UGB
Centro Universitário Geraldo Di Biase

PROJETO DE REDES
www.projetoderedes.com.br

Auditoria e Análise de Segurança da Informação

Forense Computacional

Prof. José Maurício S. Pinheiro - UGB - 2009

Forense Computacional

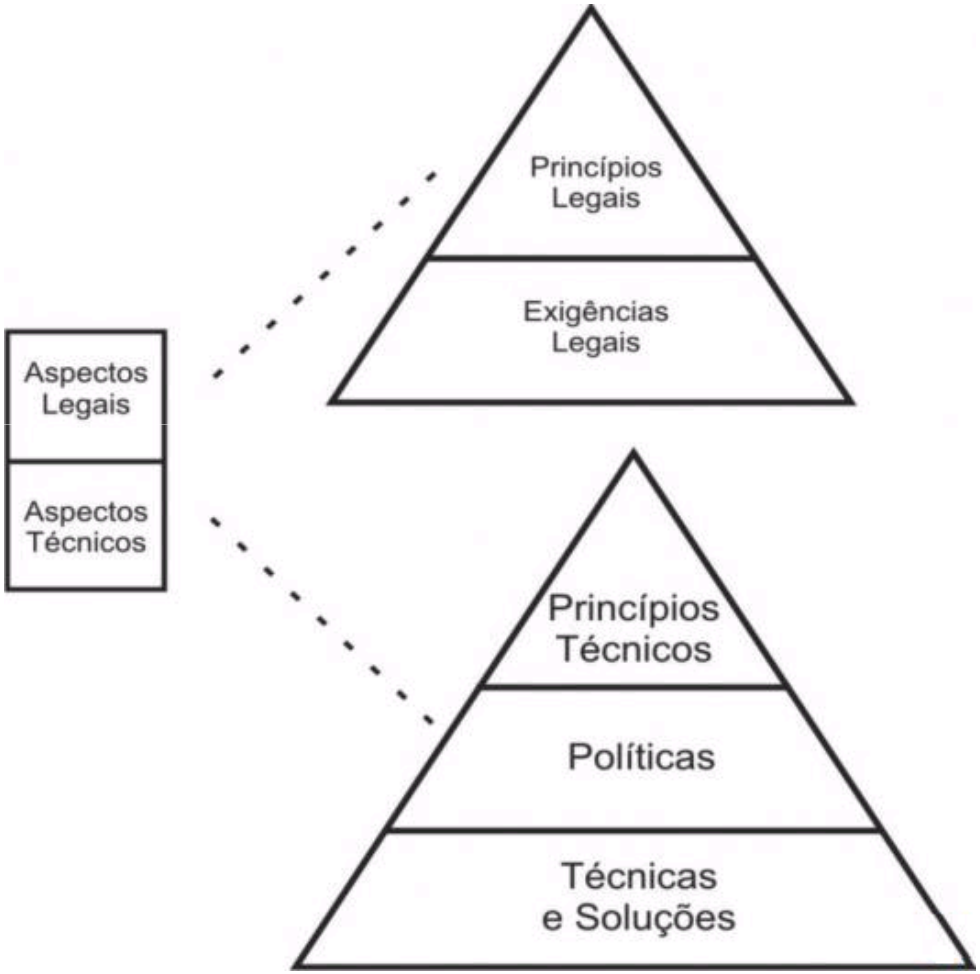
Forense Computacional

A forense computacional pode ser definida como a ciência de adquirir, preservar, recuperar e exibir dados que foram eletronicamente processados e armazenados digitalmente.

Visa, principalmente, vistoriar e analisar todos os componentes físicos e os dados que foram processados eletronicamente e armazenados em mídias computacionais.

Forense Computacional

Um modelo propõe uma estrutura hierárquica de duas classes multiníveis: (Aspectos Legais e Aspectos Técnicos).



Metodologia Forense

Os padrões metodológicos seguem o princípio de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiabilidade e a precisão das evidências.

Esse nível de qualidade pode ser atingido através da elaboração de SOP's (*Standard Operating Procedures*), que devem conter os procedimentos para todo tipo de análise conhecida e prever a utilização de técnicas aceitas na comunidade científica internacional.

Metodologia Forense

O investigador precisa estar perfeitamente sintonizado com os objetivos de cada uma das etapas da metodologia apresentadas a seguir, para poder minimizar o tempo e a quantidade de dados que deve obter, maximizando sua eficiência e eficácia.

Metodologia Forense

Obtenção e Coleta de Dados:

- Os procedimentos adotados na coleta de dados devem ser formais, seguindo toda uma metodologia e padrões de como se obter provas para apresentação judicial, como um checkList, de acordo com as normas internacionais de padronização.

Metodologia Forense

Identificação:

- Dentre os vários fatores envolvidos no caso, é extremamente necessário saber separar os fatos dos fatores, que possam vir a influenciar ou não um crime, para estabelecer uma correlação na qual se faz um levantamento das ligações relevantes como datas, nomes de pessoas, autarquias, etc., dentre as quais foi estabelecida a comunicação eletrônica.

Metodologia Forense

Preservação:

- Um Perito Forense Computacional experiente deve ter certeza de que uma evidência extraída será adequadamente manuseada e protegida para se assegurar de que nenhuma evidência seja danificada, destruída ou mesmo comprometida pelos maus procedimentos usados na investigação e que nenhum vírus ou código malicioso seja introduzido em um computador durante a análise forense.

Metodologia Forense

Análise:

- A análise será a pesquisa propriamente dita, onde o investigador se detém especificamente nos elementos relevantes ao caso em questão pois todos os filtros de camadas de informação anteriores já foram transpostos.

Metodologia Forense

Apresentação:

- Ou "substanciação da evidência", pois ocorre o enquadramento das evidências dentro do formato jurídico, sendo inseridas, pelo juiz ou pelos advogados, na esfera civil ou criminal ou mesmo em ambas. Quando se tem a certeza material das evidências, atua-se em conjunto com uma das partes descritas para a apresentação das mesmas.

Metodologia Forense

Além da correta documentação, pode-se citar mais alguns princípios das demais disciplinas forenses, herdados pelo meio computacional, para os procedimentos de perícia forense:

- **Réplicas:** efetuar as análises sobre cópias das evidências originais, evitando-se que um erro do examinador venha a comprometer as informações, inviabilizando a realização de um novo exame para a validação dos resultados alcançados;

Metodologia Forense

- **Garantia de Integridade:** existência de procedimentos que visem garantir a integridade das evidências coletadas. A autenticidade e a integridade da evidência podem ser verificadas através da utilização de algoritmos de *hash* criptográfico como o MD5, SHA-1 e o SHA-2. Além disso, é possível armazená-las em mídias para somente leitura, como CD-ROM;

- **Ferramentas Confiáveis:** não há como garantir a confiabilidade dos resultados obtidos durante uma análise se os programas utilizados não forem comprovadamente idôneos.

Obrigado!