



*Forense
computacional
em Linux for
dummies*

*“uma rápida visão
introdutória”*

João Eriberto Mota Filho
João Pessoa, PB, 08 de maio de 2010

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ Conclusão

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ Conclusão

O que é forense computacional?

Forense computacional é a ciência voltada para a obtenção, preservação e documentação de evidências, a partir de dispositivos de armazenagem eletrônica digital, como computadores, pagers, PDAs, câmeras digitais, telefones celulares e vários outros dispositivos de armazenamento em memória. Tudo deverá ser feito para preservar o valor probatório das evidências e para assegurar que isto possa ser utilizado em procedimentos legais.

(An introduction to Computer Forensics, Information Security and Forensics Society, abr. 04, disponível em <http://www.isfs.org.hk/publications/public.htm>)

O que é forense computacional?

Então...

- ✓ A forense computacional busca, em dispositivos de armazenamento, evidências de ações incompatíveis, danosas ou criminosas.
- ✓ Tais ações podem ser locais ou remotas (via rede).
- ✓ Geralmente, as citadas ações estão relacionadas a roubo de informações, fraudes, pedofilia, defacements, intrusões e crimes cibernéticos em geral.

Sumário

- ✓ O que é forense computacional?
- ✓ **Ataques via rede: o que fazer?**
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ Conclusão

Ataques via rede: o que fazer?

- ✓ Em um razoável número de vezes, forenses são conduzidas em virtude de ataques remotos (via rede).
- ✓ Após um ataque remoto:
 - > Desconecte, imediatamente, o cabo de rede.
 - > NUNCA desligue a máquina (considerando que o atacante não o tenha feito remotamente).
 - > Não toque na máquina (nem mesmo faça login).
 - > Chame, imediatamente, um perito para realizar a forense.
 - > Acompanhe, se possível, todo o trabalho do perito.

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ **Medidas iniciais nas forenses**
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ Conclusão

Medidas iniciais nas forenses

Ao tomar o primeiro contato com a máquina atacada, caso a mesma ainda esteja ligada, o perito deverá:

- ✓ Inserir um pendrive maior do que a quantidade de RAM da máquina para colher dados (nunca gravar no HD atacado).
- ✓ Logar como root e montar o dispositivo USB (/mnt?).
- ✓ Gravar no dispositivo externo os seguintes dados:
 - > Um dump de memória, com # if=/dev/mem of=/mnt/mem. (esta tem que ser a primeira ação)
 - > A situação de memória, com # free -m > /mnt/free.
 - > Os processos ativos, com # ps aux > /mnt/ps.
 - > Os processos e portas ocultos, com # unhide > /mnt/unhide.

continua...

Medidas iniciais nas forenses

continuando...

- > O tempo de vida da máquina, com `# uptime > /mnt/uptime`.
- > As conexões e portas abertas, com `# netstat -tunap > /mnt/netstat`.
- > A relação de pacotes instalados (no Debian, pode-se usar `# COLUMNS=110 dpkg -l > /mnt/pacotes`).
- > Data e hora da máquina, com `# date > /mnt/date`. Anote a hora do seu relógio neste momento, para uma comparação futura. A defasagem encontrada deverá constar no laudo.
- > Usuários logados, com `# w > /mnt/w`.
- > Utilização de discos, com `# df -hT > /mnt/df`.
- > O kernel utilizado, com `# uname -a > /mnt/uname`.

continua...

Medidas iniciais nas forenses

continuando...

- ✓ Desmontar e remover o dispositivo externo (pendrive).
- ✓ Verificar, em outra máquina, se realmente foi gravado todo o conteúdo necessário no dispositivo externo.
- ✓ Desligar a máquina sem permitir que a mesma grave dados no disco. Para isso, puxe o cabo de energia da tomada sem desligar a máquina de forma convencional.

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ **Criação da imagem da mídia atacada**
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ Conclusão

Criação da imagem da mídia atacada

- ✓ Todo o trabalho de forense deverá ser realizado em uma cópia da mídia atacada (imagem).

Para criar a imagem:

- ✓ Adicionar um HD de capacidade maior do que o da máquina atacada.
- ✓ Inicializar a máquina atacada com um live CD voltado para forense (sugestão: Insert) ou pendrive com Linux (sugestão: http://tiny.cc/pendrive_debian).
- ✓ Montar apenas a partição do HD adicional (a que irá receber as imagens).
- ✓ Criar uma imagem do HD comprometido, por inteiro, no novo HD.

Criação da imagem da mídia atacada

- ✓ Após a criação da imagem do HD, calcular dois hashes de tais imagens (pelo menos um deverá ser SHA2).
- ✓ Todo o processo de abertura física da máquina comprometida, criação da imagem e cálculo dos hashes deverá ser acompanhado por duas testemunhas.
- ✓ Ao final da operação, deverá ser gerado um **certificado de integridade**, contendo a data, o nome e o CPF do perito, das testemunhas, o número de série do HD e os hashes obtidos. Todos deverão assinar o certificado, que será um dos anexos ao laudo pericial.
- ✓ O HD original deverá ser lacrado na presença de todos e entregue para autoridade competente. O número dos lacres deverá constar no laudo (ou no certificado de integridade).

Criação da imagem da mídia atacada

- ✓ Mídias danificadas (HD, pendrive, CD-ROM) poderão ter o seu conteúdo parcial copiado com o comando `dd_rescue`. Isso irá gerar um fragmento auditável com ferramentas especiais.
- ✓ Caso seja necessário trabalhar em cada partição do HD, bastará escrever a imagem em um outro HD de maior capacidade. Isso poderá ser feito com o comando `dd`.
- ✓ É muito importante preservar ao máximo a imagem original. Uma ideia é trabalhar todo o tempo em uma cópia da mesma.

Criação da imagem da mídia atacada

Exemplo de criação de imagens:

✓ HD comprometido: /dev/sda.

✓ 2° HD: possui uma única partição, a /dev/sdb1.

✓ Criação das imagens (/dev/sdb1 montado em /mnt):

```
# dd if=/dev/sda of=/mnt/sda.img
```

✓ Caso seja necessário usar as partições da imagem, escreva a imagem em outro HD (/dev/sdc, por exemplo), com o comando:

```
# dd if=/mnt/sda.img of=/dev/sdc
```

✓ O comando anterior criará um clone do HD a ser periciado. NÃO acesse o conteúdo para não alterar as datas e horas originais. Crie uma imagem de cada partição disponível.

Criação da imagem da mídia atacada

- ✓ O `dcfldd` é uma excelente alternativa ao `dd`.
- ✓ Dentre outras coisas, o `dcfldd` exibe o andamento da operação e calcula hashes em tempo real. Exemplo:

```
# dcfldd if=/dev/sda of=/mnt/sda.img hash=md5,sha256  
md5log=/mnt/sda.img.md5 sha256log=/mnt/sda.img.sha256
```

- ✓ Comparativo (usando como base um pendrive de 2GB em um netbook Atom):

* `dd` + `md5sum` + `sha256sum` = 7 min 23 seg (só o `dd`: 5' 03").

* `dcfldd`, calculando os hashes = 5 min 04 seg.

- ✓ Exemplo de saída de tela:

```
cygnus:~# time dcfldd if=/dev/sdc1 of=/mnt/sdc1.dcfldd hash=md5,sha256 md5log=sdc1.img.md5 sha256lo  
g=/mnt/sdc1.img.sha256  
34304 blocks (1072Mb) written.█
```

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ **Utilização da imagem da mídia atacada**
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ Conclusão

Utilização da imagem da mídia atacada

- ✓ Os arquivos de imagens (completo ou das partições) poderão ser analisados diretamente ou montados em outra máquina (somente as partições, exceto se for swap).
- ✓ As imagens das partições deverão ser montadas como loop (por ser arquivo) e read-only (para não alterar o conteúdo).
- ✓ Exemplo:

```
# mount -o loop,ro /mnt/sda1.img /forense
```
- ✓ Arquivos de swap são extensão da memória e não possuem filesystem. Então, serão analisados sem montagem (não é possível montá-los).

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ **O que buscar na análise**
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ Conclusão

O que buscar na análise

- ✓ Inicie a forense ouvindo os fatos para tentar deduzir algo relevante que leve à seleção de um ponto inicial. Exemplo: em defacements, começar pela análise do `/var/www`.
- ✓ Analise os logs.
- ✓ Analise a memória, o swap e os diretórios `/tmp` e `/var/tmp`.
- ✓ Analise o diretório `/home`.
- ✓ Analise o diretório `/etc`.
- ✓ Procure por rastros do seu oponente.
- ✓ Busque por rootkits e backdoors.
- ✓ Verifique se o sistema operacional estava atualizado.

O que buscar na análise

- ✓ Busque, em imagens, por arquivos relevantes apagados, com base em palavras-chave.
- ✓ Arquivos de MS Office e BrOffice.Org suspeitos devem ser analisados profundamente. Comece pelas propriedades dos mesmos.
- ✓ Seja inteligente, criativo e perseverante. Tenha a vontade de vencer o seu oponente!

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ **Alguns comandos e ferramentas**
- ✓ Laudo da perícia
- ✓ Conclusão

Alguns comandos e ferramentas

- ✓ Instale o sleuthkit (no Debian, `# apt-get install sleuthkit`; para ver comandos: `# dpkg -L sleuthkit | grep /usr/bin`).
- ✓ Use e abuse de `# ls -lua` e `# ls -lta`.
- ✓ Garimpe imagens e arquivos com strings + grep. O comando strings, no Debian, está no pacote binutils.
- ✓ Procure por rootkits com chkrootkit e rkhunter. Exemplos:
 - `# chkrootkit -r /forense`
 - `# rkhunter --update; rkhunter -c -r /forense`
- ✓ Procure por worms com o clamscan (`# apt-get install clamav`). Exemplo:
 - `# freshclam; clamscan -r /forense`

Alguns comandos e ferramentas

- ✓ Utilize o comando `find` para procurar por arquivos criados ou modificados nos últimos 2 dias. Exemplo:

```
# find /forense/ -mtime -2 -print
```

- ✓ Utilize os comandos `magicrescue` e `foremost` para buscar arquivos apagados em imagens. Os mesmos comandos também serão úteis em fragmentos de imagens ou imagens com filesystems corrompidos.
- ✓ Utilize `hexdump` e `hexedit` para acessar conteúdos, exibindo-os em hexadecimal ou ASCII (mesmo em fragmentos). Para ASCII puro, utilize o `view` do `mc`.
- ✓ Estude muito!!! (`apt-cache search forensic`).
- ✓ DEMONSTRAÇÃO.

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ **Laudo da perícia**
- ✓ Conclusão

Laudo da perícia

- ✓ Não há um modelo específico para laudo ou relatório de forense. É difícil encontrar um modelo na Internet.
- ✓ Alguns dados interessantes para a composição do laudo:
 - > Dados pessoais do perito.
 - > Período da realização da forense.
 - > Breve relato do ocorrido (notícias iniciais).
 - > Dados gerais sobre a máquina e/ou sistema atacado (nome da máquina, portas abertas, partições existentes etc).
 - > Detalhamento dos procedimentos realizados.
 - > Dados e fatos relevantes encontrados.
 - > Conclusão e recomendações.
 - > Apêndices e anexos. (incluir certificado de integridade)

Sumário

- ✓ O que é forense computacional?
- ✓ Ataques via rede: o que fazer?
- ✓ Medidas iniciais nas forenses
- ✓ Criação da imagem da mídia atacada
- ✓ Utilização da imagem da mídia atacada
- ✓ O que buscar na análise
- ✓ Alguns comandos e ferramentas
- ✓ Laudo da perícia
- ✓ **Conclusão**

Conclusão

- ✓ A perícia forense busca encontrar dados relevantes, em meios de armazenagem digital, com o intuito de levantar provas sobre um fato.
- ✓ Um perito forense deve conhecer profundamente o sistema operacional que ele irá investigar. Caso não o conheça, poderá solicitar um auxiliar técnico.
- ✓ A astúcia e a criatividade são essenciais em qualquer investigação. Tenha a vontade de vencer o seu oponente.

Esta palestra está disponível em

<http://www.eriberto.pro.br>