

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS FORENSES

Perícia Forense Computacional (Optativa)

Ementa: Conceitos básicos de forense computacional; cenários de perícia em informática; evidências digitais; tipos de perícias; padrões de exame forense computacional; coleta e análise de evidências digitais; análise forense em redes; modelos de experimentos práticos de intrusão para prova de conceito; abordagem in vivo e post mortem; Cadeia de custódia; Descrição de materiais questionados; Estrutura mínima do laudo pericial; Estrutura do sistema pericial público; Conceito e definição de ferramentas de código livre e ferramentas de código proprietário; Estrutura de um sistema pericial privado; Legislação aplicada à perícia cível; Legislação aplicada à perícia criminal; Conceitos básicos de estruturas internas dos softwares e Configuração de auditoria e segurança de sistema operacional; Classes de redes e endereçamento IP; Descrição dos serviços ligados ao TCP/IP; Arquivos PCAP; Identificação e recuperação de Artefatos em conexões TCP; Análise dinâmica das evidências; Limitadores da Network Forensic; Projetando Redes Ideais para retenção de melhores evidências; Análise Dinâmica e de malware; Trabalhando com executáveis e com documentos maliciosos; Formato *Portable Executable*; Trabalhando com DLLs; *Memory Forensics*; Definição de Rootkits e *Web Malware*; *Packers* e *Anti-Debugging*.

Créditos/Carga Horária: 4/60h

Referências: 1. VECCHIA, E.D. Perícia Digital: da Investigação à Análise Forense. Ed. Millennium, 2019, 424p. 2. FARMER, Dan; VENEMA Wietse; Perícia Forense Computacional: Teoria e Prática Aplicada, Ed. Pearson. 2006, 190p. 3. CASEY, Eoghan; Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet, Ed. Elsevier, 2011. 4. CARVEY, Harlan; Windows Forensic Analysis, Ed. Syngress, 2009. 5. MELO, S.; Computação Forense com Software Livre, Ed. Alta Books, 2009. 6. FREITAS, Andrey R.; Perícia Forense Aplicada à Informática, Ed. Brasport, 2006. 7. VELHO, J. A. Tratado de Computação Forense, Ed. Millennium, 2016. 8. SILVA, P. M.; MACHADO, E. M. P. Desvendando a Computação Forense, Ed. Novatec, 2011. 9. MELO, S.; Computação Forense com Software Livre, Ed. Alta Books, 2009. 10. FREITAS, A.R.; Perícia Forense Aplicada à Informática, Ed. Brasport, 2006.