

Investigação digital

António Pinto
apinto@estg.ipp.pt

Escola Superior de Tecnologia e Gestão

Setembro, 2024 (v4)

Sumário

Introdução

- Visão geral

Exercícios

- Preparação das aulas

- Recuperação de ficheiros

Outros conceitos

- Técnicas anti-forense

- Funções resumo

Investigação digital

Investigação digital tenta **identificar**:

- ▶ Quais os **dispositivos envolvidos** no incidente
- ▶ Qual a **uso** dados aos dispositivos
- ▶ Qual o **motivo** por detrás do incidente
- ▶ **Quem** causou o incidente

Investigação digital **forense**:

- ▶ Forma mais restrita de investigação digital
- ▶ Possui requisitos legais (validade em tribunal)

Quando é que se aplica?

▶ **Recuperação de dados**

- ▶ Falhas em equipamentos centrais à operação
- ▶ Não existência de mecanismos de redundância
- ▶ Catástrofes naturais (não previstas)

Focus na continuidade do negócio!

▶ **Atividades não autorizadas**

- ▶ Natureza não técnica
- ▶ Ações ilícitas mal intencionadas
- ▶ Visam corromper, danificar, impedir operação, etc., de sistemas informáticos

Focus na prova pericial (polícias)!

Conceitos

Investigação digital

Técnicas e ferramentas que permitem recuperar, preservar e analisar evidências digitais armazenadas em, ou transmitidas por, dispositivos digitais. (Golden G. Richard III, 2011)

Evidência digital

Objecto digital que contém informação fidedigna que suporte ou refute uma hipótese. (Miguel Frade, IPLeiria)

Onde procurar evidências?

- ▶ Todo e qualquer suporte de armazenamento de informação (volátil ou permanente)

Que evidências é possível obter?

- ▶ Ficheiros eliminados
- ▶ Dados temporais (data de eliminação, modificação, acesso, criação, ...)
- ▶ Identificar que dispositivos de armazenamento (ex.: USB) estavam ligados a um PCs específico
- ▶ Identificar as aplicações instaladas (por vezes até após a sua desinstalação)
- ▶ Histórico de navegação na Internet
- ▶ ...

Exemplos de evidências digitais

- ▶ Documentos (docx, pptx, xlsx, ...)
- ▶ Emails (ameaças, divulgação de informação confidencial)
- ▶ Software malicioso
- ▶ Mensagens SMS, MMS (em telemóveis)
- ▶ Trabalhos de impressão eliminados
- ▶ ...

Onde procurar evidências digitais

- ▶ Ficheiros recuperados após eliminação (e respetiva informação)
- ▶ Windows Registry (histórico de dispositivos USB, últimos ficheiros acedidos, ...)
- ▶ Ficheiros de serviços de impressão (spool)
- ▶ Ficheiro de hibernação e de memória virtual (swap)
- ▶ Espaço livre, ficheiros temporários e cache de browsers
- ▶ ...

Processo de análise forense digital

1. Identificação de fontes de evidências digitais
 - ▶ Que equipamentos foram utilizados pelo suspeito?
2. Preservação e cópia de evidências digitais
 - ▶ Se possível, fazer cópias **fidedignas** para análise posterior
3. Análise minuciosa das evidências digitais
 - ▶ Recuperação de ficheiros (undelete, file carving)
 - ▶ Pesquisa por palavras chave
 - ▶ Inspeção do Windows registry
 - ▶ Geração de diagramas temporais (timelines)
4. Documentação e apresentação dos resultados
 - ▶ Elaboração de relatórios periciais
 - ▶ Depoimento ou testemunho em tribunal

Processo de análise forense digital

Princípios orientadores

1. As ações desencadeadas pelos investigadores não podem alterar os dados em análise que possam vir a ser usados como prova.
2. Em circunstâncias excepcionais, caso seja necessários aceder aos dados originais, quem o fizer deve ter competência para tal e ser capaz de explicar a relevância e implicações das suas ações.
3. Deve ser criada e preservada uma cadeia de auditoria, registando-se todos os processos aplicados aos dados, possibilitando a verificação por repetição.
4. A pessoa responsável pelo inquérito deve garantir a observância da lei e destes princípios.

Conteúdos

Introdução

Visão geral

Exercícios

Preparação das aulas

Recuperação de ficheiros

Outros conceitos

Técnicas anti-forense

Funções resumo

Kali linux

Preparação das aulas

Exercício #1 (30 minutos)

Considerando que o sistema de apoio às aulas será o Kali Linux, efetue os passos seguintes.

Descarregue o VirtualBox (incluindo o *Extension Pack*) e instale-o.
(<https://www.virtualbox.org/wiki/Downloads>)

Descarregue o Kali Linux, versão para VirtualBox, e instale-o.
[https://www.offensive-security.com/
kali-linux-vm-vmware-virtualbox-image-download/](https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/)

Por fim, atualize-o recorrendo aos comandos:

-
- 1 apt update
 - 2 apt upgrade
-

Conteúdos

Introdução

Visão geral

Exercícios

Preparação das aulas

Recuperação de ficheiros

Outros conceitos

Técnicas anti-forense

Funções resumo

Recuperação de ficheiros

Exercício #2 (15 minutos)

Descarregue a imagem de uma PEN USB 1GB do moodle.

Com os comandos seguintes, simule a ligação da PEN USB. Deverá aparecer um disco novo de 1GB no Kali.

```
1 mkdir /media/pen
2 mount -t auto -o loop pen_usb.img /media/pen
```

Verifique o conteúdo do disco. Não deverá encontrar nenhum conteúdo, porque os ficheiros foram apagados previamente.

Recuperação de ficheiros

Exercício #3 (30 minutos)

Com os comandos seguintes, recupere os ficheiros eliminados.

-
- 1 `sudo apt install foremost`
 - 2 `foremost pen_usb.img`
-

Note que foram eliminados 3 ficheiros. O comando anterior não permite recuperar ficheiros de texto simples.

Procure formas alternativas para recuperar este conteúdo (*strings*, *hexdump*, ...)

Submeta sua resposta pelo moodle (ficheiro PDF)

Conteúdos

Introdução

Visão geral

Exercícios

Preparação das aulas

Recuperação de ficheiros

Outros conceitos

Técnicas anti-forense

Funções resumo

Técnicas anti-forense

Definição

Make it hard for them to find you and impossible for them to prove they found you.¹ (S. Berinato, The Rise of Anti Forensics, 2007)

Conjunto de ferramentas que visam dificultar ou impedir a análise de evidências.

- ▶ Ferramentas que escondem informação (criptação, estenografia, ...)
- ▶ Ferramentas que removem evidências (limpeza de discos ou ficheiros, destruição de discos, ...)
- ▶ Ferramentas que escondem registos (alteração de timestamps em ficheiros, alteração de cabeçalhos de ficheiros, ...)

¹“Faz com que seja difícil encontrar-te e que seja impossível provar que te encontraram.”

Estenografia

(ou como esconder ficheiros dentro de outros ficheiros)

Exercício #4 (45 minutos)

Descarregue do moodle o ficheiro **poispois.jpg** e, com o comando seguinte, instale a aplicação Steghide.

```
1 apt install steghide
```

Analise o ficheiro de imagem usando, por exemplo o comando **exif**. Compare os resultados obtidos do ficheiro **poispois.jpg** com os da imagem original (**orig.jpg** no moodle).

```
1 exif poispois.jpg
2 exif orig.jpg
```

Tente obter mais informação com o comando seguinte.

```
1 steghide info poispois.jpg
```

Submeta sua análise crítica do ficheiro pelo moodle (ficheiro PDF)

Sumário

Introdução

Visão geral

Exercícios

Preparação das aulas

Recuperação de ficheiros

Outros conceitos

Técnicas anti-forense

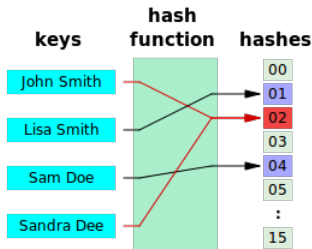
Funções resumo

Funções de resumo

Função de resumo (hash function)

Função para gerar rapidamente um bloco de bits, de tamanho fixo e pseudo-aleatório, a partir de um bloco variável de bits.

- ▶ Muito utilizado para pesquisas rápidas (hash tables)
- ▶ Permite a rápida detecção de duplicados



(fonte: Wikipedia, Jorge Stolfi)

Funções criptográficas de resumo

Função criptográficas de resumo (secure hash function)

Função de resumo que deverá garantir algumas propriedades criptográficas adicionais. (R. Anderson, 2008)

Propriedades necessárias

- ▶ One-way: Para um determinado valor y deve ser computacionalmente impossível descobrir um x tal que $H(x) = y$
- ▶ Resistente a colisões fracas: Para um determinado valor x deve ser computacionalmente impossível descobrir um x' tal que $H(x') = H(x)$
- ▶ Resistente a colisões: Deve ser computacionalmente impossível descobrir um par $x \neq y$ tal que $H(x) = H(y)$

Funções criptográficas de resumo

Exemplos

- ▶ MD4 = Message Digest 4 [RFC 1320] - operações 32 bits
~~MD4 = Message Digest 4 [RFC 1320] - operações 32 bits~~
- ▶ MD5 = Message Digest 5 [RFC 1321] - operações 32 bits
~~MD5 = Message Digest 5 [RFC 1321] - operações 32 bits~~
- ▶ SHA = Secure hash algorithm [NIST] ~~SHA = Secure hash algorithm [NIST]~~
- ▶ SHA-1 = Updated SHA ~~SHA-1 = Updated SHA~~
- ▶ SHA-2 = SHA-224, SHA-256, SHA-384, SHA-512
 - ▶ SHA-512 usa operações a 64 bits

MD4, MD5, SHA, SHA-1 já não são seguros!

Funções criptográficas de resumo

(ou funções de *hash*)

Exercício #5 (15 minutos)

Com os comandos seguintes, num terminal no Kali, crie dois ficheiros com nomes diferentes, mas com o mesmo conteúdo e calcule o resumo SHA-256 de ambos. Compare os resultados.

```
1 echo "Informatica_forense" > fich.txt
2 echo "Informatica_forense" > fich2.txt
3 sha256sum fich*.txt
```

Altere o conteúdo de um dos ficheiros e repita os testes. Compare os resultados.

Submeta sua análise crítica do ficheiro pelo moodle (ficheiro PDF)

Funções criptográficas de resumo - Colisões

Dois conjuntos de dados diferentes, por mais parecidos que sejam, devem gerar resumos criptográficos diferentes.

Função	<u>input</u>	<u>output</u>
MD5	Informática Forense	a2f62b5274a769abab7bd786ed8b6c95
MD5	informática forense	a4c94cc336407540b8f934bcb7657575

Quando dois conjuntos de dados diferentes (*input*) geram o mesmo resumo criptográfico (*output*), diz-se que estamos perante uma **colisão**, ou seja, o algoritmo foi quebrado.

Colisão MD5

Estas imagens geram uma colisão MD5

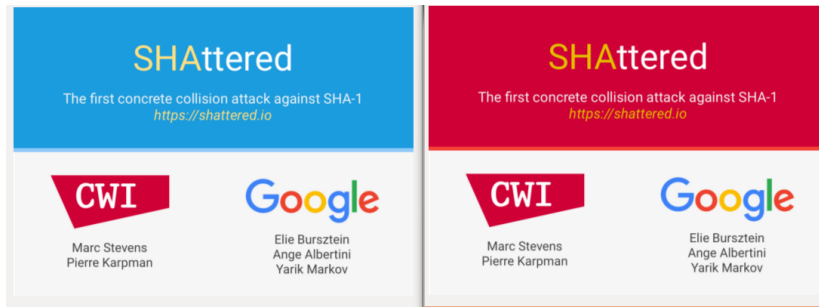


+info:

<https://natmchugh.blogspot.co.uk/2014/11/three-way-md5-collision.html>

Colisão SHA1

Estes PDFs geram uma colisão SHA1



```
└─ sha1sum *.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a 1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a 2.pdf
└─ /tmp/sha1
└─ sha256sum *.pdf
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0 1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff 2.pdf
```

0.64G 8-11h

+info: <https://shattered.io/>

Colisões MD5 e SHA1

Exercício #6 (15 minutos)

Com os comandos **md5sum** e **sha1sum**, calcule os *hashes* de todos os ficheiros que estão dentro do ficheiro **colisoes.zip** (disponível no moodle).

Compare os resultados.

Consegue identificar colisões? Se sim, quais?

Submeta sua análise crítica do ficheiro pelo moodle (ficheiro PDF)

Bibliografia

- ▶ Capítulo 2, Handbook of Digital Forensics and Investigation; Eoghan Casey; Academic Press
- ▶ A Road Map for Digital Forensic Research. (2001, August 7-8)
<http://www.dfrws.org/2001/dfrws-rm-final.pdf>
- ▶ Jones, A., & Valli, C. (2009). Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility. Burlington: Elsevier.
- ▶ Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006, August). Guide to Integrating Forensic Techniques into Incident Response.
<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
- ▶ C. Harrell (Oct 2010). Overall DF Investigation Process.
<http://journeyintoair.blogspot.pt/2010/10/overall-df-investigation-process.html>
- ▶ Lecture slides, Golden G. Richard, Disponivel online (Set, 2013)
<http://www.cs.uno.edu/~golden/Lectures/>
- ▶ Anderson, Ross. Security engineering. John Wiley & Sons, 2008.