UNIVERSIDADE CATÓLICA DE BRASÍLIA

Pós-graduação Lato Sensu em Perícia Digital

Turma 12 - Fundamentos em perícia digital - Prof. Eriberto

- Atualizado em 03 nov. 2015 -

Cronograma de aulas

Aula	Data	Previsão de aula
1	**29 ago**	• 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). Pendrives. • Inode. • Área de controle e área de dados. • Deleção de dados e formatação de discos. • Links e hard links.
2	**05 set**	• **Temas para trabalhos em grupo.** • Slack space. • Testes com filesystems. • MACB times (ou mactimes). Linha do tempo. • Integridade de arquivos. • Imagens de discos e partições.
3	**12 set**	• **Grupos x temas.** • Discos virtuais em máquinas virtuais. Conceito de arquivos com filesystems e enjaulamento. • Gerência de memória. • Imagens de memória.
4	**26 set**	• FHS. Diretórios em SO GNU/Linux. • Forensics Wiki. • Introdução à técnica de forense computacional.
5	**10 out**	• Permissões de arquivos. Permissões estendidas. • Comandos egrep (-i, -o, -v, -C, --color) e find. Influência do shell. Txt2regex. • xhost+ • Caso 00: análise conduzida.
6	**24 out**	• Caso 00: análise conduzida. • Análise parcial do Caso 00.
7	**31 out**	• Caso 00: análise conduzida.

		• Análise parcial do Caso 00.
8	**03 nov**	• Caso 00: análise conduzida. • Análise final do Caso 00. • Caso 00a: análise avançada conduzida.
9	**07 nov**	• Análise parcial do Caso 00a. • Caso 00a: análise avançada conduzida. • Análise parcial do Caso 00a.
10	**12 nov**	• Caso 00a: análise avançada conduzida. • Análise parcial do Caso 00a.
11	**14 nov**	• Caso 00a: análise avançada conduzida. • Análise final do Caso 00a. • Caso 00e: Pendrive com vírus. • Análise do Caso 00e.
12	**24 nov**	• Caso 00c: análise avançada conduzida (memória RAM). • Análise do Caso 00c. • Caso 00f: Partições perdidas. • Análise do Caso 00f. • Caso 00d: Análise de e-mail conduzida. • Análise do caso 00d.
13	**28 nov**	• Caso 02: o pendrive de um estelionatário. • Análise do caso 02. • Análise do Laudo do caso 02. • Caso 03: Invasão na Internet. • Análise do caso 03.
14	**01 dez**	• Prova teórico-prática individual. 2 horas. Consulta apenas ao Canivete suíço do shell Bash e às manpages dos comandos. • Entrega do resultado da prova.
15	**12 dez**	• Trabalho em grupo (20 minutos por grupo).
REC	**11 dez**	• 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 e dispositivos móveis.