CAMPUS: Centro de Ciências Agrárias					
CURSO: Ciência da Computação					
HABILITAÇÃO: Bacharel em Ciência da Computação					
DEPARTAMENTO RESPONSÁVEL: Departamento de Computação					
IDENTIFICAÇÃO: COMPUTAÇÃO FORENSE					
CÓDIGO	**DISCIPLINA OU ESTÁGIO**			**PERIODIZAÇÃO IDEAL**	
COM10607	Disciplina			7º período	
OBRIG./OPT.	**PRÉ/CO/REQUISITOS**			**ANUAL/SEM.**	
OPTATIVA	COM10394 – REDES DE COMPUTADORES			Anual	
CRÉDITO	**CARGA HORÁRIA TOTAL**	**DISTRIBUIÇÃO DA CARGA HORÁRIA**			
		TEÓRICA	EXERCÍCIO	LABORATÓRIO	OUTRA
3	60h	45h	0h	15h	0h
NÚMERO MÁXIMO DE ALUNOS POR TURMA					
AULAS TEÓRICAS	AULAS DE EXERCÍCIO	AULAS DE LABORATÓRIO		OUTRA	
20		20			

OBJETIVOS (Ao término da disciplina o aluno deverá ser capaz de:)

- Descrever o que é uma investigação de Digital, quais são as fontes de evidências digitais e quais são as limitações da ciência forense.
- Entender como projetar softwares para apoiar a computação forense.
- Descrever os requisitos legais para a utilização dos dados apreendidos (quando necessário).
- Compreender o processo de apreensão das evidências, desde o momento em que o foi identificada a necessidade da apreensão até a disposição (armazenamento) dos dados.
- Coletar os dados no armazenamento adequado, tanto a cópia original, quanto a cópia forense.
- Conhecer a responsabilidade e obrigação de uma pessoa no momento que ela atua como examinador forense.
- Descrever a estrutura do sistema de arquivos para um determinado dispositivo (NTFS, MFS, iNode, HFS, ...) e recuperar dados baseados na pesquisa de determinados termos em um sistema de imagens.
- Reconstruir a história de diligência a partir de seus artefatos (rastros).
- Reconstruir o histórico de navegação web a partir de seus artefatos (rastros).
- Captar e interpretar o tráfego da rede.
- Discutir os desafios associados com dispositivos móveis.
- Avaliar a presença de *malware* ou atividade maliciosa um sistema (rede, computador ou aplicativo).
- Aplicar ferramentas de análise forense para investigar violações e brechas de segurança.
- Conhecer o processo de inutilização de certas ferramentas forenses.

CONTEÚDO PROGRAMÁTICO (Título e descriminação das Unidades)

1. **Introdução:** ch. prevista: 4h/a
   1.1. Princípios básicos;
   1.2. Metodologias de análise forense digital;
   1.3. Desenvolvimento de ferramentas para a análise forense.
2. **Procedimentos legais:** ch. prevista: 4h/a
   2.1. Regras para atuar com evidências;
   2.2. Jurisdições;
   2.3. Cadeia de Custódia.
3. **Busca e apreensão de provas:** ch. prevista: 8h/a
   3.1. Provas Digitais: métodos e padrões;
   3.2. Técnicas e padrões para a preservação de dados;
   3.3. Emissão de relatórios no trabalho de perícia;
4. **Análise forense:** ch. prevista: 20h/a
   4.1. Em sistemas de arquivos;
   4.2. Em aplicações;
   4.3. Em sistemas web;
   4.4. Na rede de computadores;
   4.5. Em dispositivos móveis.
5. **Descrição de ataques:** ch. prevista: 6h/a
   5.1. De computador;
   5.2. De rede;
   5.3. De sistema.
6. **Investigação e detecção de ataques.** ch. prevista: 10h/a
7. **Métodos Anti-forense.** ch. prevista: 8h/a

BIBLIOGRAFIA BÁSICA

- Nelson, B.; Phillips, A.; Enfinger, F.; Steuart, C.; *Guide to Computer Forensics and Investigations*. 3ed, Ed. Thomson, 2007. ISBN: 9781418067335.
- Costa, M. A. S. L.; *Computação Forense*. 2ed, Ed. Milleminum, 2003. ISBN: 8586833991.
- Farmer, D.; Venema, W.; *Perícia Forense Computacional*: Teoria e Prática Aplicada. 1ed, Ed. Prentice Hall, 2007. ISBN: 8576051281.

BIBLIOGRAFIA COMPLEMENTAR

- Jones, K. J.; Bejtlich, R.; Rose, C. W.; *Real Digital Forensics*: Computer Security and In Response. Ed. Addison Wesley, 2005. ISBN: 9780321240699.
- Carvey, H.; *Windows Forensic Analysis*. Ed. Syngress, 2007. ISBN: 9781597491563.

MEIOS DIDÁTICOS E METODOLOGIA DE ENSINO

Aulas expositivas. Discussões e debates do conteúdo apresentado. Dinâmicas. Utilização dos recursos didáticos: Quadro Branco, Pincel, Projetor Multimídia (datashow), livros, artigos.

Em algumas partes do curso, além do conhecimento teórico, são abordados aspectos práticos através de experimentações e implementações de diversas técnicas ou conceitos.

Alguns tópicos são estudados procurando aprofundar os aspectos importantes, permitindo que o aluno possa dar continuidade ao estudo da área e aplicar, de forma autônoma, os conhecimentos adquiridos. Outros pontos são apresentados sem caráter formativo, mas procurando dar uma visão abrangente da área e de suas

aplicações.

As aulas tipicamente têm o seguinte roteiro geral:

• Apresentação expositiva dos conceitos;

• Apresentação de algoritmos, implementações ou exemplos de aplicação prática dos conceitos;

• Apresentação de soluções de problemas que requeiram a aplicação dos conceitos;

• Discussão sobre outras possíveis aplicações fazendo análises comparativas de pontos relacionados ao conceito que está sendo estudado;

• Proposição de exercícios de fixação ou avaliativos.

Além do acompanhamento das aulas expositivas, as principais atividades a serem desenvolvidas pelos alunos são:

• Resolução de exercícios extraídos da bibliografia básica ou elaborados pelo professor;

• Desenvolvimento de trabalhos de implementação de algoritmos e de técnicas;

• Desenvolvimento de trabalhos de experimentação de técnicas e de sistemas;

• Leitura e estudo de artigos, de capítulos de livros e de material elaborado pelo professor.

Os trabalhos extraclasse têm a finalidade de consolidar os conhecimentos vistos em sala de aula e de permitir que o aluno adquira alguma experiência na utilização prática dos mesmos.

Visando, ainda, o desenvolvimento das habilidades de elaboração e de apresentação de trabalhos, os alunos deverão entregar suas atividades no formato de uma pequena monografia. Em algumas atividades, os alunos ainda deverão fazer sua apresentação em sala usando os recursos cabíveis.

RECURSOS TECNOLÓGICOS

Como ferramentas de apoio e auxílio ao aprendizado, serão utilizados nos trabalhos práticos: programas e distribuições GNU/Linux relacionados ao escopo de forense computacional.

CRITÉRIOS DE AVALIAÇÃO DA APRENDIZAGEM

- Participação, envolvimento, análise e debates (críticos e/ou construtores) relativos ao conteúdo apresentado na aula;
- Realização das listas de exercícios utilizadas para dirigir o conteúdo programático;
- Distribuição da nota total da etapa:
    - Duas provas teóricas, totalizando 80% da nota total;
    - Trabalhos práticos no decorrer da disciplina, totalizando 20% da nota total.
- Serão utilizados os critérios de aprovação definidos no regimento interno da Universidade:
    - Mínimo de 75% de presença;
    - A nota final do aluno será a média aritmética das provas e trabalhos realizados;
    - O aluno será dispensado da Prova Final se possuir 70% da nota total;
    - Após a prova final, o aluno que obtiver média igual ou superior a 50% será considerado aprovado na disciplina, caso contrário será reprovado.

EMENTA (Tópicos que caracterizam as unidades dos programas de ensino)

Princípios básicos de Ciência Forense e áreas de atuação. Conceitos básicos da perícia criminal e cível. Tecnologias disponíveis nas áreas de Computação Forense. Ferramentas tecnológicas para processamento e

análise de evidências. Desenvolvimento de sistemas de apoio às áreas de Computação Forense.

APROVAÇÃO (Número dos respectivos documentos)		
CÂMARA DEPARTAMENTAL	COLEGIADO DE CURSO	CONSELHO DEPARTAMENTAL

ASSINATURA (S) DO(S) RESPONSÁVEL(EIS)
Prof. Jacson Rodrigues Correia da Silva _____