



O que é Forense Computacional?

É a ciência que estuda a aquisição, preservação, recuperação e análise de dados armazenados em mídias computadorizadas e procura caracterizar crimes de informática de acordo com as evidências digitais encontradas no sistema invadido. A Forense Computacional é uma área de especialização relativamente nova no mundo e está desenvolvendo-se principalmente pela necessidade das instituições legais atuarem no combate aos crimes eletrônicos. É notório e as estatísticas reveladas através das pesquisas mostram o aumento expressivo das fraudes eletrônicas, sendo que a perícia forense se mostra uma eficiente ferramenta para identificação e redução desses riscos.

As ações com base na prática de forense computacional são uma técnica científica, aplicada dentro de um processo legal que busca evidências e responsabilização de envolvidos em incidentes que usem os meios computacionais para execução de crimes ou burlar regras estabelecidas. A coleta adequada dessas evidências e o reconhecimento das autoridades legais é um desafio para os profissionais envolvidos.

Com a expansão da Internet em escala global, a eliminação de fronteiras gerou um grande problema para as instituições de combate ao crime, uma vez que possibilitou em muito a ocorrência de crimes eletrônicos onde a vítima e o criminoso estão em lugares distintos, incluindo ai até países distintos, configurando-se em delitos transjurisdicionais.



Tornou-se assim necessário e praticamente obrigatório a troca de informações e evidências eletrônicas entre as agências. Todavia, por se tratar de uma necessidade muito recente, ainda não se conta com padrões internacionais para o tratamento desse tipo de evidência. Dessa forma o valor jurídico de uma prova eletrônica manipulada sem padrões devidamente pré-estabelecidos poderia ser contestável. Levando em consideração estas novas necessidades, os nossos profissionais especialistas desenvolveram e ministram também cursos de outros temas que tem convergência com Forense Computacional, por exemplo, a comparação entre as Leis que tratam de crimes eletrônicos de outros países, em comparação com a Legislação Brasileira.

De maneira geral os seminários, eventos e treinamentos disponíveis falam da descrição de crimes, fraudes eletrônicas e seus impactos, promovem apresentação e detalhamento de algumas ferramentas, tecnologias, técnicas e metodologias de computação forense, aspectos na legislação brasileira e internacional e casos de sucessos. Todavia poucos são os que transmitem uma verdadeira e objetiva experiência prática neste tema, com uma carga horária adequada aos que tem necessidade efetiva de conhecer e implementar esta metodologia rapidamente.

Daí o nosso Curso de Forense Computacional se propor a explicar e mostrar efetivamente estes aspectos de forma relacionada e na medida exata aos que procuram por em prática estas ações em suas empresas ou em suas consultorias.



Quais são os objetivos de nosso curso sobre Forense Computacional?

Este curso permite identificar os elementos necessários para reconstituição de incidentes em segurança da informação, permitindo no próprio *notebook* do aluno uma formação prática em laboratório. Capacitar, de forma plena, os alunos a executarem perícia forense computacional em mídias, aplicações e serviços de rede, gerando laudos periciais para uso em processos judiciais ou investigações privadas.

Desta maneira os participantes terão meios para ampliarem a visão na elaboração de um plano integrado que contempla segurança da informação como um dos elementos estratégicos da Gestão Corporativa, sob a ótica da Forense Computacional.

Para quem se destina?

Gestores, consultores e técnicos nas áreas de Segurança e Tecnologia da Informação, Auditoria, Sistemas e *Compliance*. Profissionais em geral com interesse em conhecer boas práticas em Forense Computacional.

Quais são os benefícios?

- Este curso sintetiza todos os conhecimentos e áreas de segurança da informação em seu aspecto voltado para a Forense Computacional em um único curso.
- Entender e reconhecer, em linhas gerais, como questões de gerenciamento de segurança afetam e são afetadas pela organização e aprofundar o seu conhecimento com o aprendizado adquirido, em outros cursos e certificações na área de segurança em geral.



- **Conhecer em detalhes os principais componentes da segurança da informação, em seu aspecto voltado para a Forense Computacional, e como eles se integram com o objetivo de manter a integridade, disponibilidade e confidencialidade de seu conteúdo.**
- **O aluno ao fim do curso estará apto a ampliar seus conhecimentos em áreas mais específicas em segurança da informação em seu aspecto voltado para a Forense Computacional, além de se aprimorar no mercado de segurança da informação no Brasil e exterior e aplicar os conceitos gerais, do ponto de vista teórico/prático, com a realidade do dia-a-dia nas empresas.**

Quais são as palavras-chave para índice sistemático em taxonomias ou TAG's nas quais podemos classificar este curso?

**Segurança
Forense
Direito / Tecnologia
Investigação
Crimes eletrônicos**

Quais são os módulos que o curso contempla?

- **Introdução e Conceitos;**
- **Procedimentos Investigativos e fonte das provas;**
- **Metodologia forense;**
- **Ferramentas e equipamentos forenses;**
- **Desenvolvimento da análise forense;**
- **Elaboração do laudo pericial.**



Quais são os detalhes do conteúdo programático que o curso contempla?

Introdução e Conceitos

- Antecedentes da forense computacional
- O que é e o que faz um perito e perito forense informático
- O que é forense e forense computacional e onde se aplicam
- O que é ciência forense
- O que é e como são as evidências e evidências digitais
- Requisitos de uma evidência
- O que é investigação forense
- O que é prova pericial
- O que é investigação computacional
- O que é cadeia de custódia
- Fonte de evidências e provas (Meios / Imagem / Evidência Volátil)
- O que é e como se comportar em uma cena de um crime

Procedimentos Investigativos e fonte das provas

- Como se preservar as evidências e suas respectivas provas
- Ordem de preservação de evidências
- Erros em procedimentos investigativos
- Requisitos investigativos
- Princípios e processos forenses
- Forense em sistemas operacionais e sistemas de arquivos
- Forense em resposta a incidentes

Metodologia forense

- Investigação em pessoas e testemunhos
- Investigação no local do crime
- Investigação das evidências e provas
- Enfoques da investigação
- Como se concluir uma investigação
- Cuidados na recepção da evidência
- Integridade de evidências e provas
- Geração de HASH
- Geração de imagens
- Coleta de evidências em ambientes "vivos" e sistemas estáticos
- Procedimentos para Cadeia de custódia
- Análise de dados
- Palavras chave
- Linha de tempo
- Recuperação de dados
- Evasão forense (criptografia, destruição física e esteganografia)

Ferramentas e equipamentos forenses

- Soluções em software e hardware gratuitas e comerciais são apresentadas em sala de aula, incluindo Helix, ferramentas Sysinternals, Winhex entre outros.
- Referências e documentos disponíveis de forense computacional que apóiam o processo investigativo.



Desenvolvimento da análise forense

É apresentado um caso, onde evidências são oferecidas para execução de uma análise forense com as ferramentas disponíveis em sala de aula.

Elaboração do laudo pericial

Importância do laudo pericial
Cuidados na preparação do laudo
Itens de um laudo pericial