Anais do I Congresso de Ciência e Tecnologia da PUC Goiás
Disponível em: http://pucgoias.edu.br/ucg/prope/pesquisa/anais/2015/index.htm
ISSN: 2177-3327

ANALISE DE MÉTODOS FORENSE EM IMAGENS

BRUNO DIAS GARCIA EIREA; SIBELIUS VIEIRA
bnoeirea@gmail.com

Objetivo: Este trabalho tem o objetivo de analisar métodos comumente utilizados por infratores para esconder arquivos gráficos em discos rígidos, por exemplo, imagens de pedofilia. Ao longo do trabalho serão abordados técnicas de ofuscação, recuperação e detecção destes arquivos gráficos. **Método:** Os experimentos realizados neste trabalho seguem um padrão de desenvolvimento descrito em três etapas: Ofuscação da imagem (Etapa 1): Recuperação da imagem (Etapa 2): Detecção das ofuscações (Etapa 3). Para recuperar as imagens (Etapa 2), foram utilizados os mesmo programas usados na ofuscação, pois cada um deles possui uma ferramenta responsável por fazer tal ação. Na etapa 3, em todos os casos, foi copiado os arquivos alterados para um pendrive de 8Gb. Em seguida, utilizando o programa FTK Imager foi feito uma imagem no formato '.dd' deste pendrive. Depois da imagem pronta, foi utilizado os programas Forensic Toolkit (FTK), Autopsy e Foremost (Kali Linux), com o intuito de descobrir a existência de arquivos gráficos ocultos. **Resultados:** Ao todo, foi realizado 12 experimentos de esteganografia, 1 experimento de ofuscação em máquinas virtuais e 1 de ofuscação em espaço de disco não alocado. Todos os experimentos de esteganografia não foram detectados pelas ferramentas de análise forense, ao contrário dos outros experimentos. **Conclusão:** Ao fim dos experimentos, foi notado que os métodos de esteganografia são indetectáveis por softwares utilizados por peritos criminais, pois a esteganografia, geralmente, utiliza métodos de cifragem de dados, e estes softwares não realizam a decifragem. Mas outras maneiras de ofuscação, por exemplo, ofuscação em máquinas virtuais, foram facilmente detectadas por estes softwares.

Palavras-chave: Ofuscação. Forense. Esteganografia