. V. 8, N. 2, Fevereiro, 2008.

BATTULA, B. et al. **Techniques in Computer Forensics**: IJS. V. 3, 2000.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense**. São Paulo: Novatec, 2011.

FARMER, Dan; VENEMA, Wietse. **Pericia forense computacional, teoria e pratica aplicada**; Tradução Edson Furmankiewicz, Carlos Schafranski, Docware Traduções Técnicas; Revisão Técnica Pedro Luís Próspero Sanchez. São Paulo: Person Prentice Hall, 2007.

GALVÃO, R. K. M. **Introdução à análise forense em redes de computadores**: São Paulo: Novatec, 2013.

JUNIOR, C. C. N. M.; MOREIRA, J. **Roteiro investigativo em perícia forense computacional de redes**: São Carlos, 2014.

KENT, K. et al. **Guide to integrating forensic techniques into incident response**: Special publication. Gaithersburg: NIST, 2006.

LILLARD, T. et al. **Digital forensics for network, internet and cloud computing**: Burlington: Syngress, 2010.

PINHEIRO, D. O. **Um estudo experimental das ferramentas de engenharia reversa aplicadas às vulnerabilidades do software**. 42 f. Monografia, UFCE, Quixadá, 2013

YASINCAC, A.; MANZANO, Y. **Policies to enhance computer and Network Forensics**. IEEE. 2001.