UNIVERSIDADE CATÓLICA DE BRASÍLIA

Pós-graduação Lato Sensu em Perícia Digital

Turma 11 - Fundamentos em perícia digital - Prof. Eriberto

- Atualizado em 25 mai. 2015 -

Cronograma de aulas

Aula	Data	Previsão de aula
1	**27 fev**	• Apresentação e objetivos da disciplina. • Site do professor. • Guias de referência no site do professor e uso em aula e prova. • Trabalho em duplas nas aulas. • Prova teórico-prática e trabalho em grupo (não há parte impressa). • Faltas às aulas (tolerância para faltas). • Respeitar o horário de intervalo do professor. Tratamento pelo nome. • Importância de estudar e conhecer bem GNU/Linux, shell script e expressões regulares. • A língua inglesa... • Bibliografia. • Virtualbox e Cygwin como apoio ao aprendizado. ---------- • Partições, setores, filesystems, blocos e diretórios (abstração). • Inode. • Diferenças entre filesystems. Área de controle e área de dados. • Deleção de dados e formatação de discos.
2	**04 mar**	• **Temas para trabalhos em grupo.** • Links e hard links. • Slack space. • Testes com filesystems. • MACB times (ou mactimes). Linha do tempo.
3	**13 mar**	• **Grupos x temas.** • Integridade de arquivos. • Imagens de discos e partições. • Discos virtuais em máquinas virtuais. Conceito de arquivos com filesystems e enjaulamento.
4	**20 mar**	• Gerência de memória. • Imagens de memória.
5	**25 mar**	• FHS. Diretórios em SO GNU/Linux. • Ferramentas GNU/Linux para a forense computacional. • Sleuthkit. • Forensics Wiki. • Introdução à técnica de forense computacional.
6	**17 abr**	• Introdução à técnica de forense computacional. • Permissões de arquivos. Permissões estendidas. • Comandos egrep (-i, -o, -v, -C, --color) e find. Influência do shell. Txt2regex. • xhost+

7	**08 mai**	• Caso 00: análise conduzida. • Análise parcial do Caso 00.
8	**15 mai**	• Caso 00: análise conduzida. • Análise parcial do Caso 00.
9	**20 mai**	• Caso 00: análise conduzida. • Análise final do Caso 00. • Caso 00a: análise avançada conduzida.
10	**22 mai**	• Análise parcial do Caso 00a. • Caso 00a: análise avançada conduzida. • Análise parcial do Caso 00a.
11	**25 mai**	• Caso 00a: análise avançada conduzida. • Análise parcial do Caso 00a.
12	**01 jun**	• Caso 00a: análise avançada conduzida. • Análise final do Caso 00a. • Caso 00e: Pendrive com vírus. • Análise do Caso 00e.
13	**05 jun**	• Caso 00c: análise avançada conduzida (memória RAM). • Análise do Caso 00c. • Caso 00f: Partições perdidas. • Análise do Caso 00f.
14	**15 jun**	• Caso 00d: Análise de e-mail conduzida. • Análise do caso 00d. • Caso 02: o pendrive de um estelionatário. • Análise do caso 02.
15	**19 jun**	• Análise do Laudo do caso 02. • Caso 03: Invasão na Internet.
16	**22 jun**	• Caso 03: Invasão na Internet. • Análise do caso 03.
17	**26 jun**	• Prova teórico-prática individual. 2 horas. Consulta apenas ao Canivete suíço do shell Bash e às manpages dos comandos. • Entrega do resultado da prova.
18	**29 jun**	• Trabalho em grupo (20 minutos por grupo).
REC	**03 jul**	• Prova de recuperação.

Temas para trabalhos em grupo:

- Distribuições live para forense (explanar sobre, pelo menos, quatro; incluir Kaly, Caine e Win-UFO).

- Virtualização com Xen, KVM+libvirt, VMWare e VirtualBox.

- Ferramentas livres para uso na forense computacional (pelo menos cinco; incluir afflib e volatility). Não abordar live CD/DVDs.

- Ferramentas proprietárias para forense computacional (pelo menos cinco; incluir FTK e EnCase). Não abordar live CD/DVDs.

- Forense em celulares.