IPOG INSTITUTO DE PÓS-GRADUAÇÃO & GRADUAÇÃO

DESCUBRA O MELHOR QUE VOCÊ PODE SER.

CARGA HORÁRIA

432
horas/aula

PÓS GRADUAÇÃO

COMPUTAÇÃO FORENSE & PERÍCIA DIGITAL

POR QUE ESCOLHER O IPOG?

Instituição de ensino superior presente em todos os estados do Brasil e Distrito Federal.

Professores altamente qualificados e com comprovada experiência de mercado.

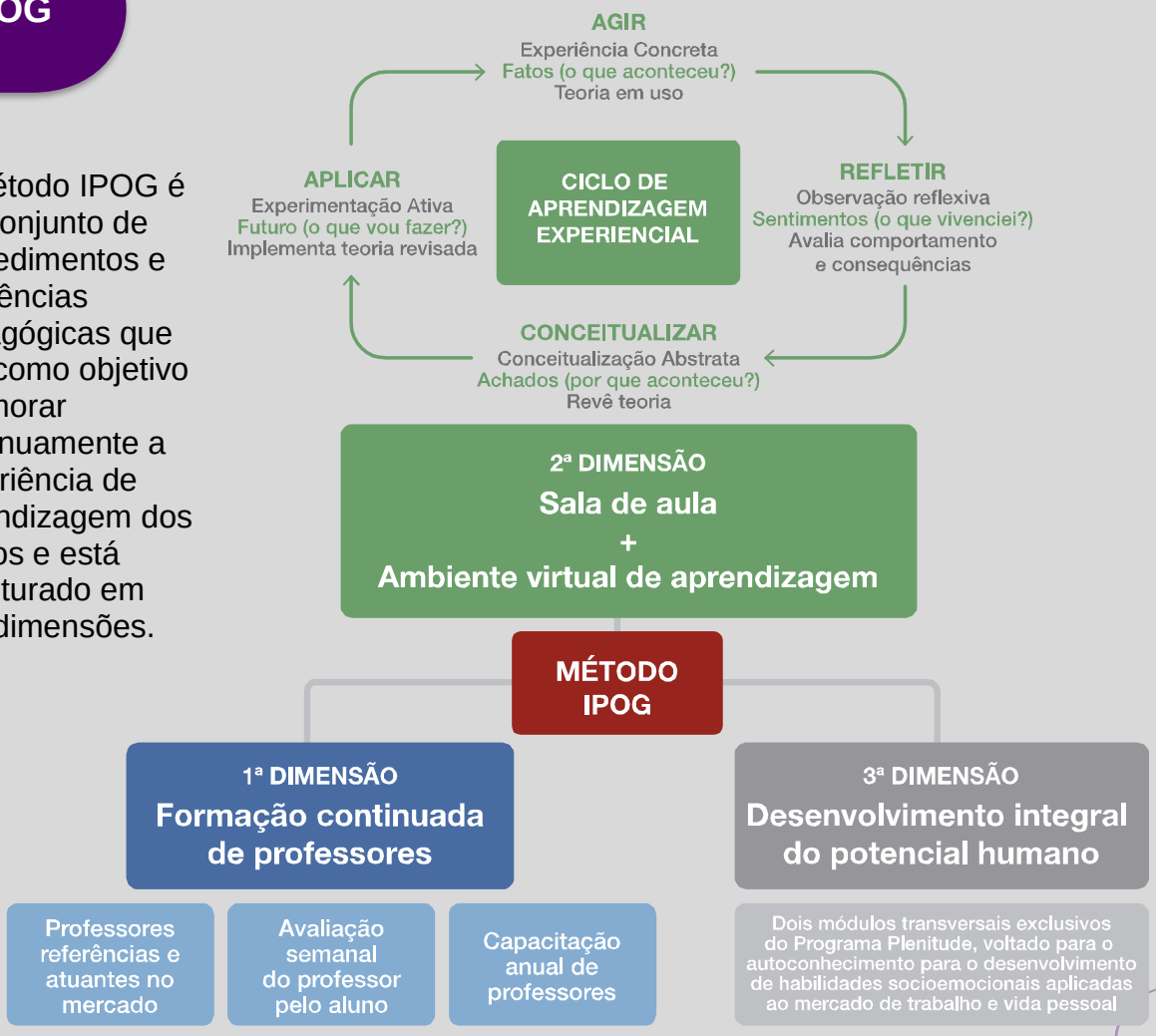
97,14% de satisfação nas avaliações dos alunos.

Cursos reconhecidos pelo MEC.

Chancela própria.

MÉTODO IPOG

O Método IPOG é um conjunto de procedimentos e referências pedagógicas que têm como objetivo aprimorar continuamente a experiência de aprendizagem dos alunos e está estruturado em três dimensões.



APRESENTAÇÃO DO CURSO

Com o incessante e rápido avanço tecnológico temos uma melhoria constante na vida das pessoas. Na mesma proporção, esses avanços também são utilizadas para o cometimento de delitos. Desta forma, devemos utilizar os avanços tecnológicos e as novas técnicas desenvolvidas na mesma relação para aprimorarmos a produção da prova material, tanto no âmbito criminal quanto civil.
Visando enfrentar a verdadeira epidemia de crimes cibernéticos que assola a rede mundial de computadores, torna-se cada vez mais necessário para profissionais de T.I. e organizações públicas e privadas o domínio de técnicas de análise forense aplicadas ao âmbito computacional.
A Análise Forense Computacional consiste em um conjunto de técnicas para coleta e exame de evidências digitais, reconstrução de dados e ataques, identificação e rastreamento de invasores. Esta especialização visa apresentar aos alunos os conceitos essenciais da investigação forense digital, tais como:

- Volatilidade de evidências e coleta de dados em um sistema em execução.
- Recuperação de informações parcialmente destruídas.
- Reconstrução da linha temporal dos eventos.
- Prevenção de armadilhas instaladas por invasores.
- Compreensão da lógica dos sistemas de arquivos.
- Reconhecimento de artefatos maliciosos e técnicas de recuperação de dados armazenados em memória.

O curso tem enfoque prático, com o objetivo de fornecer aos alunos as habilidades necessárias à investigação de sistemas potencialmente comprometidos, conhecimento sobre ataques comuns e preparação para trabalhar em uma investigação legal.
A Análise Forense Computacional é voltada para Técnicos, Analistas e Administradores de Redes que desejam obter o conhecimento e as habilidades técnicas necessárias à realização de uma investigação forense em sistemas computacionais, bem como para recuperação forense de evidência. Além disso, com a nova alteração do Código de Processo Penal algumas atribuições foram acrescentadas ao Assistente Técnico. As alterações consistem de alguns pontos básicos (Lei 11690, de 9/6/2008, artigo 159):

> § 4º O Assistente Técnico atuará a partir de sua admissão pelo Juiz e após a conclusão dos exames e elaboração do laudo pelos Peritos Oficiais, sendo as partes intimadas desta decisão.
> § 5º Durante o curso do processo judicial, é permitido às partes, quanto à perícia:
>
> I) Requerer a oitiva dos Peritos para esclarecerem a prova ou para responderem a quesitos, desde que o mandado de intimação e os quesitos ou questões a serem esclarecidas sejam encaminhados com antecedência mínima de 10 (dez) dias, podendo apresentar as respostas em laudo complementar;
>
> II) Indicar Assistentes Técnicos que poderão apresentar pareceres em prazo a ser fixado pelo Juiz ou serem inquiridos em audiência.

Por essa razão, o IPOG tem a satisfação de oferecer este curso de pós-graduação em **Computação Forense & Perícia Digital**, desenvolvido por Peritos Criminais e outros especialistas de diversas áreas do conhecimento científico. Ao final do curso, o especialista será capaz de analisar laudos emitidos nas áreas abrangidas pelas matérias ministradas, e estará tecnicamente apto a atuar como Assistente Técnico Judicial, bem como produzir esses mesmos laudos utilizando o ferramental tecnológico apresentado no curso.

OBJETIVOS

• Capacitar profissionais atuantes na área ou que nela pretendam ingressar (em conformidade com as exigências atuais do mercado de trabalho em Perícia), proporcionando conhecimentos necessários para a análise de mídias em geral e recuperação de evidências, bem como a elaboração e análise de laudos periciais.

DIFERENCIAIS DO CURSO

• Corpo docente formado por Peritos em Informática da Polícia Federal, que apresentam as mesmas técnicas e softwares utilizados nas principais polícias do mundo na elucidação dos crimes cibernéticos.
• Ampliação de atuação profissional.
• Formação curricular e ferramental inédita.
• Networking qualificado.
• Alta empregabilidade para profissionais com esta especialização.
• Módulos práticos imediatamente aplicáveis à atuação profissional.
• Utilização de softwares como ferramentas de trabalho.

PARA QUEM É ESTE CURSO?

• Profissionais com curso superior em todas as áreas afins à Tecnologia da Informação, bem como aqueles que tenham notório saber em T.I., com curso superior de graduação reconhecido pelo MEC.

FORMAÇÃO CURRICULAR

1) Introdução à Criminalística e Computação Forense
2) Introdução aos Aspectos Legais de Computação Forense
3) Tópicos em Sistemas Operacionais
4) Desenvolvimento Integral do Potencial Humano
5) Análise Forense do Sistema Operacional LINUX
6) Análise Forense do Sistema Operacional Windows
7) Análise de Mídias Utilizando Ferramenta Forense FTK I
8) Análise de Mídias Utilizando Ferramenta Forense FTK II
9) Análise de Mídias Utilizando Software Livre
10) Prática em Análise Forense I
11) Prática em Análise Forense II
12) Análise de Local na Rede Mundial
13) Análise de Tráfego e Captura de Pacotes
14) Criptografia e Criptoanálise
15) Introdução ao Processamento Forense de Imagens I
16) Introdução ao Processamento Forense de Imagens II
17) Análise de Equipamentos Computacionais Portáteis e de Telefonia Móvel
18) Tópicos Avançados em Computação Forense

MATRIZ CURRICULAR E EMENTAS

INTRODUÇÃO À CRIMINALISTICA E COMPUTAÇÃO FORENSE
Definição e histórico da criminalística. Perito e Assistente Técnico à luz do Código de Processo Penal. Vestígios, indícios e evidências. Exame de corpo de delito: Material Padrão, Material Questionado, Confronto. Laudo Pericial e Parecer Técnico. Principais áreas de atuação da criminalística: Arrombamento, Morte Violenta, Medicina Legal, Identificação Papiloscópica, Acidente de Tráfego, Incêndio, Documentoscopia, Merceologia, Balística, Veículos, Química Forense, Perícias Econômico-Financeiras, Engenharia Legal, Meio Ambiente, Audiovisual e Eletrônicos, Computação Forense. Introdução a Computação Forense. Características da Prova Digital. Tipos de mídias de armazenamento computacional. Preservação dos dados do material questionado. Espelhamento X Imagem. Integridade dos dados e utilização de funções HASH. Descrição do material examinado: identificação do estado do material questionado, da marca, modelo, número de série e capacidade dos equipamentos. Análise de dados: recuperação de arquivos apagados/danificados, busca por palavras-chave, análise de mensagens eletrônicas. Exames em sítios de Internet.

INTRODUÇÃO AOS ASPECTOS LEGAIS DE COMPUTAÇÃO FORENSE
Contexto. Apresentação técnico-processual da prova na teoria geral do processo: conceito, objeto e finalidade. As provas em espécie e suas correlações. A prova pericial: procedimentos, modalidades e figuras afins. O Perito: atribuições, responsabilidades e impedimentos. Legislação aplicada a Perícia Criminal. A prova nas Cidades Digitais. Identidade e Identificação. Questões de ordem prática.

TÓPICOS EM SISTEMAS OPERACIONAIS
Aspectos introdutórios à computação forense. Mídias de armazenamento computacional. Introdução à análise de volumes de mídias computacionais. Sistemas de arquivos da família Microsoft Windows (FAT, exFAT e NTFS). Sistema de arquivos ISO9600. Introdução à análise forense de arquivos.

DESENVOLVIMENTO INTEGRAL DO POTENCIAL HUMANO
Fatores que conduzem ao Desenvolvimento Integral do Potencial Humano; Desafios do desenvolvimento humano ao longo das 8 etapas do ciclo da vida; Sobre as diferenças entre o caminho do murchamento e o caminho do florescimento dos potenciais humanos; A diferença entre caráter e personalidade; As virtudes e as forças de caráter - Introdução à Visão Integral; As Linhas de Desenvolvimento ou Inteligências Múltiplas; Os Níveis de Desenvolvimento humano; A Dinâmica da Espiral - os 8 níveis de desenvolvimento de valores ou memes; Análise e devolutivas de instrumentos de autoconhecimento; Estados de Consciência; Quadrantes: matriz integral do desenvolvimento integral humano; A dialética do desenvolvimento: diferenciação e integração; A matriz da Plenitude; Nossa Capacidade de Transformação Pessoal (CTP).

ANÁLISE FORENSE DO SISTEMA OPERACIONAL LINUX
Conceitos básicos; Sistemas de arquivos LINUX; MAC Times; Duplicação forense em LINUX; Estudo de caso: Linux; Ferramentas de análise em sistemas Linux; Estabelecendo um *timeline* dos últimos acessos feitos em um sistema; Data Carving: procurando arquivos específicos; Outras fontes de informação em sistemas UNIX; Anti-forense em sistemas LINUX.

ANÁLISE FORENSE DO SISTEMA OPERACIONAL WINDOWS
Introdução à Análise Forense da família Microsoft Windows. Componentes do Sistema Operacional Windows. Processo de Análise Forense: metodologia *post mortem* aplicada a Sistemas Operacionais Windows. Registro do Windows: principais chaves de interesse forense. Artefatos de interesse forense do Sistema Operacional. Artefatos da web e de e-mail de interesse forense. Análise de Memória: metodologia *live analysis*, aquisição da memória RAM e análise de *dumps* de memória.

ANÁLISE DE MÍDIAS UTILIZANDO FERRAMENTA FORENSE FTK I
Instalação e configuração do FTK e seus componentes principais como *FTK Imager*, Registry Viewer, Gerenciador de Licenças, Seletor de Idioma, PRTK e Oracle. Usuários e perfil de acesso à interface do FTK. Configuração de temporários e sua relação com o desempenho do aplicativo. Utilização do FTK Imager para criar imagens de evidências digitais. Conversão de imagens em formatos DD, EnCase e AD1. Conceitos básicos de organização de mídias digitais. Conceitos Básicos de Sistemas de Arquivos FAT e NTFS. Visualização de evidências. Verificação de evidências. Exportar arquivos contidos em evidências. Propriedades de arquivos contidos em evidências. Visualizador HEX

do FTK Imager e utilitário de conversão/interpretação de valores hexadecimais. Criando um novo caso no FTK. Opções de pré-processamento e o impacto nas informações geradas. Data carving automático. Interface de visualização de artefatos: HEX, Text, Filtered e Natural. Utilizando QuickPick. Categorização de artefatos. Visualização do sistema de arquivos. Visualização de emails. Visualização de gráficos. Inserção e customização. Utilização de filtros para reduzir o espaço de buscas. Criação de filtros. Criação de Bookmarks. Indexação e busca por palavras chave. Importando lista de palavras chave. Busca sequencial. Expressões Regulares e busca por padrões de texto.

ANÁLISE DE MÍDIAS UTILIZANDO FERRAMENTA FORENSE FTK II
Revisão dos conceitos básicos do FTK. Data Carving para arquivos do tipo AOL bag files, BMP, EMF, GIF, JPEG, LINK, PDF, PNG, HTML e documentos tipo Microsoft Office (OLE). Backup e restauração de casos. Conceitos de hash; banco de dados tipo KFF. Utilização do KFF no FTK. Conceitos de FuzzyHash e sua utilização no FTK. Exportando arquivos e suas propriedades. Produção de relatório e suas configurações. Exportando lista de palavras. Introdução ao Registry Viewer, buscas no registro, chaves pré-configuradas e relatório do registro. Introdução ao PRTK. Utilizando dicionários próprios no PRTK.

ANÁLISE DE MÍDIAS UTILIZANDO SOFTWARE LIVRE
Apresentação e Introdução. Objetivos. Revisão dos conceitos básicos de análise forense em mídias: questões práticas e objetivas. Escolha do ambiente de análise. Montagem de um kit pericial de ferramentas gratuitas: alternativas e vantagens/desvantagens. Ferramentas gratuitas para duplicação (imagem e/ou espelhamento). Ferramentas gratuitas para extração, incluindo Data Carving. Ferramentas gratuitas para análise/exames. “The Sleuth Kit” e “The Autopsy Forensic Browser”: uso e principais características/funcionalidades. Ferramentas gratuitas de Virtualização. Quebra de Senhas: opções gratuitas. Sistemas operacionais forenses: C.A.I.N.E., Helix e suas ferramentas integradas. Ferramentas gratuitas para uso em mídias “Live”. Exercícios práticos: simulação de casos reais. Outras ferramentas livres e gratuitas para ambientes Windows e Linux. Dicas práticas e apresentação de casos reais sobre a análise de mídias.

PRÁTICA EM ANÁLISE FORENSE I
Apresentação e discussão do cenário do caso prático que será abordado no módulo. O tipo de caso será definido de acordo com o perfil da turma, podendo ser um caso de pornografia infanto-juvenil, análise de sistema computacional, análise de invasão de sistema, entre outros. Discussão sobre aspectos técnico-jurídicos relacionados ao caso. Discussão e definição da metodologia de análise a ser utilizada. Apresentação de estudo de caso real onde a metodologia de análise foi aplicada, destacando as ferramentas empregadas e as evidências encontradas. Análise forense prática das evidências relacionadas ao caso, utilizando ferramentas livres (já abordadas no curso), buscando artefatos e provas que irão subsidiar as conclusões periciais. Apresentação e discussão do relatório/laudo final, destacando sua construção, formatação e forma de apresentação das evidências digitais.

PRÁTICA EM ANÁLISE FORENSE II
Apresentação e solução do *forensic challenge* proposto no módulo PRÁTICA EM ANÁLISE FORENSE I. Apresentação e discussão do cenário do caso prático que será abordado no módulo. O tipo de caso, definido de acordo com o perfil da turma, será diferente daquele abordado no módulo PRÁTICA EM ANÁLISE

FORENSE I, podendo ser um caso de pornografia infanto-juvenil, análise de sistema computacional, análise de invasão de sistema, entre outros. Discussão sobre aspectos técnico-jurídicos relacionados ao caso. Discussão e definição da metodologia de análise a ser utilizada. Apresentação de estudo de caso real onde a metodologia de análise foi aplicada, destacando as ferramentas empregadas e as evidências encontradas. Análise forense prática das evidências relacionadas ao caso, utilizando ferramentas livres (já abordadas no curso), buscando artefatos e provas que irão subsidiar as conclusões periciais. Apresentação e discussão do relatório/laudo final, destacando sua construção, formatação e forma de apresentação das evidências digitais.

ANÁLISE DE LOCAL NA REDE MUNDIAL

Origem da Internet e dos crimes cibernéticos, principais crimes cibernéticos, alguns ataques cibernéticos, investigações cibernéticas, ataques nas três ondas da automação bancária, locais mais vulneráveis na rede mundial, locais de crimes cibernéticos.

ANÁLISE DE TRÁFEGO E CAPTURA DE PACOTES

Usos de redes de computadores - Aplicações comerciais, domésticas e usuários móveis. Hardware de rede: Redes locais, metropolitanas, geograficamente distribuídas, sem fio, domésticas e Inter-redes. Software de rede: Hierarquias de protocolos; Serviços orientados a conexões e serviços sem conexões, primitivas de serviço, relacionamento entre serviços e protocolos. Modelos de referência: Modelo OSI, Modelo TCP/IP. Exemplo de redes: A internet, Ethernet, LANs sem fio: 802.11. A camada física: A camada de Enlace de Dados. A subcamada de controle de acesso ao meio; A camada de rede - A camada de transporte; A camada de aplicação. Assinaturas digitais: Assinaturas de chave simétrica assinaturas de chave pública, sumário de mensagens. Segurança do correio eletrônico: PGP, PEM, S/MIME. Segurança na WEB: Ameaças, SSL, Segurança do código móvel. Gerenciamento de chaves públicas: Certificados, X.509, Infra Estrutura de chave pública. Segurança da comunicação: IPSec, Firewalls, Redes privadas virtuais, Segurança sem fio. LIBPCAP e WinPCAP: História do desenvolvimento e aplicações práticas; Análise - Wireshark .TCPDump /WinDump: Captura de pacotes para Linux/Unix e Windows; Captura de pacotes e geração de logs usando Snort NIDS; Captura de tráfego - Camada 2: Captura e análise de pacotes UDP (User Datagram Protocol). Características UDP; Tráfego NTP/DNS. Captura - Análise do TCP (Transmission Control Protocol). Serviços orientados a conexão; Regras de conexão - Criação de sockets; Filtragem do tráfego TCP; Remontagem de stream TCP; Diferenciando fluxos de Cliente e Servidor. Capturas baseadas em texto: Tetheral. Recursos e aplicações; Capturando tráfego TCP e UDP. Intranet: Captura de tráfego. Características e limitações do monitoramento; Analise da topologia da rede; Tráfego Unicast/Multicast/Broadcast; Switch Port Mirroring: SPAN. Internet: Captura de Tráfego, Características e limitações do monitoramento; Interfaces externas chaves para monitorar; Espelhamento de porta para captura; Capturando tráfego externo. Captura de tráfego baseado em WIRELESS; Características e limitações do monitoramento; Detecção de redes e hosts; Ferramentas de captura para LINUX/Windows; WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) e WPA-2; Quebra da criptografia WEP. Outros Tópicos. Características comuns do tráfego gerado por programas peer-to-peer (p2p); Netflow/IPFIX; Análise quantitativa e qualitativa do tráfego de rede utilizando a ferramenta NTOP; Captura e extração on-the-fly de arquivos.

CRIPTOGRAFIA E CRIPTOANÁLISE
Introdução à Criptografia. Objetivos Gerais. Principais Conceitos. Tipos de Ataques. História da Criptografia Simétrica (das cifras clássicas às modernas). Cifras Simétricas Modernas. Métodos de Criptografar a Informação (Fluxo e Bloco). Modos de Ciframento. Confusão, Difusão, Efeitos Avalanche e de Completeza. Visão geral da cifra RSA e ElGamal (e variantes). Funções Hash. Assinatura Digital. Protocolos Criptográficos e Gerenciamento de Chaves. Implementações de Criptografia (Kerberos, Diffie-Hellman, PGP, SSL, IPSEC). Visão geral dos principais Algoritmos de Criptografia Principais Técnicas de Criptoanálise. Criptografia Quântica. Esteganografia.

INTRODUÇÃO AO PROCESSAMENTO FORENSE DE IMAGENS I
Introdução. Imagens, conceitos e definições. Dispositivos de aquisição de imagens digitais. Sistemas ópticos, sensores e conversão A/D. Principais formatos de imagens digitais. O formato JPEG. Processamento Forense de Imagens. Panorama sobre softwares e soluções para processamento forense de imagens. Instalação do software IMAGEJ (Open Source). Instalação e configuração de plugins destinados ao processamento forense de imagens. Melhoramento de imagens. Melhoramento X Restauração de Imagens. Métodos de melhoramento de imagens usando o IMAGEJ: Transformações Radiométricas. Equalização e especificação de histogramas. Equalização local de histogramas. Algoritmo CLAHE. Equalização local em cenário forense. Operadores aritméticos. Subtração de imagens. Frame Averaging. Sinais, sistemas e transformadas bidimensionais. Filtragem no domínio espacial e no domínio frequencial. Filtros passa-baixa, passa-alta, passa-faixa, rejeita-faixa e *notch*. Filtragem Homomórfica. Aplicações práticas. Melhoramentos de imagens exemplo.

INTRODUÇÃO AO PROCESSAMENTO FORENSE DE IMAGENS II
Revisão. Revisão dos conceitos básicos sobre imagens, processamento de imagens, melhoramento e restauração. Revisão sobre os conceitos básicos do software de apoio IMAGEJ. Restauração de Imagens. Modelos de degradação de imagens. Redução de ruído. Modelos de Ruído. Filtros de redução de ruído. Filtros de média. Filtros de estatística de ordem. Filtro de redução de ruído local adaptativo. Filtro Sigma. Filtro NLM. Filtros no domínio Frequencial. Aplicações práticas. Redução de ruído de imagens exemplo. Métodos de Deconvolução. Estimação de modelos de degradação. Filtro inverso. Filtro de Wiener. Filtro de mínimos quadrado com restrições. Filtros Iterativos. Aplicações práticas. Restauração de de imagens exemplo. Fotogrametria. Correção de perspectiva planar. Perspectiva cônica e razão cruzada. Aplicações práticas. Medidas em imagens exemplo. Tópicos em verificação de edição em imagens. Conceitos. Métodos perceptuais, contextuais e numéricos.

ANÁLISE DE EQUIPAMENTOS COMPUTACIONAIS PORTÁTEIS E DE TELEFONIA MÓVEL
Apresentação e Introdução. Objetivos. Definições de Equipamentos Computacionais Portáteis. Conceitos básicos de Telefonia Móvel: as ERBs e tipos. Global System for Mobile Communications (rede GSM). Cartões SIM: características e tipos. Metodologia para análise em dispositivos móveis. Identificação e preservação de dispositivos móveis. Tipos de extração de dados nesses dispositivos: extrações manual, lógica, de sistema de arquivos, física e avançada (chip-off). Uso de cabos de dados, bluetooth e infravermelho. Análise de dados. Ferramentas forenses comerciais e gratuitas. Principais características dos sistemas operacionais móveis: Android, iOS, Windows Phone e Blackberry

OS. Dispositivos bloqueados: alternativas para acesso. Root, ClockWorkMod, JailBreak e quebra de senhas. Tablets e iPads. Exercícios práticos em laboratório, com a simulação de casos reais. Dicas práticas e apresentação de casos reais solucionados sobre exames em equipamentos computacionais portáteis. O futuro dos Smartphones.

TÓPICOS AVANÇADOS EM COMPUTAÇÃO FORENSE
Tópicos em Informática Forense: Engenharia Reversa. Introdução à Engenharia Reversa. Fundamentos de Sistemas Operacionais. Fundamentos de Arquivos Binários (Plataforma Windows). Fundamentos de Assembly. Ferramentas de Engenharia Reversa. Montando Laboratório para análise de binários. Práticas: Patching, Keygening, Unpacking.

*As ementas poderão ser ajustadas conforme demandas de mercado, novas legislações, novos cenários e contextos.

COORDENAÇÃO

JOSÉ WALBER BORGES PINHEIRO (idealizador)
Bacharel em Ciências da Computação pela Universidade Federal de Goiás; Especialista em Docência Universitária; Mestre em Educação (PUC-GO); Doutorando em Ciências da Informação (UFP-Portugal), Perito Criminal Federal Classe Especial; Ex-chefe do Setor Técnico Científico da Polícia Federal em Goiás; Professor da Universidade Estácio de Sá (Graduação e Pós-Graduação). Professor da Academia Nacional de Polícia e Professor IPOG.

CORPO DOCENTE

PAULO QUINTILIANO DA SILVA
Perito Criminal Federal da Polícia Federal, tendo sido Chefe da Perícia de Informática por 4 anos. É graduado em Ciência da Computação e em Direito, é Mestre em Ciência da Computação, é Doutor e Pós-Doutor em Processamento de Imagens e Reconhecimento de Padrões. Trabalha na área de Ciência da Computação desde 1982, em alguns órgãos públicos federais, com atuação em Segurança da Informação. Em 2005 foi eleito o Conselheiro representante da América Latina no “International Botnet Task Force Counsel”. É o fundador e o Editor-Chefe da revista científica IJoFCS (The International Journal of Forensic Computer Science). É o fundador e o Coordenador das conferências internacionais: ICCyber (Conferência Internacional de Perícias em Crimes Cibernéticos) e ICoFCS (The International Conference on Forensic Computer Science). É o fundador e foi o primeiro Presidente do Capítulo Brasília da HTCIA (High Technology Crime Investigation Association). É o fundador e o Presidente da ABEAT (Associação Brasileira de Especialistas em Alta Tecnologia). É Conselheiro do KINSA Law

Enforcement Advisory Board. É Pesquisador Associado da Universidade de Brasília (UnB).

HELVIO PEREIRA PEIXOTO
Bacharel em Ciência da Computação pela Universidade Federal de Uberlândia (UFU) e Mestre em Ciência da Computação pela Universidade Estadual de Campinas (Unicamp). PhD em Engenharia Elétrica e Computação pela Univesity of Texas at Austin (UTAustin, USA). Ministrou aulas de Programação Orientada a Objetos em C++ na UTAustin e foi Diretor do curso de Engenharia de Computação na Universidade de Uberaba. Foi Gerente de Projetos por três anos no Logic Technology Development Group da Intel Corp - USA. Atualmente exerce o cargo de Perito Criminal Federal em Brasília. Idealizador e responsável pela implantação do Mestrado Profissionalizante em Engenharia Elétrica com Ênfase em Informática Forense e Segurança da Informação pela Universidade de Brasília, UNB. É certificado em Computação Forense pela AccessData (ACE - Accessdata Certified Examiner), Guidance Software (EnCE – Encase Certified Examiner) e IACIS (International Association of Computer Investigative Specialists).

MARCELO ABDALLA DOS REIS
Bacharel em Ciência da Computação pela UFMS e Mestre em Ciência da Computação pela UNICAMP, na área de Segurança de Redes. Perito Criminal Federal “Primeira Classe”, Área de Informática. EnCase Certified Examiner (EnCE) e AccessData Certified Examiner (ACE). Autor de artigos, palestras e cursos ministrados em eventos nacionais e internacionais.

LUCIANO KUPPENS
Perito Criminal Federal desde 2005, com graduação em Engenharia de
Redes de Comunicação pela Universidade de Brasília (2003), graduação em Tecnologia em Processamento de Dados pelo Centro de Ensino Superior Unificado de Brasília (2001), especialização em Gestão em Redes e Segurança da Informação pela União Pioneira de Integração Social (2004), especialização em Criptografia pela Universidade Federal Fluminense (2010) e mestrado em Engenharia Elétrica, área de concentração em Informática Forense e Segurança da Informação, pela Universidade de Brasília (2012). Encontra-se lotado no Serviço de Perícias em Informática do Instituto Nacional de Criminalística do Departamento de Polícia Federal, sendo responsável pelo Laboratório de Decifragem de Arquivos. Atua também como Professor na Academia Nacional de Polícia (ANP), nas disciplinas Informática Forense e Noções de Criminalística. Coautor dos Procedimentos Operacionais Padrão em Informática Forense da Secretaria Nacional de Segurança Pública (SENASP).

JOSÉ HELANO MATOS NOGUEIRA
Doutor em Administração de Empresas pela Universidade de Liverpool, Inglaterra. Possui mestrado *stricto sensu* em Informática pela PUC/RJ e diversos cursos de pós-graduação lato sensu, destacando MBA em Ciências Forenses pela Universidade da Flórida (EUA) e MBA em Gestão de Políticas de Segurança Pública pela Academia Nacional da Polícia Federal. Possui bacharelado em Ciência da Computação e Licenciatura Plena em Matemática pela UECE. Foi Pesquisador de Desenvolvimento Científico Regional do CNPq, onde iniciou sua brilhante carreira no meio científico nacional. Atualmente leciona na Faculdade Farias Brito e já lecionou em diversas universidades e instituições de nível superior do Brasil, dentre elas UFC/CE, UECE/CE, FURG/RS, PUC/RJ, ANP/DPF/DF, dentre outras. Orientou uma gama de alunos nas mais diversas linhas de pesquisa

da Administração (Sistema de Informação, Liderança e Gestão Estratégica), Computação (Inteligência Artificial, Segurança da Informação e Engenharia de Software), Direito (Criminalística e Processo Eletrônico). Já publicou dezenas de trabalhos científicos em livros, revistas, congressos e simpósios, tendo sido premiado em âmbito nacional e internacional, com vários de seus trabalhos. No campo profissional teve notoriedade em sua atuação em diversas áreas. No campo da gestão pública, foi o primeiro Policial brasileiro a ser Diretor da INTERPOL ocupando a posição de Diretor Mundial da Perícia Policial da INTERPOL, na sede em Lyon, França; foi o Coordenador de Cooperação Policial Internacional para Copa do Mundo FIFA; foi Assistente do Diretor da Polícia Científica da Polícia Federal; foi Chefe do Grupo de Bombas e Explosivos da Policia Federal. Atualmente, é o Chefe da Perícia Criminal da Policia Federal no Estado do Ceará.

PEDRO MONTEIRO DA SILVA ELEUTERIO
Graduado em Engenharia de Computação pela Universidade Federal de São Carlos (UFSCar) e Mestre em Computação, área de Hipermídia, pela Universidade de São Paulo (USP). Desde 2006, é Perito Criminal Federal da área de Informática, do Departamento de Polícia Federal, onde trabalha diariamente solucionando os mais variados crimes cometidos com o uso do computador. No início de 2011, lançou o livro “Desvendando a Computação Forense”, pela Novatec Editora, uma das primeiras obras nacionais na área de Computação Forense.

BRENO RANGEL
Engenheiro de Computação pela Universidade Federal de Goiás (UFG). Especialista em Docência Superior pela FacLions. Experiência profissional: Gestor de TI - Estado de Goiás, Perito Criminal Federal da Área de Informática em Goiás.

GALILEU BATISTA DE SOUSA
Graduado em Ciência da Computação pela Universidade Federal do Ceará e Mestre em Computação pela Universidade de Campinas (Unicamp). Foi Professor de várias instituições e universidades, incluindo Universidade Federal do Ceará, Universidade Católica de Pernambuco e Universidade Federal do Rio Grande do Norte. Desde 2005 é Perito Criminal Federal, trabalhando atualmente na Superintendência da Polícia Federal no Estado do Rio Grande do Norte. Ganhou vários prêmios por publicações relacionadas à Computação Forense.

RODRIGO ALBERNAZ
Bacharel em Engenharia Elétrica (ênfase em sistemas de computação) pela Universidade Federal de Goiás (UFG) e Tecnólogo em Redes de Comunicação (ênfase em Telecomunicação) pelo Centro Federal de Educação Tecnológica de Goiás (CEFET/GO). Perito Criminal Federal com experiência em exames na área de informática, tendo atuado em Tocantins e Goiás. Especialista em Criptografia e Segurança da Informação pela Universidade Federal Fluminense (UFF) e Mestre Profissionalizante em Engenharia Elétrica com Ênfase em Informática Forense e Segurança da Informação pela Universidade de Brasília (UNB). Coautor de dois capítulos do livro “Fundamentos de Redes - Passo a passo”, 1ª edição, Editora Terra, 2003.

SIBELIUS LELLIS VIEIRA
Graduação em Física (UFG), Mestrado e Doutorado na Unicamp (Instrumentação e Engenharia Elétrica [Automação], respectivamente) e Pós-doutorado em Ciência da Computação na Universidade da Virginia (EUA). Graduação em Direito na PUC

Goiás. Professor Titular da PUC Goiás do Departamento de Computação, Professor do Mestrado em Engenharia de Produção e Sistemas da PUC Goiás e Perito Criminal da Polícia Técnico-Científica do Estado de Goiás.

ALEXANDRE MOREIRA VAZ
Técnico em Telecomunicações, Bacharel em Ciências da Computação. Especialista em Docência Universitária; Ex-Instrutor do SENAC-GO. Ex-Instrutor de Microsoft Solution Providers. Ex-Policial Rodoviário Federal. Perito Criminal Federal. Professor convidado da Universidade Federal de Goiás. Instrutor da Academia Nacional de Polícia (ANP).

PAULO MAX GIL INNOCENCIO REIS
Perito Criminal Federal, lotado no Serviço de Perícias em Audiovisuais e Eletrônicos do Instituto Nacional de Criminalística (INC) do Departamento de Polícia Federal (DPF). Graduou-se em Engenharia de Comunicações pelo Instituto Militar de Engenharia (IME) em 1998. Pós-graduado, possui MBA Executivo em Telecomunicações, pelo Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET/RJ, 2003), e Aperfeiçoamento em Conhecimentos Militares pela Escola de Aperfeiçoamento de Oficiais (ESAO/RJ, 2005). Atuou na área de Sistemas de Telecomunicações por 4 anos (2001-2004), Gerenciando as Redes Corporativas de Voz e Dados da Presidência da República e do Exército Brasileiro. Tem experiência em Sistemas de Comunicações Digitais, Processamento Digital de Sinais e Processamento Digital de Imagens, atuando em projetos de pesquisa no Instituto Militar de Engenharia (2005-2006) e, como Perito Criminal Federal, na análise de registros de áudio e imagens (desde 2006). Professor dos cursos de Processamento Forense de Imagens, Reconhecimento Facial, Introdução às Perícias em Registros de Áudio, e Investigação e Busca de Aparatos de interceptação, todos da Academia Nacional de Polícia (ANP). Professor do curso preparatório para o concurso de Perito Criminal Federal da rede de ensino LFG (2010 - 2012). Tem interesse em problemas relacionados à Análise Forense de Sistemas de Telecomunicações, Análise Forense de Imagens, Análise Forense de Registros de Áudio, Biometria Facial, Reconhecimento de Locutor, Reconhecimento de Padrões, Processamento Digital de Sinais e Processamento Digital de Imagens.

* Professores titulares. Sujeitos a alterações.

DOCUMENTAÇÃO NECESSÁRIA

• Diploma de graduação original.
• Cópia do RG e CPF / ID Profissional / CNH.

MATERIAL PARA ESTUDO

É imprescindível que o estudante disponha de um notebook próprio para utilização durante as aulas, com no mínimo 8GB de memória RAM.

DURAÇÃO / PERIODICIDADE

18 meses (um final de semana por mês).

- Sexta, das 18h às 23h.
- Sábado, das 8h às 19h.
- Domingo, das 8h às 13h.

IPOG INSTITUTO DE PÓS-GRADUAÇÃO & GRADUAÇÃO

ipog.edu.br