ETAPAS DO PROCESSO DE COMPUTAÇÃO FORENSE

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

Palavras-chave: Processo de Computação Forense, Etapas forenses, técnicas e aspectos.

INTRODUÇÃO

A Computação forense é uma arte de descobrir e recuperar informações sobre um fato, de tal forma, a torná-lo admissíveis em tribunal (YASINCAC, MANZANO, 2001). Por meio desse conceito, 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.

OBJETIVO

Descrever o processo de computação forense, explicando brevemente os aspectos relevantes de cada etapa deste processo.

METODOLOGIA

Nesta revisão, foram consultados referências clássicas, todas com domínio pertinente ao nosso assunto: computação forense e suas etapas.

RESULTADOS E DISCUSSÃO

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. De acordo com Eleutério e Machado (2001), a Computação Forense tem quatro etapas

principais: Coleta, Exame, Análise e Relatório. Na etapa coleta, o objetivo dessa 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. No exame: identificar e extrair as informações relevantes a partir dos dados coletados utilizando ferramentas e técnicas forenses adequadas. Na análise: Analisar os resultados do exame para gerar respostas úteis para as questões apresentadas nas fases anteriores. Em 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 (ELEUTÉRIO; MACHADO, 2011). A seguir, serão apresentados os principais aspectos que acontecem nas Etapas supracitadas. **Aspectos relevantes da Etapa de Coleta:** de acordo com LILLARD et al (2010) é fundamental que 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. 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). Segundo BATTULA (2000), Imagem e Espelhamento são técnicas de duplicação/cópia utilizadas na fase de coleta. Existem ainda 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. Em relação à 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), 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. **Aspectos relevantes da Etapa de extração:** segundo LILLARD et al (2010), 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. No processo de extração, duas técnicas se destacam: o Data caving, e a indexação de dados**.** 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). Já 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). **Aspectos relevantes da 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. De acordo com Eleutério e Machado (2001), sobre a análise em dispositivos de armazenamento, 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. Nesse sentido, diversas ferramentas, técnicas e procedimentos podem ser usados para tornar a fase de na análise mais eficiente e viável.

CONCLUSÃO

Computação forense é a fonte para encontrar a evidência da cena do crime através das evidências digitais. A equipe forense computacional trabalha em processo que inclui a identificação, coleta, preservação, análise e relatório. Este processo funciona de forma eficiente para ajudar diversos tipos de investigação. Muitas são as técnicas e ferramentas envolvidas nesse processo.

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;** São Paulo: Person Prentice Hall, 2007.

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

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

AGRADECIMENTOS

Ao professor Dr. Luiz Claudio Machado dos Santos pelas contribuições ao conteúdo deste trabalho.

Não foram declarados conflitos de interesse associados à publicação deste artigo.