



Segurança Forense

Aquisição de Prova Digital

 TÉCNICO
LISBOA

Seminário

2019

Nuno Santos



As pessoas deixam rasto digital em todo o lado

- ▶ Ficheiros pessoais, histórico web, etc. são guardados no desktop, telefones, e serviços cloud como Dropbox
- ▶ Ao logar-se em sites como o Gmail, o seu comportamento pode ser ligado ao seu nome real e endereço de email
- ▶ Tudo que pesquisa na Web e compra em sites como a Amazon ou põe no Facebook fica gravado para sempre
- ▶ Dispositivos móveis deixam rastos: as chamadas feitas, a localização, etc.
- ▶ Câmaras de vigilância no metro e autocarros registam a sua entrada e saída nos transportes
- ▶ ...



É possível utilizar estes rastos digitais como prova em tribunal?

▶ 2 Segurança Forense - Nuno Santos 2019

Sim!

Mashable

Facebook Pic of Police Car Gas-Siphoning Leads to Arrest

6.7K SHARES

BY TODD WASSERMAN
APR 19, 2012

A Kentucky man landed in jail after posting a picture of himself on Facebook siphoning gas from a police car.

Burglar leaves his Facebook page on victim's computer

September 16, 2009
By Edward Marshall, Journal Staff Writer

Save |

MARTINSBURG - The popular online social networking site Facebook helped lead to an alleged burglar's arrest after he stopped check his account on the victim's computer, but forgot to log out before leaving the home with two diamond rings.

▶ 3 Segurança Forense - Nuno Santos 2019

Exemplos (mais) sérios

Anthony trial: 'Chloroform' searched on computer

See show times +
NANCY GRACE
By Ashley Hayes, CNN
June 8, 2011 – Updated 2116 GMT (0516 HKT)

(CNN) -- Someone conducted keyword searches on "chloroform" using a desktop computer located in the home Casey Anthony shared with her parents, a computer examiner testified Wednesday in Anthony's capital murder trial.

The searches were found in a portion of the computer's hard drive that indicated they had been deleted, Detective Sandra Osborne of the Orange County Sheriff's Office testified.

However, she told jurors, deleted material remains on a computer's hard drive and can be retrieved until it is overwritten by new data. It had not been overwritten on the Anthonys' computer, she said, and "a complete Internet history" was obtained.

UK's youngest terrorist convicted of bomb plot

News > UK > Crime
Schoolboy from a respected Muslim family was part of cell that plotted to make explosives and napalm. Jonathan Brown and Michael Savage report

Monday 18 August 2008

A schoolboy who possessed a guide to making napalm on his computer and had notes on martyrdom under his bed became Britain's youngest convicted terrorist yesterday.

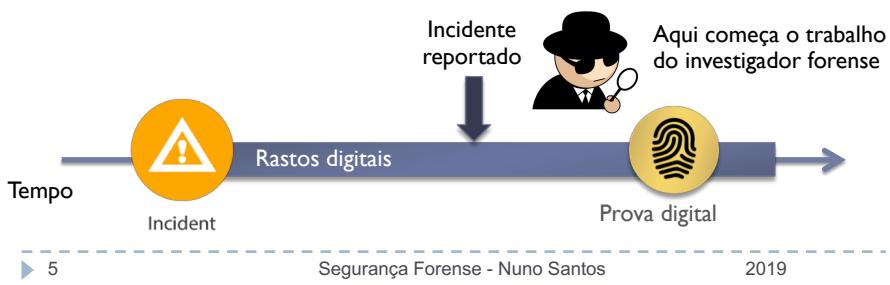
▶ 4 Segurança Forense - Nuno Santos 2019



O que é segurança forense?

► Segurança forense (AKA: ciber-segurança forense):

- ▶ Ramo de ciência forense que se ocupa com a aquisição, preservação, e análise de prova digital, tipicamente depois da ocorrência de acesso não autorizado



O que é prova digital?

► **Prova digital:** consiste em toda a informação de teor probatório armazenada ou transmitida em formato digital que possa ser usada em tribunal

▶ Ex., emails, fotografias digitais, registos de transações ATM, bases de dados, backups, etc.

▶ O objectivo da **segurança forense** consiste em explicar o estado actual de um determinado rastro digital



Casos de uso de segurança forense

▶ Processos criminais

- ▶ Baseiam-se em rastos obtidos a partir de um ou mais computadores para processar suspeitos e usar como prova

▶ Litígios civis

- ▶ Dados pessoais ou de empresas descobertos em computadores que podem ter sido usados em casos de fraude, divórcio, perseguição, ou discriminação

▶ Companhias de seguros

- ▶ Prova em computadores que pode ser utilizada para atenuar custos (fraude, compensação de trabalhadores, incendios, etc.)

▶ 7

Segurança Forense - Nuno Santos

2019



Casos de uso de segurança forense

▶ Empresas particulares

- ▶ Para obter prova de computadores de empregados em casos de perseguição, fraude, extorsão, e corrupção

▶ Agentes da lei (polícias)

- ▶ Usam métodos de segurança forense para recolha de prova em buscas e tratamento / manuseamento de prova após apreensão

▶ Individuos / investigadores privados

- ▶ Obtenção de serviços por parte de analistas forenses profissionais para suportar alegações em casos de perseguição, abuso, ou despedimento indevido do emprego

▶ 8

Segurança Forense - Nuno Santos

2019



Alguns casos muito mediáticos

The BTK Killer

From 1974 to 1991, 10 murders were committed in and around Wichita, Kansas, all by the same criminal dubbed the BTK Killer in the media. Although the killer communicated with police and media regularly, his identity remained a mystery, and investigators had given up hope of solving the case until he reinitiated contact in 2004. He delivered this message on a floppy disk, based on police "assurances" that documents saved on a floppy disk are not traceable. **However, using metadata on a deleted Microsoft Word document, police were quickly able to trace BTK's true identity: Dennis Rader.** Rader is now serving 10 consecutive life sentences in a Kansas prison. BTK's floppy disk error made his trial one of the most famous forensic cases ever.

The Corcoran Group

This lawsuit occurred over a fairly insignificant crime; plaintiffs claimed that defendants, including the real estate firm The Corcoran Group, knowingly sold them a condominium that flooded during storms, but failed to disclose this information to the buyers. The court discovered **that the Corcoran Group defendants had deleted many emails relevant to the case once litigation began.** This case changed the legal precedent on storage and deletion of electronically stored information, establishing an obligation to preserve electronically stored information relevant to a lawsuit that is underway or that seems likely to occur in the future.

▶ 9

Segurança Forense - Nuno Santos

2019



Exemplos de casos não resolvidos

The WANK Worm (1989)

Possibly the first "hacktivist" (hacking activist) attack, the WANK worm hit NASA offices in Greenbelt, Maryland. WANK (Worms Against Nuclear Killers) ran a banner (pictured) across system computers as part of a **protest to stop the launch of the plutonium-fueled, Jupiter-bound Galileo probe.** Cleaning up after the crack has been said to have cost NASA up to a half of a million dollars in time and resources. To this day, no one is quite sure where the attack originated, though many fingers have pointed to Melbourne, Australia-based hackers.



CD Universe Credit Card Breach (2000)

A blackmail scheme gone wrong, the posting of over 300,000 credit card numbers by hacker Maxim on a Web site entitled "The Maxus Credit Card Pipeline" has remained unsolved since early 2000. Maxim **stole the credit card information by breaching CDUniverse.com;** he or she then demanded \$100,000 from the Web site in exchange for destroying the data. While Maxim is believed to be from Eastern Europe, the case remains as of yet unsolved.

▶ 10

Segurança Forense - Nuno Santos

2019



Evolução temporal da segurança forense

- ▶ 70's
 - ▶ Primeiros casos de crimes envolvendo computadores, sobretudo fraude financeira
- ▶ 80's
 - ▶ FBI Computer Analysis and Response Team (CART) foi criada
- ▶ 90's
 - ▶ International Organization on Computer Evidence (IOCE)
- ▶ 00's
 - ▶ USA PATRIOT Act ("Computer Crime") permitiu a agências governamentais grande liberdade em investigação forense para combate ao terrorismo
 - ▶ Casos tratados pelo FBI CART ultrapassam 6500 casos (782 TB de dados)
 - ▶ Em Portugal, Lei do Cibercrime (Lei nº 109/2009)

▶ 11

Segurança Forense - Nuno Santos

2019



Ramos (não oficiais) da segurança forense

Segurança
Forense

- ▶ Computer forensics
 - ▶ Flash, HDD, dispositivos USB
- ▶ Network forensics
 - ▶ Monitorização e análise de tráfego de rede
- ▶ Mobile device forensics
 - ▶ Obtenção de prova de dispositivos móveis
- ▶ Cloud forensics
 - ▶ Análise forense de infraestruturas de núvem
 - ▶ ...

▶ 12

Segurança Forense - Nuno Santos

2019



Segurança forense vs. outras disciplinas



▶ **Segurança de computadores** debruça-se sobretudo com prevenção de acesso não autorizado, bem como a manutenção de confiabilidade, integridade, e disponibilidade de sistemas de computadores



▶ **Recuperação de dados** é o processo de recuperar dados inacessíveis a partir de sistemas de computadores corrompidos ou danificados não necessariamente no âmbito de uma investigação digital

▶ 13

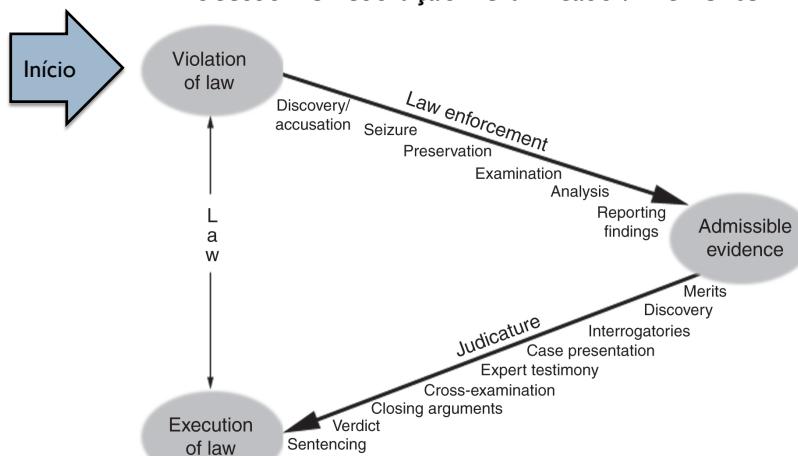
Segurança Forense - Nuno Santos

2019



Ciclo de vida da segurança forense

Processo de resolução de um caso / incidente



▶ 14

Segurança Forense - Nuno Santos

2019



Foco principal deste seminário

Aquisição de prova digital em cenários de investigação forense



► 15

Segurança Forense - Nuno Santos

2019



Processo de investigação digital

16

Segurança Forense - Nuno Santos

2019



Prova deve ser admissível em tribunal

- ▶ O que torna a prova “admissível”?
 - ▶ Resposta curta – se o juiz diz que sim, então é...
- ▶ Juízes usam regras gerais para avaliar admissibilidade:
 - ▶ A prova é relevante?
 - ▶ A prova é autentica?
 - ▶ A prova é crédivel?
 - ▶ A prova foi recolhida de forma legal?
- ▶ Princípio mais importante é a “regra excludente” que diz que não é admissível se estes critérios não são satisfeitos

► 17

Segurança Forense - Nuno Santos

2019



Lei do Cibercrime

- ▶ Lei n.º 109/2009, de 15 de Setembro
- ▶ CAPÍTULO III: Disposições processuais
 - ▶ Artigo 12.º: Preservação expedita de dados
 - ▶ Artigo 13.º: Revelação expedita de dados de tráfego
 - ▶ Artigo 15.º: Pesquisa de dados informáticos
 - ▶ Artigo 16.º: Apreensão de dados informáticos
 - ▶ Artigo 17.º: Apreensão de correio electrónico e registos de comunicações de natureza semelhante

► 18

Segurança Forense - Nuno Santos

2019



What is the goal of a digital investigation?

- ▶ To uncover the truth by producing **admissible evidence**
- ▶ To be admissible, evidence must meet the following criteria:
 - ▶ **Relevance:** be related to the case and prove something
 - ▶ **Authenticity:** evidence is the same as the originally seized
 - ▶ **Credibility:** the original evidence or admissible hearsay
 - ▶ **Legality:** search and seizure are authorized and privacy is assured
- ▶ Ultimately, the judge decides, but the digital investigator is responsible for ensuring all these criteria are met

▶ 19

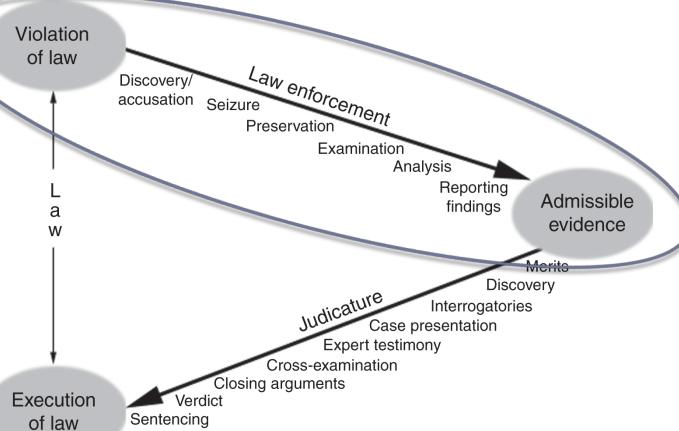
Segurança Forense - Nuno Santos

2019



Objectivo do processo de investigação forense?

Descobrir a verdade produzindo prova admissível em tribunal



▶ 20

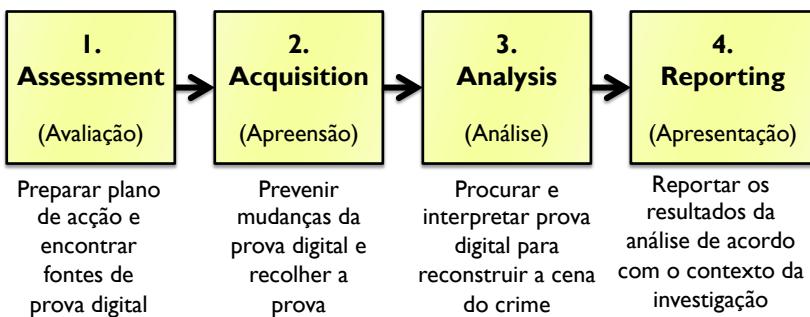
Segurança Forense - Nuno Santos

2019



First reference model for digital forensics

- ▶ Referência para ajudar a garantir admissibilidade



▶ 21

Segurança Forense - Nuno Santos

2019



1. Avaliação

- ▶ Primeiros passos:

- ▶ Definir o **âmbito** e se possível o **local** da recolha de prova
- ▶ Obter toda a **documentação legal** necessária
 - ▶ Obter sobretudo permissões para recolha de prova
- ▶ Determinar prováveis **fontes de prova** para aquele caso
 - ▶ Essas fontes devem ser fidedignas

▶ 22

Segurança Forense - Nuno Santos

2019



Níveis de autorização requeridos

- ▶ Para investigações internas
 - ▶ Autorização por parte da organização responsável
 - ▶ Para investigações **civis e criminais**
 - ▶ É preciso uma ordem do tribunal

United States District Court

SOUTHERN DISTRICT OF INDIANA

23

Securanca Forense - Nuno Santos

- 2019 -



Identificação das fontes de prova

- ▶ Dica geral: Seguir o caminho dos dados
 - ▶ Depende do tipo de caso ou da categoria de crime
 - ▶ Ex., recomendações do Departamento de Justiça dos EUA:

Chapter 7. Electronic Crime and Digital Evidence Considerations by Crime Category	35
Child Abuse or Exploitation	36
Computer Intrusion	37
Counterfeiting	38
Death Investigation	38
Domestic Violence, Threats, and Extortion	39
E-mail Threats, Harassment, and Stalking	40
Gambling	41
Identity Theft	41
Narcotics	42
Online or Economic Fraud	43
Prostitution	44
Software Piracy	45
Telecommunication Fraud	45
Terrorism (Homeland Security)	46

24

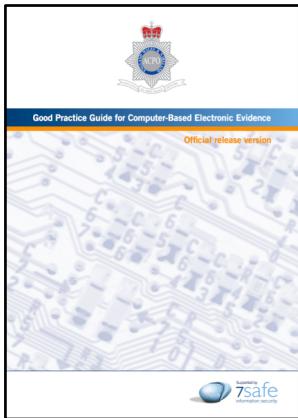
Segurança Forense - Nuno Santos

2019



Guidelines da polícia

- ▶ Policia e outras entidades têm guias de boas práticas:
 - ▶ O que deve ser apresndido, como, etc.



[ACPO] Association of Chief Police Officers, UK

▶ 25



[NIJ04] National Institute of Justice, USA

Segurança Forense - Nuno Santos

2019



2. Aquisição

- ▶ Métodos de recolha de prova devem assegurar que:
 - ▶ Todos os aspectos **legais** de “search & seizure” são seguidos
 - ▶ A **integridade** da prova foi preservada na extração
 - ▶ A prova apresentada em tribunal é **autêntica**
 - ▶ A recolha de prova é tão **completa** quanto possível

▶ 26

Segurança Forense - Nuno Santos

2019



Cadeia de custódia

- ▶ Manter uma **cadeia de custódia**, ou continuidade de posse:
 - ▶ É um dos aspectos mais importantes: manter e documentar a cadeia de custódia da prova
 - ▶ Começa com os primeiros objectos recolhidos
 - ▶ Tempo e data da recolha
 - ▶ Por quem e onde
 - ▶ Descrição completa de cada objecto
 - ▶ Cada vez que objecto muda de mãos deve ser actualizada
 - ▶ Tempo, data, e pessoa envolvida (com assinaturas dos curadores)

▶ 27

Segurança Forense - Nuno Santos

2019

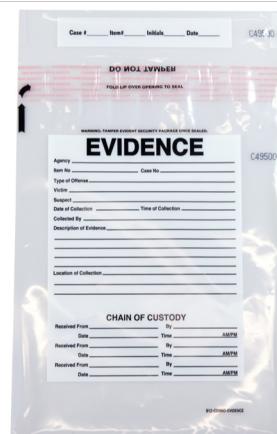


Formulário de uma cadeia de custódia

- ▶ Exemplos:

CERTIFIED INVENTORY OF EVIDENCE			
CASE NAME:		Date:	
Inventoried By:			
ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY			
Date	Action	Released by Sign and print name	Received by Sign and print name



▶ 28

Segurança Forense - Nuno Santos

2019



Potenciais irregularidades com cadeia de custódia

- ▶ Incompleta: falhas
- ▶ Datas inconsistentes
- ▶ Falta de identificação ou de assinatura do curador
- ▶ Curador não é competente ou autorizado

▶ 29

Segurança Forense - Nuno Santos

2019



Validações de integridade

- ▶ Garantir que a prova não foi alterada desde que foi recolhida até à apresentação em tribunal (garante autenticidade)
- ▶ Envolve comparação de **impressão digital digital (digital fingerprint)** do objecto recolhido no local
- ▶ Digital fingerprint é produzida por função de hash, ex., MD5

```
nuno$ md5 exams.pdf
MD5 (exams.pdf) = 3cbe84778b9c8600659ea182c270c289
celina:~ nuno$ shasum exams.pdf
01f427a4f4029651fc3865070dcfa8f4e94eed30  exams.pdf
celina:~ nuno$
```

▶ 30

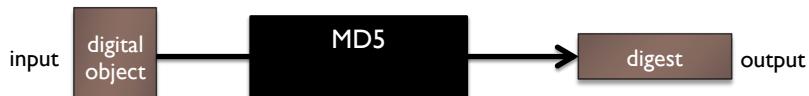
Segurança Forense - Nuno Santos

2019



Geração de digital fingerprints

- ▶ Uma função de hash funciona assim:



- ▶ Tem duas propriedades importantes:

- ▶ Produz sempre o mesmo número para um dado objecto
- ▶ Produz sempre números diferentes para diferentes objectos

▶ 31

Segurança Forense - Nuno Santos

2019



Why hash functions work well

- ▶ Basta alterar um único byte para o resultado final da digital fingerprint ser completamente diferente

Digital input	MD5 output
The suspect's name is John	0dc789ca62a3799abca7f1199f7c6d8c
The suspect's name is Joan	d5b5034d2f3bd578a136e18946e5777a

- ▶ As funções de hash mais usadas:

- ▶ MD5: produz valor de hash de 128-bit (“fingerprint”)
- ▶ SHA-1: produz valor de hash de 160-bit (20-byte)

▶ 32

Segurança Forense - Nuno Santos

2019



3. Análise

- ▶ Usar ferramentas forenses para localizar e extrair toda a prova, que seja:
 - ▶ **Inculpatória:** prova que sustenta uma dada teoria
 - ▶ **Desculpatória:** prova que contraria uma dada teoria
- ▶ Usar ferramentas forenses aprovadas pelo tribunal e documentar tudo

► 33

Segurança Forense - Nuno Santos

2019



O que procurar nos objectos recolhidos

- ▶ **Prova em claro**
 - ▶ Por exemplo, imagens, documentos, spreadsheets, etc. que possam ser relevantes
- ▶ **Prova escondida**
 - ▶ Objectos que possam ter sido intencionalmente escondidos
- ▶ **Prova apagada**
 - ▶ Documentos apagados pelo utilizador mas que ainda possa ser possível recuperar
- ▶ **Rasto de ferramentas anti-forense**
 - ▶ Rastos de técnicas anti-forense que foram usadas, ex. cifra, partições escondidas, software anti-forense, etc.

► 34

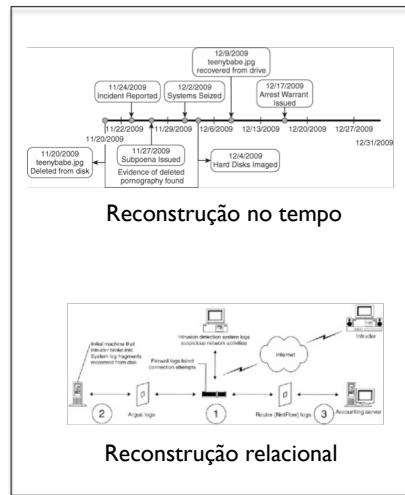
Segurança Forense - Nuno Santos

2019



Formas de reconstituição

- ▶ **Temporal** (quando)
 - ▶ Identificar sequências e padrões de eventos ao longo do tempo
- ▶ **Relacional** (quem, o quê, onde):
 - ▶ Componentes envolvidos e as relações entre eles
- ▶ **Funcional** (como)
 - ▶ O que foi possível tecnicamente (ex., verificar se o computador do suspeito tinha capacidade para descarregar quantidade de documentos apresentados como prova)



▶ 35

Segurança Forense - Nuno Santos

2019



4. Apresentação

- ▶ O resultado do trabalho de análise é a **documentação**
- ▶ Sem boa documentação, o caso não é sólido
 - ▶ Deve permitir a reprodução dos resultados
- ▶ **5 de documentação:**
 1. Documentação geral do caso
 2. Documentação procedural
 3. Documentação processual
 4. Timeline
 5. Cadeia de custódia



▶ 36

Segurança Forense - Nuno Santos

2019

Ferramentas para aquisição de prova

37

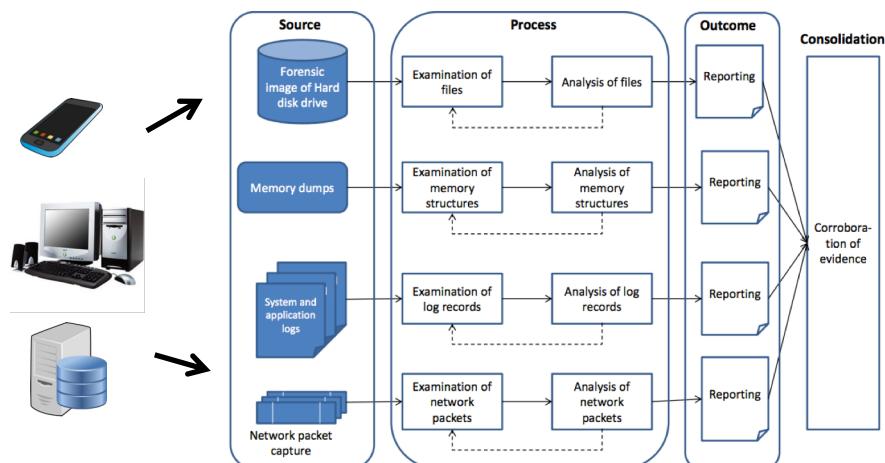
Segurança Forense - Nuno Santos

2019



Ciclo de utilização de ferramentas forenses

Setas indicam os passos em que as ferramentas são usadas



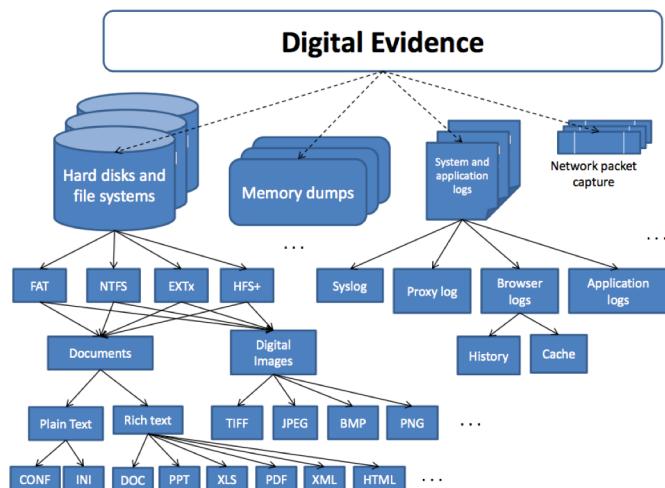
38

Segurança Forense - Nuno Santos

2019



No processo, muitos itens de dados são gerados



▶ 39

Segurança Forense - Nuno Santos

2019



Toolkit do analista forense

► Mochila ou mala com:

- ▶ Estação móvel forense (laptop)
- ▶ OS bootable “forensically-sound”
- ▶ Dispositivos de armazenamento saneados para recolha de prova: USB pen, drives externas
- ▶ Write blocker
- ▶ Saco Faraday
- ▶ Outros acessórios: cabo alimentação, adaptadores eléctricos, cabos de rede, baterias



Saco Faraday



Estação móvel forense



Write blocker

▶ 40

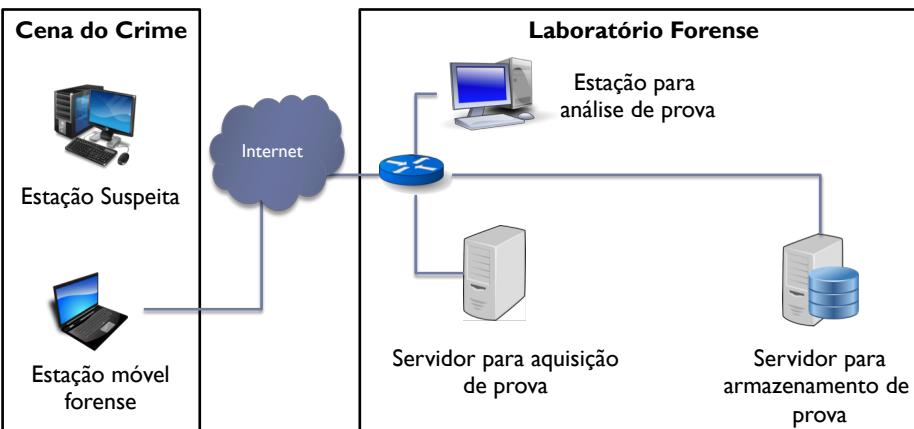
Segurança Forense - Nuno Santos

2019



Laboratório forense

- Contém equipamento para preservar prova digital e assistir na sua análise



► 41

Segurança Forense - Nuno Santos

2019



Obstáculos para a aquisição de prova

42

Segurança Forense - Nuno Santos

2019

Obstáculo #1: Heterogeneidade da tecnologia

Variedade de plataformas

Diversidade de componentes

Variedade de tecnologias para as mesmas plataformas

Múltiplas gerações de hardware

▶ 43 Segurança Forense - Nuno Santos 2019

Heterogeneidade do hardware, software, e dados

Desktop applications

Web applications

Server-side applications

Mobile applications

Operating systems

▶ 44 Segurança Forense - Nuno Santos 2019



Obstáculo #2: Dinamismo do sistema

- ▶ O estado do sistema muda, o que torna mais difícil obter um **retrato consistente** (snapshot) da prova
- ▶ Quanto menor for o dinamismo maior a precisão da prova obtida porque os dados serão mais consistentes

▶ 45

Segurança Forense - Nuno Santos

2019



Obstáculo #3: Volatilidade da prova digital

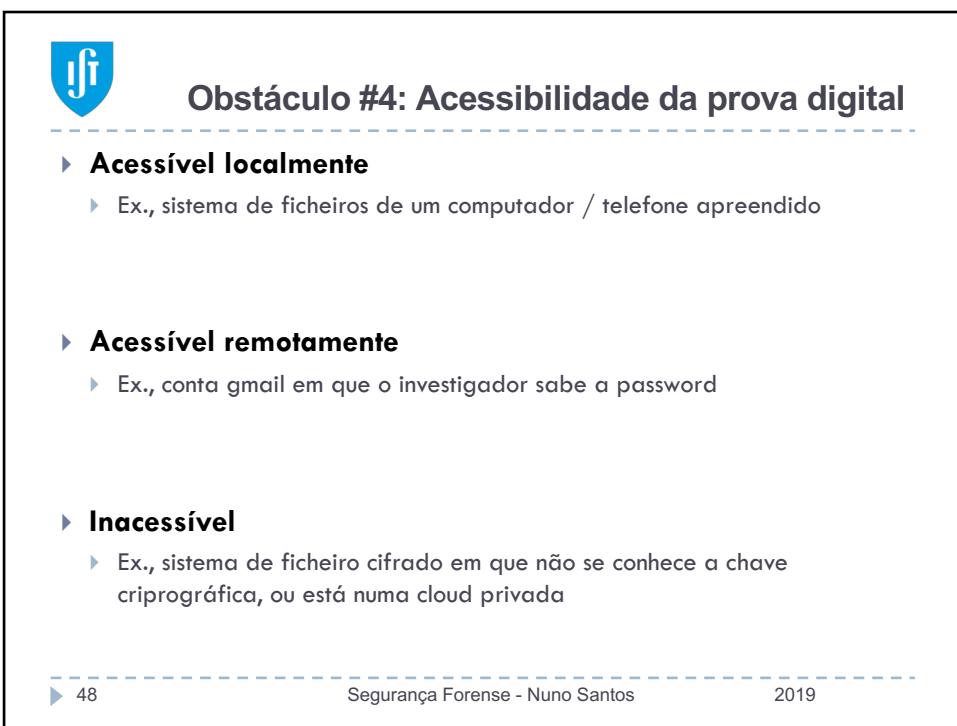
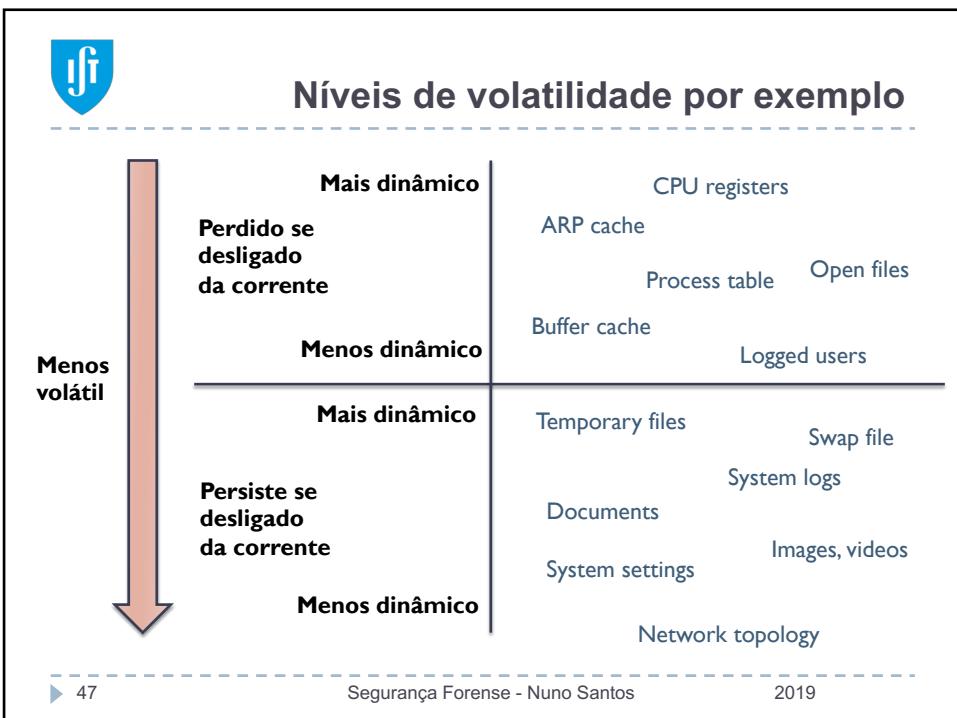
- ▶ Diz **por quanto tempo** os dados podem sobreviver no sistema
- ▶ O nível de volatilidade dos dados depende de:
 - ▶ Ser necessário alimentação eléctrica permanente para garantir o armazenamento dos dados
 - ▶ Quão rápido mudam os dados



▶ 46

Segurança Forense - Nuno Santos

2019





Outros factores que complicam

► Dados escondidos

- ▶ Armazenados em slack space, metadados, or em bebidos em conteúdos

► Dados apagados

- ▶ Dados apagados mas que talvez ainda será possível recuperar

► Dados corrompidos

- ▶ Sectores estragados, imagens danificadas, etc.

► Dados cifrados

- ▶ Ficheiros cifrados

► 49

Segurança Forense - Nuno Santos

2019



Obstáculo #5: Potencialmente muitos dados

► Dados gerados em 2010

- ▶ 1200 triliões de gigabytes (1.2 zettabytes)
- ▶ 89 pilhas de livros cada uma desde a Terra ao Sol



► Pode ser necessário fazer uma triagem

OPERAÇÃO MARQUÉS

Base de dados da Operação Marquês é quase o dobro dos Panama Papers

19/9/2016, 16:33 835 13

Base dados de documentos da Operação Marquês tem quase o dobro do tamanho da dos Panama Papers. São mais de 4,2 de terabytes que representam mais de 9 milhões de ficheiros informáticos.

► 50

Segurança Forense - Nuno Santos

2019

Acquisição de prova de computadores

51

Segurança Forense - Nuno Santos

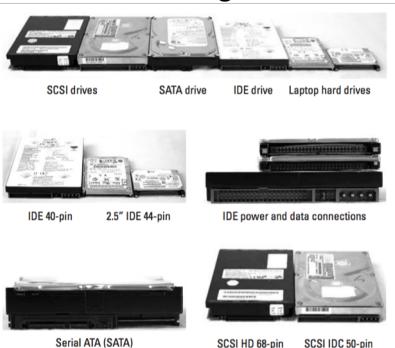
2019



Dispositivos de armazenamento na cena do crime

Como manusear esses dispositivos?

Discos rígidos



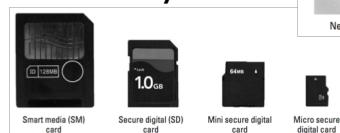
Thumb Drives



External Hard Drives



Memory Cards



▶ 52

Segurança Forense - Nuno Santos

2019



Procedimento geral para lidar com dispositivos de armazenamento persistente

- ▶ Se pudermos levar o dispositivo:
 - ▶ “Tag, bag, create chain of custody, bring to lab for data extraction”
- ▶ Caso contrário, é preciso efectuar extracção de dados no local
 - ▶ Extrair para a estação móvel forense e enviar para o laboratório
- ▶ Procedimento para extraír os dados do dispositivo:
 - ▶ Copiar os dados do dispositivo sem causar alterações
 - ▶ Calcular a hash desses dados
 - ▶ Criar pelo menos uma cópia (verificar a hash)

▶ 53

Segurança Forense - Nuno Santos

2019



Write blockers



- ▶ Cuidado a aceder (montar) o dispositivo fonte!
 - ▶ Ex., Windows cria miniaturas e pastas para recycle bin folders!
- ▶ Write blockers permitem aquisição de dados dos dispositivos sem modificar o seu conteúdo
 - ▶ As escritas são bloqueadas
 - ▶ Apenas comandos de leitura podem passar através do write blocker
 - ▶ Tipos de blockers: hardware e software

▶ 54

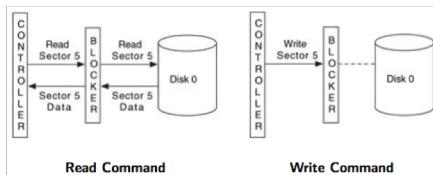
Segurança Forense - Nuno Santos

2019



Hardware write blocker

- ▶ HWB liga a estação forense e o dispositivo fonte
 - ▶ Várias interfaces suportadas: ATA, SCSI, Firewire, USB ou SATA
- ▶ O controlador não consegue escrever valores no registo de controle, responsável por escrever ou apagar dados no dispositivo



▶ 55

Segurança Forense - Nuno Santos

2019



Métodos para copiar os dados

- ▶ **Aquisição lógica**
 - ▶ Selecionar ficheiros relevantes para serem copiados
 - ▶ Mais rápido, menos espaço, mas incompleto
- ▶ **Bit-stream copy**
 - ▶ Cópia exacta bit-by-bit do original
 - ▶ Captura inclui meta-dados e quer objectos activos (ficheiros criados) como inativos (fragmentos de ficheiros apagados)
 - ▶ O destino pode ser um **disco**:
 - ▶ Deve estar saneado a zeros antes da cópia
 - ▶ Não deve estar montado no sistema de aquisição
 - ▶ Ou pode ser **ficheiro**, chamado imagem bit-stream (ex., image.dd)
 - ▶ O ficheiro pode ser guardado por exemplo num disco rígido

▶ 56

Segurança Forense - Nuno Santos

2019



Um computador na cena do crime

O computador está desligado. O que fazer primeiro?



▶ 57

Segurança Forense - Nuno Santos

2019



Ligar o computador pode alterar dados!

► Exemplos de ficheiros mudados no boot de um Windows XP

```
/WINDOWS/system32/config/system  
/pagefile.sys  
/hiberfil.sys  
/Documents and Settings/NetworkService/Local Settings/History  
/Documents and Settings/NetworkService/Local Settings/Application Data  
/WINDOWS/Debug/PASSWD.LOG  
/Documents and Settings/NetworkService/Local Settings/desktop.ini  
/Documents and Settings/NetworkService/ntuser.ini  
/Documents and Settings/NetworkService/Local Settings  
/Documents and Settings/NetworkService/Local Settings/Temporary Internet Files  
/WINDOWS/bootstat.dat  
/Documents and Settings/LocalService/Local Settings  
/Documents and Settings/LocalService/ntuser.ini  
/Documents and Settings/LocalService/Local Settings/desktop.ini  
/Documents and Settings/LocalService/Local Settings/Application Data  
/Documents and Settings/qwert/Local Settings/Application Data  
/Documents and Settings/qwert/Local Settings  
/Documents and Settings/qwert/Local Settings/Temporary Internet Files  
/Documents and Settings/qwert/Local Settings/desktop.ini  
/Documents and Settings/qwert/ntuser.ini  
/Documents and Settings/qwert/qwert/Local Settings/History  
/WINDOWS/system32/config/SAM.LOG  
/WINDOWS/Prefetch  
...
```

▶ 58

Segurança Forense - Nuno Santos

2019



Se ligamos o computador...

- ▶ Prova digital pode ser corrompida ou destruída!
 - ▶ Ficheiros no processo de arranque podem ser modificados
 - ▶ Executadas funções Autorun / scripts boot up
 - ▶ Malware executado durante o arranque

Se o computador está desligado, deixá-lo desligado

▶ 59

Segurança Forense - Nuno Santos

2019



Apreender um computador

- ▶ Proteger o conector do cabo de energia com fita adesiva
- ▶ Apreender também os cabos de energia
- ▶ Se o computador for um laptop, e se possível, remover a bateria e classificá-la

▶ 60

Segurança Forense - Nuno Santos

2019



E se não for possível levar o computador?

- ▶ Trazer os discos rígidos
 - ▶ Abrir a caixa
 - ▶ Extrair o disco



- ▶ Se não for possível extrair o disco rígido
 - ▶ Arracar a partir de um OS forense (e.g., Kali) de um DVD / USB drive
 - ▶ Pode ser necessário modificar a sequência de arranque na boot
 - ▶ Identificar o dispositivo (em /dev) que corresponde ao disco fonte
 - ▶ Efectuar uma cópia lógica ou bit-stream do disco
 - ▶ Nota: usar apenas ferramentas forenses de um OS forense fidedigno!

▶ 61

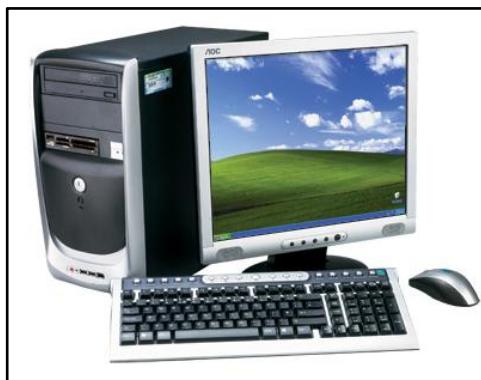
Segurança Forense - Nuno Santos

2019



E se o computador estiver ligado?

O que fazer nesta situação?



▶ 62

Segurança Forense - Nuno Santos

2019



Desligar de forma ordeira pode modificar dados!

► Ficheiros modificados ao desligar o Windows XP

```
/WINDOWS/system32/wbem/Logs/wmiprov.log  
/WINDOWS/system32/wbem/Logs/WinMgmt.log  
/Documents and Settings/qwert/NTUSER.DAT.LOG  
/Documents and Settings/qwert/NTUSER.DAT  
/Documents and Settings/qwert/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat  
/Documents and Settings/qwert/ntuser.ini  
/WINDOWS/system32/wbem/Repository/FS  
/WINDOWS/Tasks/SA.DAT  
/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP  
/WINDOWS/system32/wbem/Logs/wbemess.log  
/WINDOWS/5chedLgU.Txt  
/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP  
/WINDOWS/system32/config/SysEvent.Evt  
/WINDOWS/system32/config/software.LOG  
/WINDOWS/bootstat.dat  
/WINDOWS/inf/wkstamig.inf (deleted-realloc)  
/WINDOWS/system32/config/software  
/Documents and Settings/NetworkService/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat  
/WINDOWS/system32/config/system.LOG  
/Documents and Settings/LocalService/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat  
/WINDOWS/system32/config/system  
/WINDOWS/system32/config/SECURITY  
/Documents and Settings/NetworkService/NTUSER.DAT  
/Documents and Settings/LocalService/NTUSER.DAT  
/WINDOWS/system32/config/default  
/WINDOWS/system32/config/SAM
```

► 63

Segurança Forense - Nuno Santos

2019



Puxamos o cabo da corrente?

- No passado, puxar o cabo da corrente era o procedimento recomendado, mesmo se o computador estivesse a correr
- Dizia-se que não era muito importante preservar o estado da RAM



► 64

Segurança Forense - Nuno Santos

2019



Vantagens de desligar o cabo de alimentação

- ▶ Pode ajudar a preservar prova digital, por exemplo:
 - ▶ Um script de um suspeito programado para correr se o computador for desligado não vai ser executado
 - ▶ Ficheiros temporários de documentos word e outros permanecem no disco rígido, e poderiam ser apagados se a aplicação fosse terminada de forma ordeira

▶ 65

Segurança Forense - Nuno Santos

2019



Desvantagens de puxar o cabo eléctrico

- ▶ Perda de informação devido a **volatilidade** dos dados
 - ▶ Muita informação é mantida na RAM sobre process context information, network state information, e muito mais
 - ▶ Se desligarmos um sistema, essa informação é perdida
- ▶ Exemplos:
 - ▶ Mensagem importante do suspeito preservada na RAM
 - ▶ Em intrusões em redes, é importante capturar informação relacionada com processos em execução e malware residente em memória

▶ 66

Segurança Forense - Nuno Santos

2019



Um dilema semelhante: Desligar o cabo de rede

- ▶ Para impedir que alguém externo aceda ao cenário do crime, é recomendável **desligar** a conectividade dos sistemas
- ▶ No entanto, por vezes essa ação pode conduzir à **destruição de prova** e eliminar futuras oportunidades de investigação



▶ 67

Segurança Forense - Nuno Santos

2019



Riscos ao desligar o cabo de rede

- ▶ Perder possibilidade de **listar ligações activas**
 - ▶ Podemos nunca saber que outros computadores na rede podem ter prova relevante
- ▶ Perder possibilidade de **recolher tráfego de rede**
 - ▶ Muito importante em casos como intrusões em redes
- ▶ Causar impacto sério no **negócio**
 - ▶ Por exemplo, desligar o servidor de email de um site de e-commerce

▶ 68

Segurança Forense - Nuno Santos

2019



Live forensics

- ▶ Pode ser necessário realizar **operações de recolha** no próprio sistema que contém a prova
 - ▶ Ex., conta logada com utilizador, sistemas de rede, etc.
- ▶ **Live forensics vs. dead/postmortem forensics**
 - ▶ Live: análise é feita quando o sistema ainda está operacional
 - ▶ Dead/postmortem: análise feita em sistema desligado
- ▶ **Procedimento geral para live forensics:**
 - ▶ Correr as ferramentas forenses de DVD or USB stick
 - ▶ Recolher prova para armazenamento externo ou remoto
 - ▶ Criar log para todos os comandos executados

▶ 69

Segurança Forense - Nuno Santos

2019



Dados úteis a recolher em live forensics

- ▶ **Ficheiros e ligações rede**
 - ▶ List open files
 - ▶ lsof -nDr
 - ▶ List network connections
 - ▶ netstat -nap
 - ▶ List network routes
 - ▶ netstat -nr
 - ▶ List deleted and open files
 - ▶ ils -O /dev/hdaN
 - ▶ List network addresses
 - ▶ ifconfig
- ▶ **Processos**
 - ▶ List processes
 - ▶ ps auxl | \$nc # linux: suspect processes
 - ▶ Capture process memory
 - ▶ pcat <PID>
- ▶ **Utilizadores**
 - ▶ List active users
 - ▶ who -iHl
 - ▶ Obtain system information
 - ▶ tar cf - /proc

▶ 70

Segurança Forense - Nuno Santos

2019



Dados úteis a recolher em live forensics

► Memória

- ▶ Memory dump
 - ▶ volatility
- ▶ Swap space
 - ▶ dd if=/dev/SWAPdev bs=2k

► Volumes, sistemas de ficheiros

- ▶ Encrypted volumes
 - ▶ dd if=/dev/hdaN bs=2k
- ▶ Temporary partitions
 - ▶ dd if=/dev/TMPdev bs=2k
- ▶ File access times
 - ▶ ls -alRu

► Estruturas do OS

- ▶ Windows registry
- ▶ Windows event log

► Aplicações

- ▶ Browsers
 - ▶ Password caches
 - ▶ Web cache
- ▶ Cloud applications
 - ▶ Dropbox, Google Drive
- ▶ Messaging & social networks
 - ▶ Email clients
 - ▶ Facebook and Twitter accounts

Que dados recolher depende do caso em análise

► 71

Segurança Forense - Nuno Santos

2019



Análise de risco antes de live forensics

► Tipos de informação relevantes

- ▶ Ex. Memória contém: aplicações decifradas, chaves criptográficas, passwords, dados ainda não colocados em disco, etc.

► Pode ser importante ver se vale a pena terminar certas aplicações, mas é necessário saber o que se faz

- ▶ Fechar o Microsoft Internet Explorer coloca todos os dados em disco, pode ser útil para evitar perda de dados
- ▶ Mas fechar o KaZaA, pode resultar em perda de dados

► 72

Segurança Forense - Nuno Santos

2019

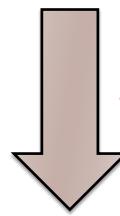


Por que ordem recolher a prova?

► Do mais volátil para o menos volátil

► Exemplo:

1. ARP cache
2. Process table
3. Kernel statistics and modules
4. Logs
5. User files



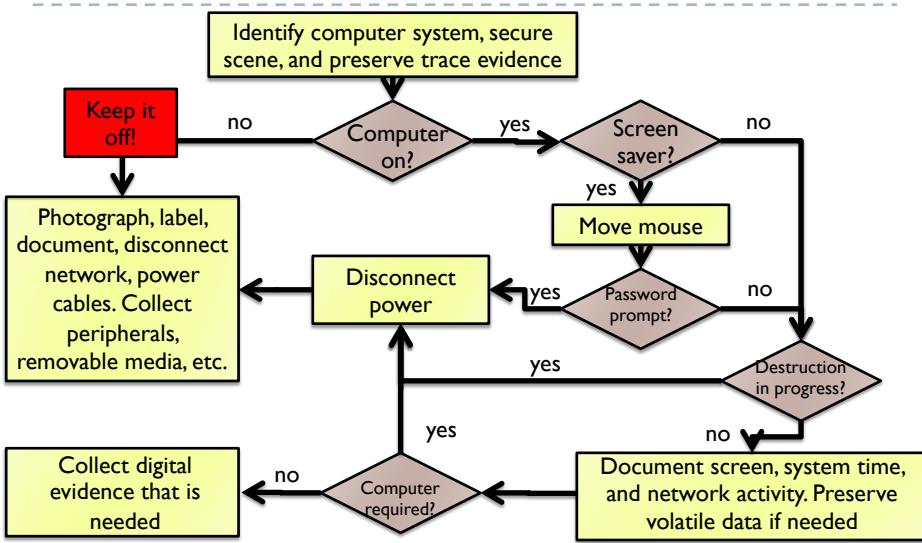
▶ 73

Segurança Forense - Nuno Santos

2019



Sumário de decisões em live forensics



▶ 74

Segurança Forense - Nuno Santos

2019



E dispositivos móveis na cena do crime?

Como adquirir prova desses dispositivos?

Mobile Phones



Smartphones



PDAs



▶ 75

Segurança Forense - Nuno Santos

2019



Dificuldades especiais

► Não é possível remover a memória interna

- Ao contrário dos discos rígidos

► O firmware e o OS restringem o acesso aos dados

- Ex., Android's debug bridge não deixa aceder a dados privados

► Conectados com exterior através de wireless

- Comandos enviados por 4G ou WiFi podem destruir dados

► Depende da bateria para alimentação

- Dados podem perder-se ou ficar inacessíveis se ficar sem bateria

▶ 76

Segurança Forense - Nuno Santos

2019



Formas de isolar da rede



Place the device in Airplane mode



Suspend account with carrier



Place the device in a Faraday bag: shield the interior from external electromagnetic radiation



Remove the SIM card



Turn off the device

▶ 77

Segurança Forense - Nuno Santos

2019



Conclusões

- ▶ Segurança forense desempenha um papel cada vez mais relevante na recolha de prova para resolução de processos judiciais
- ▶ Deve ser conduzida de forma extremamente rigorosa por forma a preservar a admissibilidade de prova em tribunal
- ▶ Para adquirir prova digital de sistemas de computadores, é necessário ter muitos factores em conta, por exemplo se se deve desligar o cabo de alimentação ou de rede

▶ 78

Segurança Forense - Nuno Santos

2019

ANEXO

Ferramentas forenses representativas

79

CSF - © Nuno Santos

2016/17



Representative tools

► Software tools

- Tools for post-mortem forensics
 - Storage-related tools
 - Networking tools
- Tools for live forensics
- General purpose tools

► Hardware tools

► 80

CSF - © Nuno Santos

2016/17



Representative tools

► Software tools

- ▶ Tools for post-mortem forensics
 - ▶ Storage-related tools
 - ▶ Networking tools
- ▶ Tools for live forensics
- ▶ General purpose tools

► Hardware tools

► 81

CSF - © Nuno Santos

2016/17



dd

► dd: “data dump” command

- ▶ Linux command to create bit-to-bit data copy of block device
- ▶ Need to mount the drive locally (read-only)

► Usage examples:

- ▶ Full disk
 - ▶ `dd if=/dev/sda of=/mnt/usb/sda.img bs=512`
- ▶ Partition
 - ▶ `dd if=/dev/sda1 of=/mnt/usb/sda1.img bs=512`

► 82

CSF - © Nuno Santos

2016/17



dcfldd

- ▶ **dcfldd: enhanced data dump command for forensics**
 - ▶ Specify hex patterns or text for clearing disk space
 - ▶ Log errors to an output file for analysis and review
 - ▶ Can calculate integrity checks (using MD5, etc.)
 - ▶ Verify acquired data with original disk or media data
- ▶ **Usage example:**
 - ▶ `dcfldd if=/dev/sourcedrive hash=md5 hashwindow=10M md5log=md5.txt bs=512 of=driveimage.dd`

▶ 83

CSF - © Nuno Santos

2016/17



Linux tools for image handling and inspection

- ▶ **Mount disk image/partition:**
 - ▶ `mount -o loop, ro, offset=XXXX disk_image.dd /mnt/mount_point`
- ▶ **Obtain partition information:**
 - ▶ `sfdisk -l disk_image.dd`
 - ▶ `fdisk -lu disk_image.dd`
- ▶ **Either work on the whole image**
 - ▶ Use the “offset” parameter
- ▶ **Can split (and mount) the image to individual partitions**
 - ▶ `dd if=disk_image.dd bs= 512 skip=xxx count=xxx of=partition.dd`

▶ 84

CSF - © Nuno Santos

2016/17



The Sleuth Toolkit (TSK)

- ▶ The Sleuth Toolkit (TSK) is a collection of command line volume and file system analysis tools

Tool Type	Tool Name
File system layer tools	fsstat
File name layer tools	ffind, fls
Meta data layer tools	lcat, ifind, ils, istat
Data unit layer tools	dcat, dls, dstat, dcalc
File system journal tools	jcat, jls
Media management tools	mmls
Image file tools	img_stat, mg_cat
Disk tools	disk_sreset, disk_stat
Other tools	hfind, mactime, sorter, sigfind

▶ 85

CSF - © Nuno Santos

2016/17



Autopsy

- ▶ Autopsy: tool for case management, interface to STK

create a new case

add new disk image

86

CSF - © Nuno Santos

2016/17

Autopsy

► Autopsy: perform a keyword search operation

show the results

▶ 87 CSF - © Nuno Santos 2016/17

Autopsy

► Autopsy: entering timeline options

▶ 88 CSF - © Nuno Santos 2016/17



File carvers

- ▶ **File carvers:** can recover deleted files from unallocated space

- ▶ Examples:

- ▶ Foremost
- ▶ Scalpel

▶ 89

CSF - © Nuno Santos

2016/17



Specialized file analysis tools

- ▶ **Windows registry**

- ▶ RegRipper
- ▶ Regslac
- ▶ Reg.exe

- ▶ **Mail**

- ▶ Scanpst
- ▶ MailBag
- ▶ FINALeMAIL
- ▶ Paraben
- ▶ DBXtract

- ▶ **Web Proxy Logs**

- ▶ Squidview
- ▶ Splunk

- ▶ **Images**

- ▶ EXIF Reader
- ▶ ThumbsPlus
- ▶ ACDSee

- ▶ **Mobile**

- ▶ XRY
- ▶ Cellebrite

▶ 90

CSF - © Nuno Santos

2016/17



EnCase

- ▶ EnCase is a commercial forensic software for FS analysis
 - ▶ Used in various court systems, e.g., in the case of BTK Killer

The screenshot shows the EnCase Enterprise Training software interface. At the top, there's a menu bar with options like Case (Sweep 7.5.2), View, Tools, Enterprise, EnScript, and Add Evidence. Below the menu is a toolbar with various icons. The main area has a tree view on the left showing a hierarchy of records, specifically Machine - DAMIRDELL, Windows, and SYS. To the right is a table titled 'Selected 1/52' with columns for Name, Tag, File Ext, Logical Size, Item Type, and Ca. The table lists nine items from 1 to 9, all of which are 'Operating System' type 'Folders'. At the bottom, there's a navigation bar with Report, Text, Hex, Decode, Doc, Transcript, Picture, Console, Fields, and a zoom control (Zoom In, Zoom Out, 100%, Previous Item, Next Item). A status bar at the bottom indicates the path: Sweep 7.5.2\Machine - DAMIRDELL\SYS\Windows\damirdeLL (Live Registry)\Operating System.

▶ 91

CSF - © Nuno Santos

2016/17



Representative tools

▶ Software tools

- ▶ Tools for post-mortem forensics
 - ▶ Storage-related tools
 - ▶ **Networking tools**
- ▶ Tools for live forensics
- ▶ General purpose tools

▶ Hardware tools

▶ 92

CSF - © Nuno Santos

2016/17

Capture packets using tcpdump

- ▶ Execute tcpdump command without any option will capture all the packets flowing through all interfaces
 - ▶ -i option allows you to filter on a particular ethernet interface

```
$ tcpdump -i eth1

14:59:26.608728 IP xx.domain.netbcp.net.52497 >
    valh4.lell.net.ssh: . ack 540 win 16554

14:59:26.610602 IP resolver.lell.net.domain >
    valh4.lell.net.24151: 4278 1/0/0 (73)

14:59:26.611262 IP valh4.lell.net.38527 >
    resolver.lell.net.domain: 26364+ PTR?
    244.207.104.10.in-addr.arpa. (45)
```

▶ 93

CSF - © Nuno Santos

2016/17

Wireshark: Sample packet capture

- E.g., you can scan through the HTTP traffic until you find a packet with an image (packet 48)

http_with_image.cap: Wireshark

Filter: | [Egrettions...](#) | [Close](#) | [Apply](#)

No.	Time	Source	Destination	Protocol	Info
43	2004-11-19 14:29:15.506923	10.1.1.101	10.1.1.101	TCP	csrv-proxy > HTTP [SYN] Seq=0 Win=40 MSS=1460
44	2004-11-19 14:29:15.541124	10.1.1.101	10.1.1.101	TCP	HTTP > csrv-proxy [SYN+ACK] Seq=1 Ack=1 Win=840 Len=0 MSS=1460
45	2004-11-19 14:29:15.543179	10.1.1.101	10.1.1.101	TCP	csrv-proxy > HTTP [ACK] Seq=1 Ack=1 Win=8535 Len=0
46	2004-11-19 14:29:15.561903	10.1.1.101	10.1.1.101	TCP	hrcm-cmn-pnrt > http [RTT, ACK] Seq=575 Ack=401 Win=6314 Len=0
47	2004-11-19 14:29:15.562335	10.1.1.101	10.1.1.101	TCP	http > brcm-com-pnrt [ACK] Seq=4403 Ack=576 Win=6888 Len=0
48	2004-11-19 14:29:15.564154	10.1.1.101	10.1.1.101	TCP	http > pole-infex [ACK] Seq=598 Win=6067 Len=0
49	2004-11-19 14:29:15.564154	10.1.1.1	10.1.1.101	TCP	pole-infex > [ACK] Seq=1 Ack=598 Win=6067 Len=0
50	2004-11-19 14:29:15.564207	10.1.1.101	10.1.1.1	HTTP	get /Websidain/images/synny.jpg HTTP/1.1
51	2004-11-19 14:29:15.564207	10.1.1.101	10.1.1.101	TCP	HTTP > pole-infex [ACK] Seq=2 Ack=598 Win=6060 Len=0
52	2004-11-19 14:29:15.567567	10.1.1.1	10.1.1.101	TCP	[TCP segment of a reassembled PDU]
53	2004-11-19 14:29:15.568009	10.1.1.1	10.1.1.101	TCP	[TCP segment of a reassembled PDU]
44	2004-11-19 14:29:15.568876	10.1.1.101	10.1.1.101	TCP	pole-infex > http [ACK] Seq=599 Ack=4921 Win=65551 Len=0
55	2004-11-19 14:29:15.571004	10.1.1.101	10.1.1.101	TCP	[TCP segment of a reassembled PDU]
56	2004-11-19 14:29:15.571979	10.1.1.1	10.1.1.101	TCP	[TCP segment of a reassembled PDU]
57	2004-11-19 14:29:15.572081	10.1.1.101	10.1.1.101	TCP	pole-infex > http [ACK] Seq=599 Ack=4381 Win=65535 Len=0
58	2004-11-19 14:29:15.572101	10.1.1.101	10.1.1.101	TCP	[TCP segment of a reassembled PDU]
59	2004-11-19 14:29:15.574543	10.1.1.1	10.1.1.101	TCP	[TCP segment of a reassembled PDU]

Frame 48: 651 bytes on wire (52 KB, 651 bytes captured)
Src: Ethernet II, Src: SmcNetwo...22:5a:02 (00:0c:20:a2:22:5a:02), Dst: Kyle_20:c5:df (00:c0:df:20:c5:df)
Internet Protocol Version 4 (IPv4) Src Port: 10.1.1.101 (10.1.1.101), Dst Port: 10.1.1.1 (10.1.1.1)
Transmission Control Protocol Src Port: pole-infex (3189), Dst Port: http (80), seq: 1, Ack: 1, Len: 597
Hypertext Transfer Protocol

Frame	Time	Source	Destination	Protocol	Info
0000	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	HTTP	GET / HTTP/1.1
0001	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	HTTP	HTTP/1.1 200 OK
0002	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	HTTP	Content-Type: image/jpeg
0003	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	HTTP	Content-Length: 102400
0004	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	HTTP	Connection: keep-alive
0005	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	HTTP	Date: Sat, 19 Nov 2004 14:29:15 GMT

▶ 94

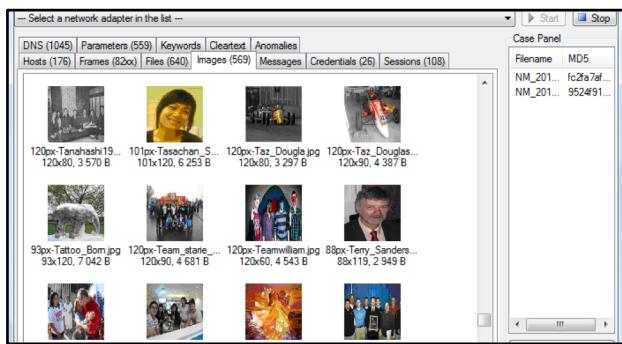
CSF - © Nuno Santos

2016/17



Flow analysis tools

- ▶ **Tcpflow, Pcapcat**
 - ▶ Follow TCP stream and saves every flow automatically in a file
- ▶ **Tcpextract**
 - ▶ Carve files from streams (e.g., attachments)
- ▶ **Network Miner**



▶ 95

CSF - © Nuno Santos

2016/17



Representative tools

- ▶ **Software tools**
 - ▶ Tools for post-mortem forensics
 - ▶ Storage-related tools
 - ▶ Networking tools
 - ▶ **Tools for live forensics**
 - ▶ General purpose tools
- ▶ **Hardware tools**

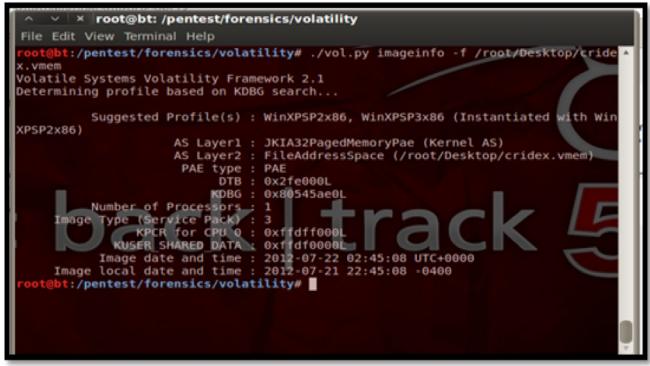
▶ 96

CSF - © Nuno Santos

2016/17

 **volatility**

► volatility: live memory image acquisition and analysis



```

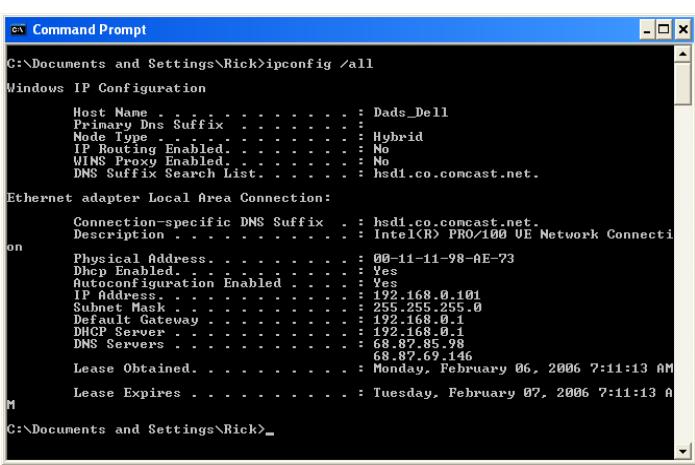
root@bt:/pentest/forensics/volatility
File Edit View Terminal Help
root@bt:/pentest/forensics/volatility# ./vol.py imageinfo -f /root/Desktop/crider.vmem
Volatile Systems Volatility Framework 2.1
Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : JKIA32PagedMemoryPae (Kernel AS)
AS Layer2 : FltAddressSpace (/root/Desktop/crider.vmem)
PAE : No
DTB : 0x2fe000L
KDBG : 0x80545ae0L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffffffff000L
KUSER_SHARED_DATA : 0xffffffff000L
Image date and time : 2012-07-22 02:45:08 UTC+0000
Image local date and time : 2012-07-21 22:45:08 -0400
root@bt:/pentest/forensics/volatility#

```

▶ 97 CSF - © Nuno Santos 2016/17

 **ipconfig**

► ipconfig: determine the state of the network



```

C:\Documents and Settings\Rick>ipconfig /all
Windows IP Configuration

Host Name . . . . . : Dads_Dell
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : hsdi.co.comcast.net.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : hsdi.co.comcast.net.
Description . . . . . : Intel(R) PRO/100 VE Network Connecti
on
Physical Address . . . . . : 00-11-11-98-AE-73
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address . . . . . : 192.168.0.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : 68.87.85.98
          68.87.69.146
Lease Obtained. . . . . : Monday, February 06, 2006 7:11:13 AM
Lease Expires . . . . . : Tuesday, February 07, 2006 7:11:13 AM

C:\Documents and Settings\Rick>

```

▶ 98 CSF - © Nuno Santos 2016/17



netstat

- ▶ netstat: lists current network connections

Proto	Local Address	Foreign Address	State
TCP	MCB09-0314:1282	localhost:1283	ESTABLISHED
TCP	MCB09-0314:1283	localhost:1282	ESTABLISHED
TCP	MCB09-0314:1284	localhost:1285	ESTABLISHED
TCP	MCB09-0314:1285	localhost:1284	ESTABLISHED
TCP	MCB09-0314:5152	localhost:4906	CLOSE_WAIT
TCP	MCB09-0314:1141	itads01.unco.edu:49157	ESTABLISHED
TCP	MCB09-0314:1143	itads01.unco.edu:49157	ESTABLISHED
TCP	MCB09-0314:1144	itex05.unco.edu:1259	ESTABLISHED
TCP	MCB09-0314:1146	itads01.unco.edu:49157	ESTABLISHED
TCP	MCB09-0314:1147	itads01.unco.edu:49157	ESTABLISHED
TCP	MCB09-0314:1148	itads01.unco.edu:49157	ESTABLISHED
TCP	MCB09-0314:1259	itads01.unco.edu:49157	ESTABLISHED
TCP	MCB09-0314:1388	itsepm02.unco.edu:http	ESTABLISHED
TCP	MCB09-0314:1389	uncsrv4.unco.edu:microsoft-ds	TIME_WAIT
TCP	MCB09-0314:1401	uncsrv4.unco.edu:microsoft-ds	ESTABLISHED
TCP	MCB09-0314:2607	uncsrv2.unco.edu:netbios-ssn	ESTABLISHED

▶ 99

CSF - © Nuno Santos

2016/17



Representative tools

- ▶ Software tools

- ▶ Tools for post-mortem forensics
 - ▶ Storage-related tools
 - ▶ Networking tools

- ▶ Tools for live forensics

- ▶ **General purpose tools**

- ▶ Hardware tools

▶ 100

CSF - © Nuno Santos

2016/17



General purpose tools

► SW forensic toolkits

- ▶ Helix:
 - ▶ <http://www.e-fense.com>
- ▶ Kali:
 - ▶ <https://www.kali.org>
- ▶ Knoppix STD:
 - ▶ <http://s-t-d.org>
- ▶ Caine
 - ▶ <http://www.caine-live.net>

► Compressing and archival utilities

- ▶ E.g., zip, tar, WinRAR

► Generation of hashes, checksums, & signatures

- ▶ e.g., sha1sum, a checksum-enabled dd, SafeBack, pgp

► Password crackers

- ▶ e.g., John the Ripper

► Editors

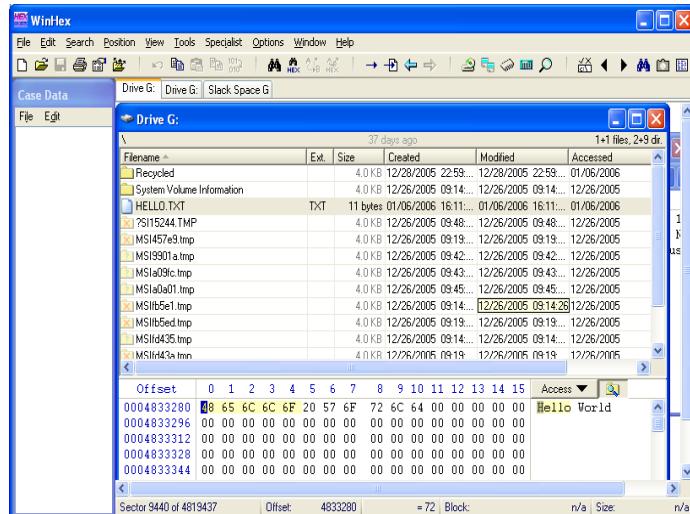
► 101

CSF - © Nuno Santos

2016/17



Hex Editors



► 102

CSF - © Nuno Santos

2016/17



Representative tools

► Software tools

- ▶ Tools for post-mortem forensics
 - ▶ Storage-related tools
 - ▶ Networking tools
- ▶ Tools for live forensics
- ▶ General purpose tools

► **Hardware tools**

► 103

CSF - © Nuno Santos

2016/17



Hardware tools

► HW tools can be for **incident response** and **laboratory**



Mobile forensic workstation



Toolkit



Faraday cage



Write blocker

► 104

CSF - © Nuno Santos

2016/17



Anti-forensic tools

▶ Anti-forensics

- ▶ Tools, methods, and processes aimed to hinder forensic analysis

▶ Main categories of anti-forensic tools:

- ▶ Artifact wiping
- ▶ Data hiding
- ▶ Anonymization
- ▶ Trail obfuscation
- ▶ Attacks against forensic tools



▶ 105

CSF - © Nuno Santos

2016/17



Artifact wiping

▶ Disk cleaning utilities

- ▶ DBAN, srm, KillDisk
 - ▶ Use variety of methods to overwrite data on disk
- ▶ CMRR Secure Erase
 - ▶ Uses the Secure Erase command built into the ATA specification

▶ File wiping utilities

- ▶ BCWipe
- ▶ Eraser

▶ Registry wiping tools

- ▶ CCleaner



▶ 106

CSF - © Nuno Santos

2016/17



Data hiding

► Generic data hiding tools

- ▶ Slacker
 - ▶ In the slack space of FAT or NTFS
- ▶ FragFS
 - ▶ In the NTFS Master File Table
- ▶ RuneFS
 - ▶ In bad blocks
- ▶ Waffen FS
 - ▶ In the ext3 journal file
- ▶ KY FS
 - ▶ In directories
- ▶ Data Mule FS
 - ▶ In inode reserved space

► Encryption tools

- ▶ TrueCrypt, CipherShed
 - ▶ Encrypted partitions

► Steganography tools

- ▶ Steganos
 - ▶ In BMP, VOC, WAV and ASCII files
- ▶ S-Tools
 - ▶ In GIF, and JPEG files



► 107

CSF - © Nuno Santos

2016/17



Anonymization

► Browsers

- ▶ Chrome's Incognito mode
- ▶ Safari's Private mode

► Web login sharing

- ▶ BugMeNot

► Web proxies

- ▶ <http://proxy.org/>
- ▶ Proxify
- ▶ Anonymouse
- ▶ Hide My Ass



► VPN

- ▶ <http://vpnbook.com>
- ▶ <http://freevpn.me>
- ▶ <http://vpnme.me>



► Onion routing

- ▶ Tor

► Anonymous mailers

- ▶ AnonymousEmail.me
- ▶ Anonymouse, Hide My Ass
- ▶ Tor Mail

► 108

CSF - © Nuno Santos

2016/17



Program obfuscation

- ▶ **Program packers:** prevent reverse engineering or detection
 - ▶ PECompact, Burney
 - ▶ Take 2nd program, compress and/or encrypt it, and wrap it in extractor
 - ▶ Shiva
 - ▶ Exit if its process is being traced

▶ 109

CSF - © Nuno Santos

2016/17



Trail obfuscation

- ▶ **Touch**
 - ▶ Unix command that modifies timestamps on allocated files
- ▶ **Defiler's Toolkit**
 - ▶ Can overwrite inode timestamps and deleted directory entries on Unixes
- ▶ **Timestop**
 - ▶ Can overwrite NTFS “create,” “modify,” “access,” and “change” timestamps
- ▶ **Transmogrify**
 - ▶ Allows the user to change the header information of a file, e.g., jpg to doc



▶ 110

CSF - © Nuno Santos

2016/17



Attacks against forensic tools

Breaking Forensics Software: Weaknesses in Critical Evidence Collection

Tim Newsham - <tim[at]isecpartners[dot]com>
Chris Palmer - <chris[at]isecpartners[dot]com>
Alex Stamos - <alex[at]isecpartners[dot]com>

iSEC Partners, Inc
115 Sansome Street, Suite 1005
San Francisco, CA 94104
<http://www.isecpartners.com>

July 1, 2007

▶ 111

CSF - © Nuno Santos

2016/17



A few anti-forensic countermeasure tools

▶ AF tool profiling

- ▶ Burndump

▶ Steganalysis tools

- ▶ StegSpy V2.0

▶ Cryptanalysis tools

- ▶ EverCrack



▶ 112

CSF - © Nuno Santos

2016/17