MINICURSO – ANÁLISE FORENSE COM AUTOPSY E PALADIN 7

Petter

WWW.PERICIACOMPUTACIONAL.COM

Sumário

1 INTRODUÇÃO 2
2 ESTRUTURA 3
2.1 Coleta 3
2.2 Exame e análise, técnicas e ferramentas 3
3 RESULTADO 3
3.1 Desafio proposto 3
Quesitos apresentados: 4
3.2 Cópia forense, coleta 4
3.3 Respondendo os quesitos. 5
5 CONSIDERAÇÕES FINAIS 10
6 REFERENCES 11
Sobre o autor 12

Minicurso – Análise forense com AUTOPSY e PALADIN 7

Petter Anderson Lopes[1]

Resumo: O objetivo deste mini-curso é fornecer uma visão geral da coleta e análise de dados forenses com a distribuição Linux Paladin 7 e a ferramenta de análise Autopsy. Como tal, a apresentação não tem o objetivo de esgotar o assunto. A apresentação passa para um exemplo de procedimento de coleta forense usando a ferramenta Toolbox da distribuição Paladin 7, depois que a ferramenta Autopsy é usada para analisar o sistema operacional Windows. Esses procedimentos representam as etapas que o Perito Forense aborda para responder as questões técnicas propostas.

1 INTRODUÇÃO

Devido ao grande avanço tecnológico, os sistemas operacionais são atualizados em todos os momentos, portanto, a computação forense também precisa evoluir para acompanhar os objetos de análise. Desta forma, a pesquisa e análise de evidências digitais, tanto para fins legais como comerciais, requer um profissional treinado, que é o Perito Forense ou Especialista Forense.

Para fazer um procedimento correto de coleta e análise, visando a excelência para a elaboração de relatórios, é necessário seguir algumas etapas rigorosas e bem documentadas, o objetivo deste estudo foi explicar algumas etapas para examinar evidências, durante a leitura, será possível fazer uma análise crítica sobre esses tópicos.

Existem muitas ferramentas comerciais para coleta e análise forense no mercado. No entanto, o custo das ferramentas pagas é muitas vezes muito alto, de modo que o uso das ferramentas contidas na distribuição Paladin 7 mostrou-se mais interessante porque são totalmente gratuitos.

[1] System Development, Ethical Hacker, Computer Forensic Expert.