Relatório Forense

João Fiuza de Alencastro 15/0131933

***Abstract*—Relatório destinado à matéria de Segurança de Redes do Departamento de engenharia Elétrica da Universidade de Brasília. Experimento realizado a fim de explorar a vasta área da ciência forense computacional. Será feita uma abordagem teórica, assim como uma abordagem prática.**

***Index Terms*—Segurança, redes, Forensics, Autopsy, p0f, imaging, carving, digital, physical environment.**

I. Introduction

O Termo forense, surge no direito, e é relacionado ao solucionamento de crimes. A Ciência Forense é uma união de aplicações a fim de desvendar o crime, às vezes é uma rotina de testes, outras vezes são só buscas simples. Porém, aqui será estudado um ramo específico da Forense, a Ciência Forense Computacional, voltado somente para a prática dentro do mundo computacional, mais precisamente o armazenamento digital.

Ao pensar em Ciência Forense, devem ser feitos dois questionamentos: ”Quem?” e ”Quando?”. E o armazenamento digital comumente deixa rastros dessas duas perguntas.

Um exemplo encontrado em [2], demonstra a importância dos rastros virtuais para a justiça brasileira: ”Na justiça trabalhista, a Computação Forense adquiriu extrema importância, já que a partir da portaria 1510 de 2009 do MTE, o Registro Eletrônico deve ser utilizado em todas as empresas em território nacional, descontinuando o arcaico relógio e as assinaturas em folhas de sulfite, devendo emitir um comprovante para o funcionário. Já no ano de 2012 a portaria 373/12, habilitou sistemas alternativos para a marcação do ponto, permitindo o uso de aplicativos, mensagem de texto, softwares específicos, código de barras, basicamente qualquer sistema que garanta a integridade dos registros”. Todos os exemplos citados servem como evidências de auditoria e podem ser utilizados no tribunal.

A Forense Computacional atualmente, é dividida em três partes: Análise (Digital), Coleta (imaging) e a Extração (carving). Essa divisão mantém uma organização do fluxo de trabalho. Assim como testes de penetração, a prática forense deve ser realizada sequencialmente, de forma responsável, para que não haja perdas de evidências e provas valiosas.

A. Digital Forensics (Análise)

A análise

B. Imaging Forensics (Coleta)

C. Carving Forensics (Extração)

II. Conclusion

References

[1] https://www.significados.com.br/forense/
[2] https://www.contabeis.com.br/artigos/5035/seguindo-os-rastros-virtuais-computacao-forense/