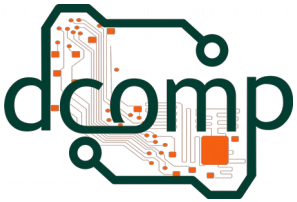
Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCA UFES
Departamento de Computação



Introdução à Computação Forense

Computação Forense
Site: http://jeiks.net
E-mail: jacsonrcsilva@gmail.com

Tópicos

- Introdução:
  - Princípios básicos;
  - História Resumida da Computação Forense.

Computação Forense

- A Computação Forense está envolvida com a obtenção e análise de informação digital para utilizá-la como evidência em um caso civil, criminal ou administrativo.

- Várias são as questões sobre os dados e sobre a quem pertence seu direito de acesso e utilização.

Passos de uma investigação

- Tipicamente, a investigação em dispositivos computacionais inclui:

  1. coletar de forma segura os dados de um computador;
  2. examinar dados suspeitos para determinar detalhes, como a origem e o seu conteúdo.
  3. apresentar as informações obtidas dos dispositivos computacionais para os tribunais.
  4. aplicar as leis quanto a utilização do dispositivo computacional.

Investigação Digital

- A investigação forense investiga dados que podem ser recuperados de um disco rígido de um computador ou de outros meios de armazenamento.
- O trabalho de um perito forense é como de um arqueólogo escavando um local.
  - O perito busca recuperar informações escondidas, perdidas, obsturas de um computador ou de seus componentes.
- Sobre a informação buscada:
  - pode não ser fácil de encontrar ou de decifrar;
  - às vezes deve-se apresentar qual foi a forma que o autor (réu) conseguiu acesso ou utilizou os dados pesquisados.

Diversos tipos de análises

- Além disso, alguns tipos de análise forense, como o de Redes de Computadores, trabalham na busca de informações em *logs* do sistema e em arquivos novos ou modificados deixados para trás no computador da vítima.

Forense e Recuperação de Dados

A computação forense é **diferente** de recuperação de dados

- Ambos envolvem a recuperação de informações de um computador que foi excluída.
- Porém, em recuperação de dados você sabe o que está procurando;
- Mas em computação forense você pesquisa por dados que os utilizadores esconderam ou eliminaram para não serem encontrados.
  - Além disso, você deve assegurar que os dados recuperados serão válidos de modo que possam ser utilizados como prova de um caso judicial.

Evidências

- Os dados que serão utilizados em tribunais são chamados de evidências.
- A evidência pode ser condenatória (incriminatória, em casos criminais) ou de defesa, que pode livrar o suspeito de uma acusação.
- Como deve ser realizada a busca:
  - Inicialmente, pesquisar os meios de armazenamento existentes;
  - Logo após, pesquisar as evidências existentes. Processo geralmente realizado com a utilização de *softwares*.
- Em casos mais extremos, até mesmo microscópios eletrônicos e outros equipamentos sofisticados podem ser utilizados para obter informações de máquinas danificadas ou formatadas de forma propositais.

Recuperação de desastres

- Empresas que trabalham com recuperação de desastres também utilizam técnicas de computação forense para resgatar informações perdidas.
- Essas empresas também tem outros meios de manter as informações, como:
  - prevenção de perda de dados utilizando backups;
  - dispositivos de fonte de alimentação ininterrupta; e
  - monitoramento *off-site*.

Investigar Informações

- A função de investigar informações faz parte de uma tríade que compõe a segurança da informação:
  1. Análise da vulnerabilidade e gerenciamento de risco;
  2. Detecção de intrusão de rede e resposta à incidentes;
  3. Investigações computacionais;
- Cada um dos itens dessa tríade:
  - É um grupo ou departamento responsável.
  - Onde cada um trabalha de uma forma, porém fornecendo e gerando informações para o outro durante uma investigação.

Litígio

- A pesquisa de informações de um perito pode resolver divergências entre duas partes.
- Nesse caso, o perito trabalhará em um Litígio.
  - processo de solicitar a um tribunal que decida uma disputa, ou seja, que estabeleça uma responsabilidade civil ou tribunal.
- Assim, o perito realizará uma análise forense dos sistemas suspeitos para obter provas relacionadas a um incidente ou a um crime e fornecerá esses dados ao tribunal.

Computação Forense

O que é Computação Forense?

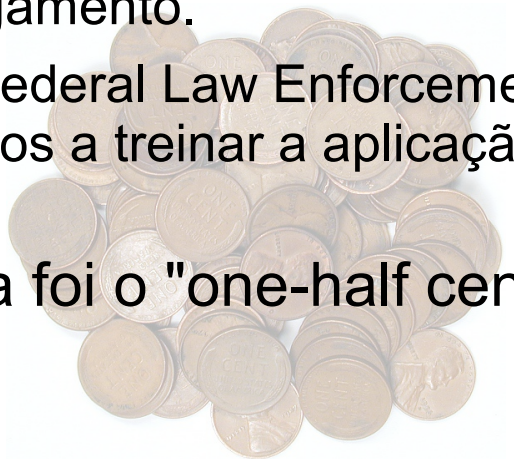
Computação Forense

Uma das definições:

A arte de resgatar evidências de uma mídia de armazenamento para resolver litígios de forma lícita e incontestável, com comprovação científica dos fatos apresentados.

História da Computação Forense

- Em 1970:
  - os crimes eletrônicos aumentaram, principalmente no setor financial.
  - a maioria dos computadores era mainframe, utilizados por pessoas treinadas para trabalhar em financias, engenharia e academia.
  - nessa época, os policiais:
    - não conheciam computadores; e
    - não sabiam realizar as perguntas corretas para descobrir o crime, ou para preservar as provas para o julgamento.
    - Muitos começaram a participar do Federal Law Enforcement Training Center (FLETC), que eram destinados a treinar a aplicação da lei na recuperação de dados digitais.
  - o crime mais conhecido nessa era foi o "one-half cent crime".



História da Computação Forense

- Em 1980:
  - os Computadores Pessoais começaram a ter popularidade e vários sistemas operacionais apareceram:
    - Apple 2E em 1983 e o Macintosh em 1984, pela Apple.
    - E depois surgiram Sistemas Operacionais de Disco (DOS), incluindo PC-DOS, QDOS, DR-DOS, IBM-DOS e MS-DOS.
  - Nessa época, as ferramentas forenses eram:
    - simples. *Por quê??*
    - criadas pelas agencias governamentais:
      - Royal Canadian Mounted Police – RCMP
      - U.S. Internal Revenue Service – IRS
    - mas não eram fornecidas ao público.

História da Computação Forense

- no meio de 1980:
  - surgiu no mercado o Xtree Gold, que:
    - reconhecia tipos de arquivos,
    - recuperava arquivos perdidos ou apagados; e
    - permitia ver o código de um binário, convertendo seus bytes para ASCII.
  - apareceu então o Norton DiskEdit para recuperar arquivos.
  - Obs.: os HDs possuíam tamanho de 10MB;
- Em 1987, a Apple produziu o Mac SE, que era um Macintosh com um disco rígido externo de 60MB.

História da Computação Forense

- No início de 1990:
  - ferramentas especializadas para computação forense foram disponibilizadas.
  - a International *Association of Computer Investigative Specialists* (IACIS) iniciou o treinamento sobre softwares de investigações forenses e o IRS criou programas de pesquisa de produtos sob garantia de licença.
  - Surgiu o primeiro software não comercial com modo gráfico:
    - o ASR Data criado para peritos para Macintosh.
  - Até que um dos patrocinadores saiu do projeto e criou o EnCase, que tornou-se a ferramenta forense mais popular da época.

História da Computação Forense

- Após isso, os softwares, as tecnologias e as capacidades de disco rígidos cresceram e tornaram-se mais numerosas e populares entre a população.
- Alguns softwares comuns nos dias de hoje são:
  - o ILook; e
  - o AccessData Forensic Toolkit (FTK).

Que tal por a mão na massa agora?

Exemplo de resgate de informações.