

Perícia Forense Computacional

Material de aula

- [Introdução - Definições](#)
- [Introdução - Terminologia](#)
- [Duplicação de mídias - Recuperação de arquivos apagados](#)
- [Noções de Data Carving](#)
- [Análise de memória RAM](#)
 - [Link para documentação do Volatility Framework](#)
- [Captura e Análise de Tráfego](#)
- [Análise de LOGs](#)
- [Análise de máquinas comprometidas](#)
- [Recomendações para relatórios](#)

Práticas

- [Duplicação de mídias - Local](#)
- [Duplicação de mídias - Remoto](#)
- [Recuperação de arquivos apagados](#)
 - Link para download da imagem será enviado via SUAP
 - Usando Windows? Os softwares (*FTK Imager* e *sha256sum.exe*), podem ser baixados da Internet
- [Descrição da segunda prática de carving](#)
 - [Imagem da partição para a segunda prática de carving](#)
- [Descrição da atividade - análise de memória](#)
 - Baixe [este](#) arquivo, descomprima, e proceda com a análise utilizando o [Volatility Framework](#).
- Prática de análise de tráfego:
 - [descrição aqui](#)
 - Arquivo no formato *libpcap* para testes [aqui](#)
- Análise de LOGs [prática 01](#)
 - SHA256SUM:
8fd43b6898a934546f82ed5dc13c1506bc405f09b0157b42c780ab23595127a1

Trabalhos e atividades avaliativas

- [Descrição da atividade - carving email](#)
 - [Mensagem de e-mail](#) (este arquivo está comprimido, pois só consigo enviar para a página desta forma. Descomprima o mesmo antes de iniciar a atividade)

- [Descrição da atividade - carving arquivo](#)

- **Observação** : baixe

este

arquivo, descomprima e inicie o trabalho.

From:
<http://diatinf.ifrn.edu.br/prof/> - **Docentes da DIATINF**

Permanent link:
http://diatinf.ifrn.edu.br/prof/doku.php?id=user:1379492:pericia_forense_computacional&rev=1568050431

Last update: **2019/09/09 17:33**

