Perícia em informática: passado, presente e futuro

Ivo de Carvalho Peixinho
Perito Criminal Federal
Coordenação de TI - CTI
CTI/DLOG/DPF

Tópicos

- Perícia Criminal Federal
- Perícia em Informática
- Equipamentos e ferramentas
- Desafios atuais
- Visão do futuro e conclusões

Perícia Criminal Federal - PCF

- **Produção de laudos periciais através da Criminalística**
  - Evidências e questionamentos (IPL)
- **Divididos em diversas áreas**
  - Perícias Contábeis e Econômicas
  - Perícias de Engenharia e Meio Ambiente
  - Perícias de Laboratório
  - **Perícias em Informática**
  - Documentoscopia
  - Etc...

Perícia em Informática

- **Informática forense**
- **Produção de laudos periciais através da Criminalística**
- **Objetiva determinar a dinâmica, a materialidade e a autoria de ilícitos**
- **Identificar, processar e transformar evidências digitais em provas materiais de crimes através de métodos técnico-científicos, com a finalidade de conferir-lhes validade probatória em juízo**

Evidência Digital

- **Evidência: aquilo que indica, com probabilidade, a existência de (algo); indicação, indício, sinal, traço**
- **Qualquer informação com valor probatório armazenada ou transmitida no formato digital**
- **Exemplos de evidências relacionadas a locais de crimes cibernéticos (corpo de delito):**
  - **Mensagens de correio eletrônico e bate-papo**
  - **Imagens de pornografia infantil**
  - **Dados cifrados**
  - **Registros de impressão**
  - **Registros de conexão à Internet**
  - **Fragmentos de arquivos**

Organograma

- Direção-Geral
  - **Diretoria Técnico-Científica**
    - **Instituto Nacional de Criminalística**
      - **Serviço de Perícias em Informática**
    - Instituto Nacional de Identificação
  - 27 Superintendências Regionais
    - **27 Setores Técnico-Científicos + 05 Núcleos de Criminalística**

Escopo de Atuação

- **Perícias em mídias digitais**
  - HDôs, pendrives, cartões de memória, etc.
- **Perícias em máquinas caça-níqueis (MEP)**
- **Perícias em aparelhos celulares, PDA's e SmartPhones**
- **Perícias na Internet (local de crime)**

Atuação - Exames Periciais

Local de Crime: Coleta

Mandado Judicial

Apreensão

Duplicação Pericial

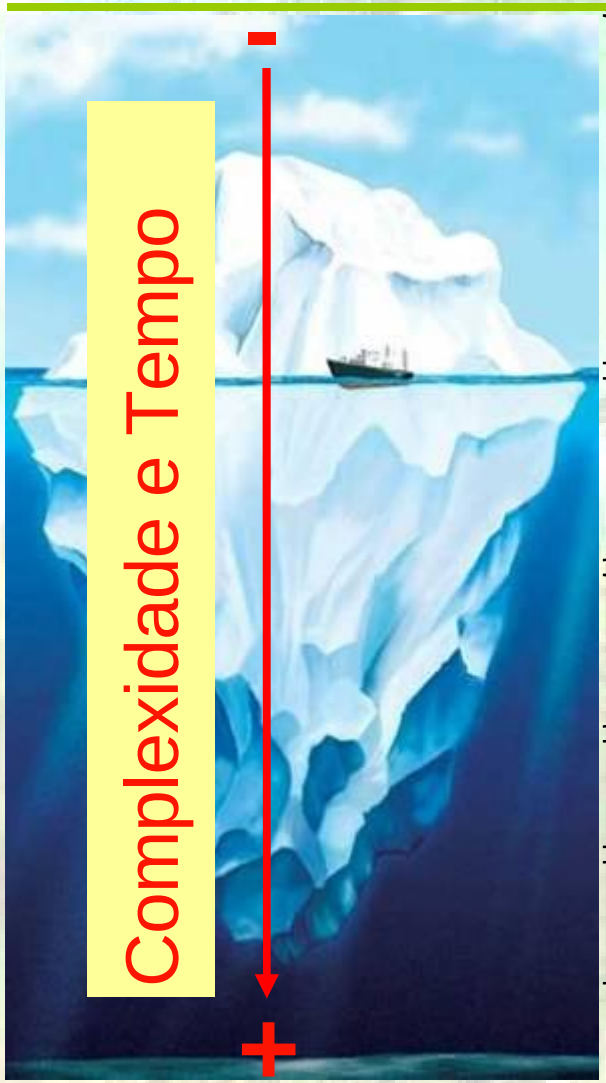
Análise (nas cópias)

- Mensagens de E-mail
- Documentos/imagens
- Registros de impressão
- Arquivos apagados; fragmentos
- Quebra de senhas
- Uso da Internet
- Engenharia reversa de programas
- Conversão de banco de dados

Documentação

Laudo

Análise de evidências digitais



Arquivos visíveis

Arquivos apagados

Sistemas/bancos de dados, registros de impressão, uso da Internet. etc

Arquivos ocultos / criptografados

Fragmentos de arquivo

... No passado

- **Pouca capacidade de armazenamento**
  - Ex: Disquetes, HDs de pequeno tamanho
  - Facilidade de duplicação
- **Poucos computadores ligados em rede**
- **Conhecimento em informática pouco disseminado**
  - Sistemas complexos de operar
- **Quantidade de computadores reduzida**
  - Sistemas centralizados

... Atualmente

- **Quase todos os crimes hoje em dia utilizam algum recurso computacional.**
- **Computadores ligados em rede**
  - ï Internet
- **Alta capacidade de armazenamento**
  - ï 80gb, 120gb, 1Tera!!
- **Conhecimento em informática bastante disseminado**
- **Inclusão digital**
- **Grande quantidade de computadores**
- **Organizações criminosas cibernéticas**
- **Novos dispositivos e tecnologias**
  - ï Iphones, criptografia forte, etc.

Projeto Promotec / Pro-Amazônia

- **Convênio de cooperação e financiamento entre o governo do Brasil e os governos da França-SOFREMI e da Alemanha**
- **Firmado em 12 de março de 1997**
- **Finalidade: modernização e reaparelhamento do DPF com fornecimento de equipamentos franceses e alemães**

Especificações

- **Final de 2005 – Divisão em 2 lotes**
- **1ª Fase:**
  - **Hardware/Software de uso individual dos peritos**
  - **Equipamentos com ampla disponibilidade comercial**
- **2ª Fase:**
  - **Soluções específicas p/ interceptação telemática, recuperação de mídias, quebra de senhas, S.A.R.D.**
  - **Equipamentos para novos peritos**

Hardware de Uso Individual

- **Estação de Trabalho Pericial + Notebook**

Notebook

Estação de Trabalho Pericial

20" Wide

20" Wide

KVM

No-Break

4GB

Hardware de Uso Individual

- **Duplicador de HDs**

HD IDE 500GB

HD SATA2 750GB

HD SATA2 320GB

INC

- **Leitor automático de CDs e DVDs**
- **Leitores externos**
  - ï Jazz, Fitas DAT e SDLT
- **Microcomputador Macintosh**
- **Rainbow Tables**
  - ï Tabelas para facilitar quebra de senhas
  - ï Projeto de armazenamento em storage da CTI
- **Compiladores**
  - ï C++ Builder, Delphi, etc.

Tecnologias desenvolvidas no DPF

- **Ferramenta Para Monitoramento de Redes P2P – EspiaMule**
- **Desenvolvido pelos PCF's Guilherme Martini Dalpian e Carlos Augusto Amelin Benites**

EspiaMule

- **Aplicativo eMule modificado a partir do código fonte, disponível na web**
- **Armazena IP, data e hora de todos os clientes compartilhando os arquivos baixados**
- **Bloqueio total de upload**
- **Forma de uso:**
  - Idêntico ao aplicativo eMule disponível na rede
  - Permite buscas nas redes Kad e eDonkey
  - Permite buscas por palavras-chave ou download a partir de links ED2K

EspiaMule

- **Processamento do log:**
  - Aplicativo em java
  - Identifica os usuários pelo país
  - Separa automaticamente usuários por provedor através de pesquisas WHOIS
  - Pode agrupar clientes com diversos arquivos a partir do hash de usuário ou IP
- **Utilizado na operação Carrossel (dez/2007)**

Tecnologias desenvolvidas no DPF

- **Colaboração entre os Peritos (geograficamente dispersos)**
  - Wiki
  - Lista de discussão
  - Jabber (Instant Messenger)
- **Laboratório de análise de *malware***
  - Curso ICCYBER 2007
- **Sistema criminalística**
  - Armazenamento de informações sobre laudos
- **KFF's (Known File Filters)**
- **Pesquisas sobre evidências em sistemas operacionais e dispositivos novos**

Capacitação e Treinamento

- **Iccyber (www.iccyber.org)**
  - Conferência Internacional de Perícias em Crimes Cibernéticos
  - Organizada pela perícia de informática
  - Oportunidade de troca de experiências com outras polícias e outros países
  - Possibilidade de realização no Brasil de treinamentos com instrutores internacionais (redução de custos)
  - Interação da perícia de informática com o público em geral

Operações

- CAVALO-DE-TRÓIA – Novembro/2003

Pará, Maranhão, Teresina e Ceará. 54 prisões

- CAVALO-DE-TRÓIA II – Outubro/2004

Pará, Maranhão, Tocantins e Ceará. 77 prisões

- MATRIX – Março/2005

Rio Grande do Sul 8 Prisões

- ANJO DA GUARDA I – Julho/2005

Buscas em 8 Estados Prisão em Volta Redonda-RJ,

- ANJO DA GUARDA II – Agosto /2005

cumprimento de prisões em PR, SP, MA

- PEGASUS - setembro/2005

127 Prisões em Goiás, Tocantins, Pará, ES, SP e MG;

Operações

- **GALÁCTICOS - agosto /06 - hacher**

cerca de 65 prisões
Imperatriz/MA

- **REPLICANTE – setembro/06 – hacker**

cerca de 60 prisões
Goiânia/GO

- **CTRL ALT DEL- dezembro/06 - hacker**

cerca 39 prisões no Pará

- **CARROSSEL - dezembro – 07 – ação contra a pedofilia**

cerca de 14 estados no BR e 78 países

  - Participação da perícia na fase de investigação
  - Utilização do EspiaMule para determinar os alvos

Desafios atuais

- **Aumento exponencial do volume de dados**
  - Material para análise
- **Popularização da criptografia**
  - Skype, Truecrypt, Microsoft Bitlocker
- **Rastreamento de crimes no *cyberespaço***
- **Organizações criminosas agindo na Internet**

Dificuldades - Rastreamento

Dificuldades

- **Omissões na legislação federal existente:**
  - ï Obrigações dos provedores e usuários
  - ï Retenção de *logs* de acesso e dados cadastrais
- **Regulamentação de funcionamento:**
  - ï Cyber-cafés
  - ï Salas de bate-papo
- **Cooperação internacional às vezes é lenta e ineficiente**

Visão de futuro

- **Aumento dos crimes cometidos usando computador**
  - Puros
  - Impuros
- **Novos dispositivos com maiores capacidades de armazenamento e menor tamanho**
  - Novos campos de informática forense
  - Facilidade de ocultação de dispositivos
- **Novas táticas dos criminosos**
  - Criptografia, obfuscação, etc.

Conclusões

- **Renovações e novas tecnologias a todo momento**
- **O perito em informática deve estar sempre informado e atento às mudanças**
- **Novas áreas de informática forense**
  - ï Bancos de dados, aparelhos embarcados, etc.
- **Cooperação entre as perícias e outras polícias pelo mundo**
- **Novas tecnologias no auxílio da perícia**
  - ï Mas não substituem o cérebro!!

Obrigado!

Ivo de Carvalho Peixinho