DATA CARVING: ANÁLISE UTILIZANDO FOREMOST EM DUMPS DE MEMÓRIA VOLÁTIL E NÃO VOLÁTIL

Bruno Roberto Bricce[1]; Henrique Pachioni Martins[1]

[1]Pró-Reitoria de Pesquisa e Pós Graduação - Universidade do Sagrado Coração (USC). E-mail: bruno.bricce@gmail.com; henrique.martins@usc.br

Tipo de pesquisa: Artigo Científico
Agência de Fomento: Não há
Área de conhecimento: Ciências Exatas – Segurança da Informação

Atualmente surgem diversas situações onde é necessária a recuperação de dados, seja em uma perícia envolvendo recursos computacionais ou até mesmo dados pessoais que foram apagados. Para isso existem ferramentas e técnicas que tornam possíveis a recuperação de arquivos. A ferramenta *foremost* foi desenvolvida para uso em distribuições Linux, com esse aplicativo é possível resgatar conteúdos apagados de memórias não voláteis ou processos que estavam sendo executados em uma memória volátil (RAM). A fim de demonstrar o desempenho da ferramenta de recuperação de dados, este trabalho é uma pesquisa que teve como o objetivo analisar o uso da ferramenta de recuperação de dados *foresmost* em *dumps* de memórias. Mostrando-se capaz de recuperar arquivos em memórias voláteis e não voláteis, o aplicativo pode ser utilizado para uma investigação forense de acordo com a metodologia adotada pelo perito, visto que alguns arquivos dependeriam da utilização de softwares específicos para recuperação total ou parcial de dados. Mesmo com certa limitação, a ferramenta se mostrou adequada na recuperação de arquivos e processos da memória RAM, assim como de um disco rígido. Por se tratar de um software gratuito e ao mesmo tempo estar disponível em distribuições Linux, em alguns já pré-instalados, o *foremost* é um aplicativo hábil e que cumpre o seu papel na recuperação de arquivos e processos a partir de *dumps* e cópias bit a bit.

Palavras-chave: *Foremost*. Forense Computacional. Recuperação de Arquivos.