



AUGUST 3, 2013  
#481920  
LOG: 0

# Forense Computacional com Software Livre: do desktop aos dispositivos móveis!

Palestrante:  
Eng. Ézyo Lamarca da Silva



**5º CAFÉ**

COM SOFTWARE LIVRE

11 DE NOVEMBRO

# Ézyo Lamarca da Silva

AUGUST 3, 2013

#481920

L000

JULY 9, 2013



**INFOSEC COMPETENCE LEADERS**



**ÉZIO LAMARCA**

2º: Alcyon Júnior

3º: Fernando Torres

# Ézyo Lamarca da Silva

AUGUST 3, 2013

#481920

LOGO

Engenheiro Eletricista (UFPA) com ênfase em computação, com 30 anos de experiência na área de Tecnologia da Informação e Comunicação (TIC), 22 anos atuando na área de Segurança da Informação (SI) e com mais de 20 anos de trabalho em Administração de redes Windows, Linux e Novell nas maiores empresas públicas do Brasil (ECT, SERPRO, PRODEPA), certificado em Linux (LPIC-1) e Forense Computacional (DSFE), com especialização em Gestão de Segurança da informação (UNISUL) e aperfeiçoamento em Gestão da Inovação (UFSC); trabalhou como professor universitário na graduação nos cursos de Sistemas de informação (FEAPA) e Redes de Computadores (UNAMA) e nas especializações em Redes Linux (IESAM), Segurança Computacional/Direito Digital e Criminalística Computacional (IESAM/Estácio) e Cibersegurança/Perícia Forense Computacional (UNISAL), tendo ministrado aulas de Segurança da Informação e Forense Computacional como instrutor e monitor em grandes instituições nacionais (ESR/RNP e UNIFAMAZ), além de ter atuado em Forense Computacional Corporativa no setor público (SERPRO) e privado (auxiliar técnico em perícias para pessoas físicas e jurídicas), com o manual "Prática de Forense Computacional" de autoria própria sendo utilizado por entidades diversas em vários Estados pelo país. Atualmente é Agente Correccional na Divisão de Investigação Correccional na Corregedoria do SERPRO, tendo trabalhado anteriormente como Auditor Interno no SERPRO na área de Tecnologia e Negócios, participando de auditorias nas áreas de Segurança da Informação, Computação em Nuvem e LGPD. Professor da UniSENAI Florianópolis no curso de Análise e Desenvolvimento de Sistemas na disciplina Algoritmos e Programação. Vencedor do Prêmio Infosec Competence Leaders Brazil 2018/2019 na categoria Application Security. Palestrantes em diversos eventos de Software Livre pelo Brasil como FPSL (PA), FESLA (AP), ESLAM (AM), FISL (RS), FLISOL (PA), ConFLOSS (SC), dentre outros. Fundador do grupo de usuários Linux Pai d'Égua, o maior grupo de Software Livre do Norte do Brasil do começo dos anos 2000. Mais informações: [www.lamarca.eng.br](http://www.lamarca.eng.br)



# Forense Computacional

A Forense Computacional é uma ramificação da Ciência da Computação, podendo, entretanto, também ser considerada como um ramo da Criminalística, compondo uma área de conhecimento comum entre ambas.

AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1





# Forense Computacional

A Computação Forense (Computer Forensics) compreende a aquisição, preservação, restauração e análise de evidências computacionais, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais.

AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1



# Forense Computacional

Consiste, portanto, no uso de métodos científicos na preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital, produzindo informações diretas como meio de prova legal.

AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1

# Forense Computacional

Uma evidência digital é a informação armazenada ou transmitida em meio digital de valor probatório (SWGDE e IOCE, 2000). Possui como características próprias a possibilidade de ser duplicada com exatidão, a verificação de sua integridade por meio de ferramentas apropriadas, e a capacidade de ser recuperada mesmo depois de sua destruição.

# Forense Computacional

Atuando na análise forense computacional o profissional da informática é denominado perito judicial ou não oficial, perito criminal ou oficial, e perito em computação. Em todos os casos cuidará dos aspectos técnicos da investigação, produzindo, ao final, o laudo técnico ou pericial. Porém, sem se descuidar dos aspectos legais, recebendo, para tanto, o devido acompanhamento jurídico.





# Forense Computacional

Entretanto, a atuação do especialista em computação forense não se limita apenas a processos judiciais, podendo também ser contratado por empresas para investigações, questões relativas à segurança da informação e em equipes de resposta a incidentes, sendo, nesses casos, denominado perito em computação.



# Forense Computacional

## Fases da perícia forense computacional

No processo de perícia forense computacional toda a informação relevante deve ser coletada para análise e, conforme as evidências digitais são encontradas, serem extraídas, restauradas (caso as evidências estejam danificadas ou cifradas), documentadas e devidamente preservadas.



# Forense Computacional

Fases da perícia forense computacional

Este processo pode ser dividido em quatro fases bem distintas, sendo elas: identificação das evidências, preservação das evidências, análise das evidências, e apresentação das evidências.

# Forense Computacional

## Fases da Perícia Forense Computacional

Mídias → Dados → Informações → Evidências

**Coleta**

**Exame**

**Análise**

**Resultados  
Obtidos**

- Isolar a área
- Coletar as evidências
- Garantir a integridade
- Identificar equipamentos
- Embarcar evidências
- Etiquetar evidências
- Cadeia de Custódia

- Identificar
- Extrair
- Filtrar
- Documentar

- Identificar ( pessoas, locais e eventos)
- Correlacionar ( pessoas, locais e eventos)
- Reconstruir a cena
- Documentar

- Redigir laudo
- Anexar evidências e demais documentos

# Forense Computacional

## Software Livre



AUGUST 3, 2013

#481920

LOG: 1

JULY 9, 2013

#453201

LOG: 1

Fases	Descrição	FTK
Preparação	Esterilizar as mídias que serão utilizadas na investigação	wipe
Coleta dos Dados	Data hora do sistema operacional	Sistema Operacional
	Conexões de rede ativas	
	Processos em execução	
	Arquivos abertos	
	Imagem das mídias	AIR
	Geração de Hash (integridade das evidências)	md5
	Cadeia de Custódia	Formulário de Custódia
	Recuperar arquivos deletados	Fatback, e2undel
	Manipulação de sistemas de arquivos NTFS	ntfsprogs, scrounge-ntfs

# Forense Computacional

## Software Livre



AUGUST 3, 2013

#481920

LOG: 1

JULY 9, 2013

#453201

LOG: 1

Fases	Descrição	FDTK
Exame dos Dados	Visualizar imagens	comix
	Acessar arquivos compactados	p7zip
	Quebrar senhas de arquivos	ophcrack
	Coletar mac time de arquivos e diretórios	mactime
	Deteção da presença de rootkits	chkrootkit
	Leitores para varias extensões proprietárias da MS	Antiword, evtreader
Análise das Evidências	Analisar bases de dados de email MS	eindeutig
	Analisar cookies do Windows	cookie_cruncher.pl
	Script perl para ler arquivo history.dat do Firefox	mork.pl
	Visualizador de históricos de navegadores	browser-history-viewer
	Ferramentas para várias finalidades	autopsy

# Forense Computacional

## LibreOffice / OpenOffice



AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1

Sistema de Acompanhamento Forense - SAfo - modelo.odt

Banco de dados

Tarefas

- Tabelas
- Consultas
- Formulários
- Relatórios

Formulários

- 01 - Identificação do Caso
- 02 - Tarefas Forenses
- 03 - Artefatos Gerados
- 04 - Evidências Encontradas
- 05 - Visão Geral

Nenhum

Banco de dados incorporado      Firebird incorporado

Sistema de Acompanhamento Forense - SAfo - modelo.odt : 01 - Identificação do Caso

Número do Caso: 1

Nome do Caso: Perda Total

Nome do Perito: Eryo Lamarca da Silva

Descrição: Caso de exemplo

Comentários: Caso usado no curso de Forense Computacional

Data de Inicio: 10/02/18 08:00

Data de Fim:

**DigitalSec**

# Forense Computacional

## Kanboard



AUGUST 3, 2013

#481920

LOG: 1

JULY 9, 2013

#453201

LOG: 1

forenses.digitalsec.com.br

### KB Forenses

Exibir outro projeto

Visão global **Quadro** Lista status:open

+ Backlog (30)	+ A fazer	+ Em andamento	+ Feito
<b>#1</b> 0. Referências P 1 [104d][104d] P0			
<b>#2</b> 0.0. Relato inicial do caso P 1 [104d][104d] P0			
<b>#3</b> 0.1. Hardware de trabalho P 1 [104d][104d] P0			
<b>#4</b> 0.2. Software utilizado P 1 [104d][104d] P0			
<b>#5</b> 0.3. Mídias de armazenamento P 1 [104d][104d] P0			
<b>#6</b> 1. Coleta P 1 [104d][5d] P0			
<b>#7</b> 1.1. Reunião inicial com o cliente P 1 [104d][104d] P0			
<b>#8</b> 1.2. Aquisição da Imagem Forense P 1 [104d][104d] P0			



# Forense Computacional

## ownCloud



AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1

Houve problemas com a verificação de integridade do código. Mais informações...

Arquivos

Todos os arquivos

Favoritos

Compartilhado com você

Compartilhado com outros

Compartilhado por link

Etiquetas

Arquivos apagados

Configurações

Forenses > Modelo > +

Nome

Tamanho

Modificado



Sistema de Acompanhamento Forense - SAFo - modelo.odt



2.7 MB

há um mês



kanboard-forenses.tar.bz2



2.5 MB

há 5 meses



4-Relatório



0 KB

há 2 meses



3-Análise



0 KB

há 2 meses



2-Exame



0 KB

há 2 meses



1-Coleta



0 KB

há 2 meses



0-Referências



0 KB

há 2 meses

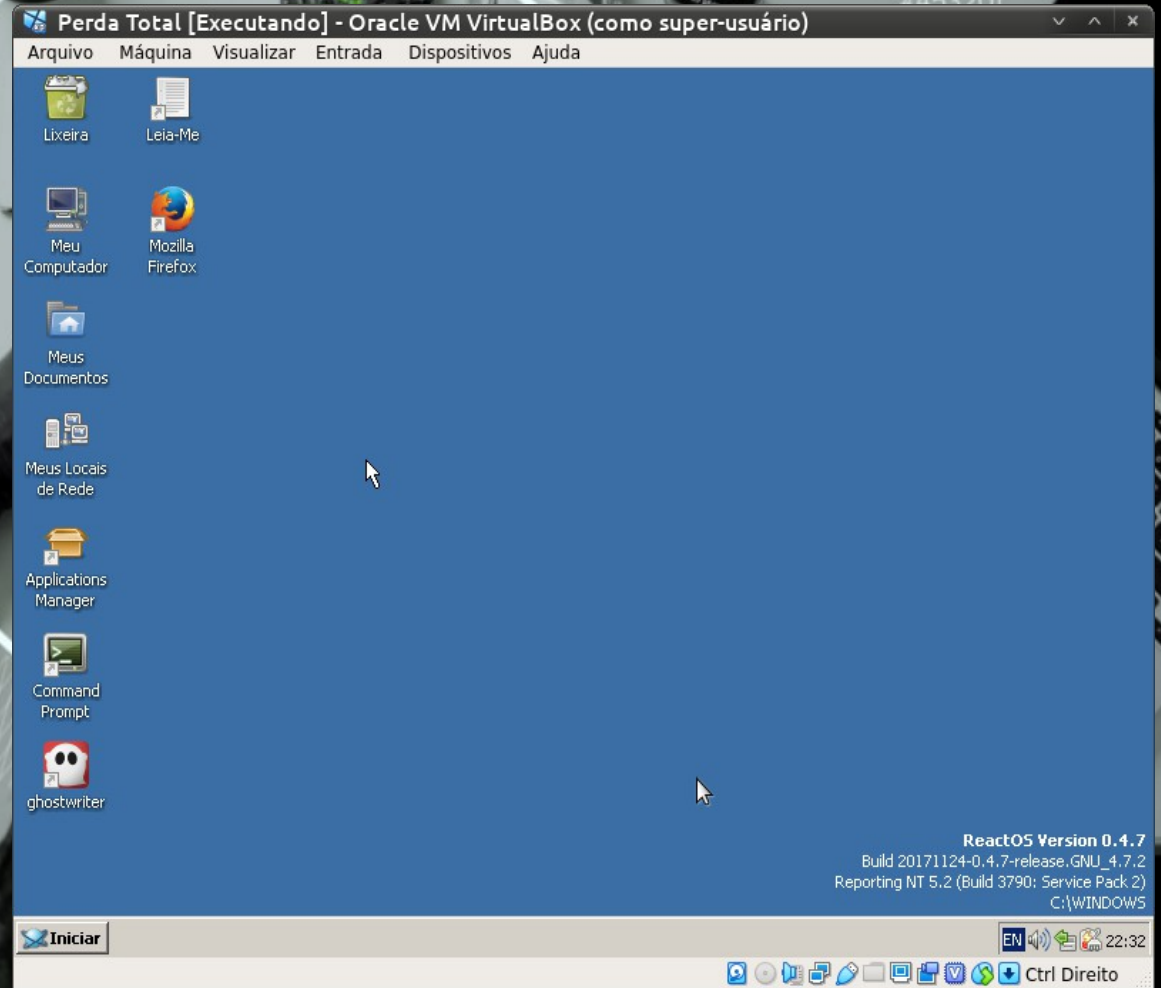
5 pastas e 2 arquivos

5.2 MB

# Forense Computacional

VirtualBox

ReactOS



# Forense Computacional

## Comandos: mount, grep, strings



AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1

```
perito@ultra: ~/Perda_Total
Arquivo Editar Ver Pesquisar Terminal Ajuda
perito@ultra:~/Perda_Total$ time strings Forense_Coleta.dd > Perda_Total.dd.strings
real    1m0,731s
user    0m48,408s
sys     0m2,654s
perito@ultra:~/Perda_Total$ grep -i rootkit --color Perda_Total.dd.strings
rootkit/SM
rootkit/a
chkrootkit
rootkit-ul/n
perito@ultra:~/Perda_Total$ grep -i backdoor --color Perda_Total.dd.strings
backdoor
backdoor/a
backdoor
backdoor
backdoor/N0sT
backdoors
perito@ultra:~/Perda_Total$ grep -i portscan --color Perda_Total.dd.strings
(%s:%d) VideoPortScanRom RomBase %p RomLength 0x%x String %s
VideoPortScanRom
VideoPortScanRom
perito@ultra:~/Perda_Total$
```

# Forense Computacional

## The Sleuth Kit



```
perito@ultra: ~/Perda_Total
Arquivo Editar Ver Pesquisar Terminal Ajuda
perito@ultra:~/Perda_Total$ fls -o 63 Forense_Coleta.dd
d/d 3: WINDOWS
r/r 4: freeldr.sys
r/r 5: freeldr.ini
r/r 6: pagefile.sys
d/d 9: Documents and Settings
d/d 12: Arquivos de programas
d/d 13: RECYCLED
r/r * 14: _oneca.zip
v/v 100457107: $MBR
v/v 100457108: $FAT1
v/v 100457109: $FAT2
V/V 100457110: $OrphanFiles
perito@ultra:~/Perda_Total$ fls -r -m '/' -o 63 Forense_Coleta.dd > bodyfile.txt
perito@ultra:~/Perda_Total$ mactime -b bodyfile.txt -d > timeline.csv
perito@ultra:~/Perda_Total$ libreoffice timeline.csv
```

AUGUST 3, 2013  
#481920  
LOG:1

JULY 9, 2013  
#453201  
LOG:1



timeline.csv - LibreOffice Calc

A1	Date							
6314	Sat Feb 10 2018 23:17:02	4257197..b	rfmseevexes	0	0	37561114	/Arquivos de programas/7-Zip/_oneca.zip (deleted)	
6315	Sat Feb 10 2018 23:17:22	4257197.m...	rfmseevexes	0	0	36945662	RECYCLED/DeD.jpg	
6316	Sun Feb 11 2018 00:00:00	736547.a...	rfmseevexes	0	0	3322409	Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)	
6317	Sun Feb 11 2018 00:00:00	1209051.a...	rfmseevexes	0	0	3322413	Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)	
6318	Sun Feb 11 2018 00:00:00	531424.a...	rfmseevexes	0	0	3322419	Documents and Settings/Administrator/Meus Documentos/stockvault-art-and-nature9967.jpg	
6319	Sun Feb 11 2018 00:00:00	4899735.a...	rfmseevexes	0	0	3322431	Documents and Settings/Administrator/Meus Documentos/stockvault-artistic-rude111056.jpg	
6320	Sun Feb 11 2018 00:00:00	101257.a...	rfmseevexes	0	0	3322436	Documents and Settings/Administrator/Meus Documentos/stockvault-close-up-nude-body-woman175004.jpg	
6321	Sun Feb 11 2018 00:00:00	1869728.a...	rfmseevexes	0	0	3322441	Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111901.jpg (deleted)	
6322	Sun Feb 11 2018 00:00:00	1967942.a...	rfmseevexes	0	0	3322446	Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111903.jpg (deleted)	
6323	Sun Feb 11 2018 00:00:00	2431415.a...	rfmseevexes	0	0	3322451	Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111904.jpg (deleted)	
6324	Sun Feb 11 2018 00:00:00	28.a...	rfmseevexes	0	0	50179978	Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.m.lock (deleted)	
6325	Sun Feb 11 2018 00:00:00	2302.a...	rfmseevexes	0	0	50179981	Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.m.lock (deleted)	
6326	Sun Feb 11 2018 00:00:00	2302.a...	rfmseevexes	0	0	50179984	Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.m.mDR876 (deleted)	
6327	Sun Feb 11 2018 00:00:00	21.a...	rfmseevexes	0	0	51168775	Documents and Settings/Administrator/Meus Documentos/boneca/senhã_boneca.tst (deleted)	
6328	Sun Feb 11 2018 03:39:08	21..b	rfmseevexes	0	0	51168775	Documents and Settings/Administrator/Meus Documentos/boneca/senhã_boneca.tst (deleted)	
6329	Sun Feb 11 2018 03:40:24	21.m...	rfmseevexes	0	0	51168775	Documents and Settings/Administrator/Meus Documentos/boneca/senhã_boneca.tst (deleted)	
6330	Sun Feb 11 2018 03:40:28	28.m.b	rfmseevexes	0	0	50179978	Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.m.lock (deleted)	
6331	Sun Feb 11 2018 03:40:28	2302.m.b	rfmseevexes	0	0	50179981	Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.m.lock (deleted)	
6332	Sun Feb 11 2018 03:40:28	2302.m.b	rfmseevexes	0	0	50179984	Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.m.mDR876 (deleted)	
6333	Sun Feb 11 2018 03:41:24	1869728.m...	rfmseevexes	0	0	3322441	Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111901.jpg (deleted)	
6334	Sun Feb 11 2018 03:41:54	1209051.m...	rfmseevexes	0	0	3322413	Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)	
6335	Sun Feb 11 2018 03:42:14	736547.a...	rfmseevexes	0	0	3322409	Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)	
6336	Sun Feb 11 2018 03:44:30	736547..b	rfmseevexes	0	0	3322409	Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-back114947.jpg (deleted)	
6337	Sun Feb 11 2018 03:44:30	1209051..b	rfmseevexes	0	0	3322413	Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)	
6338	Sun Feb 11 2018 03:44:32	1869728..b	rfmseevexes	0	0	3322441	Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111901.jpg (deleted)	
6339	Sun Feb 11 2018 03:44:32	1967942..b	rfmseevexes	0	0	3322446	Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111903.jpg (deleted)	
6340	Sun Feb 11 2018 03:44:34	2431415..b	rfmseevexes	0	0	3322451	Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111904.jpg (deleted)	
6341	Thu May 02 2019 00:00:00	12.a...	rfmseevexes	0	0	190	WINDOWS/booster.dat	
6342	Thu May 02 2019 00:00:00	155648.a...	rfmseevexes	0	0	33208491	Documents and Settings/LocalService/rtuser.dat	
6343	Thu May 02 2019 00:00:00	155648.a...	rfmseevexes	0	0	33228529	Documents and Settings/Branden/Screenshot.jpg	

# Forense Computacional

## FDTK



AUGUST 3, 2013

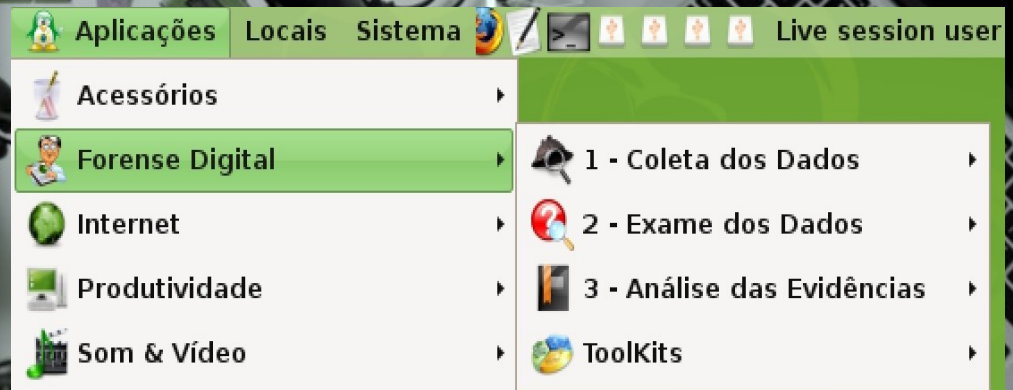
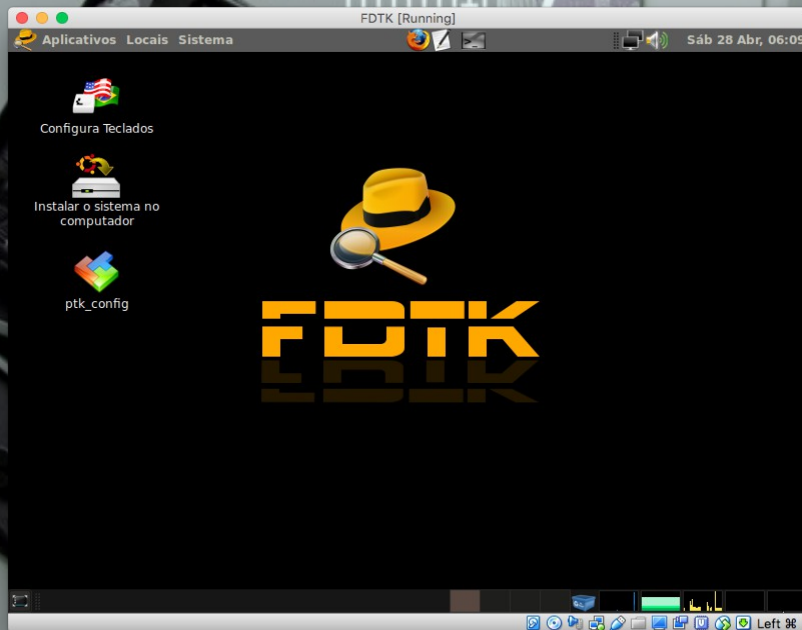
#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1



# Forense Computacional

## PeriBR



AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1



PeriBR



Instalar o sistema  
no computador



Teclado



Vídeo



# Forense Computacional

## SIFT (SANS Investigate Forensic Toolkit)



Applications Places System

SIFTWORKSTATION

- sansforensics's Home
- cases
- mount\_points
- VMware-Shared-Drive
- SIFT WORKSTATION README and TOOL LIST.pdf
- SIFT Workstation Cheat Sheet 1.5.pdf

PTK - Mozilla Firefox

http://localhost/ptk/index.php

SANS - Computer ... SANS Computer F...

PTK

Username: admin

Password: [masked]

Login

Done jSESSIONID=undefined FoxyProxy: Disabled

**SANS** COMPUTER FORENSICS  
and Incident Response with Rob Lee

# Forense Computacional

## DEFT (Digital Evidence & Forensic Toolkit)



AUGUST 3, 2013

#481920

LOG: 1

JULY 9, 2013

#453201

LOG: 1





# Forense Computacional

## CAINE (Computer Aided Investigative Environment)



AUGUST 3, 2013

#481920

LOG:2

JULY 9, 2013

#153201

LOG:1

Caine [Running]

QUANTUM

**CAINE**

Computer Aided INvestigative Environment

en 22.5 KiB/s 1.1 KiB/s Left 98

# Forense Computacional

## Autopsy



AUGUST 3, 2013

#481920

LOG: 2

JULY 9, 2013

#453201

LOG: 1

Big Ben - Autopsy 4.6.0

Case: Escolher Ferramentas Janela Ajuda

Add Data Source Images/Videos Timeline Generate Report Close Case

Show Rejected Results Listing Data Sources 1 Results

Name	Type	Size (Bytes)	Sector Size (Bytes)	MD5 Hash	Timezone	Device ID
Forense_Coleta_DS005_2018_FNS.dd	Image	500107862016	512		America/Sao_Paulo	c52448b5-a664-429c-abfb-1a5571

Hex Strings | File Metadata | Results | Message | Indexed Text | Media | Other Occurrences

Recent Activity for Forense\_Coleta\_DS005\_2018\_FNS.dd (Mais 2...) 202

# Autopsy<sup>®</sup>

OPEN | EXTENSIBLE | FAST

Carregando módulos de serviços...

# Forense Computacional

## IPED



Indexador e Processador de Evidências Digitais 3.15.6

A guarde, decodificando imagem E:\Forense\_Coleta.dd

Pré-visualizar caso    Pausar

Estatísticas:	
Tempo decorrido	0h 2m 42s
Término estimado	-
Velocidade média	0 GB/h
Velocidade atual	0 GB/h
Volume descoberto	0 MB
Volume processado	0 MB
Itens descobertos	0
Itens processados	0
Itens ativos processados	0
Subitens extraídos	0
Itens de carving	0
Carvings ignorados	0
Itens exportados	0
Itens ignorados	0
Erros de parsing	0
Erros de leitura	0
Timeouts	0

Tempos de execução por tarefa:	
IgnoreHardLinkTask	0s (0%)
TempFileTask	-
SignatureTask	0s (0%)
SetTypeTask	0s (0%)
SetCategoryTask	0s (0%)
RefineCategoryTask	0s (0%)
HashTask	0s (0%)
KFFTask	-
LedKFFTask	-
DuplicateTask	0s (0%)
ParsingTask	0s (0%)
RegexTask	0s (0%)
LanguageDetectTask	0s (0%)
NamedEntityTask	-
ExportFileTask	0s (0%)
MakePreviewTask	0s (0%)
ImageThumbTask	0s (0%)
VideoThumbTask	0s (0%)
DIETask	-
KFFCarveTask	-
CarveTask	0s (0%)
KnownMetCarveTask	0s (0%)
EntropyTask	0s (0%)
IndexTask	0s (0%)
ExportCSVTask	0s (0%)
HTMLReportTask	0s (0%)

Itens em processamento:	
Worker-0	Aguardando item...

Indexador e Processador de Evidências Digitais 3.15.6 [Caso: C:\IPED\Perda\_Total]

[Sem Filtro]    Filtrar Duplicados Listados    Pesquisar: [Digite ou escolha a expressão a ser pesquisada]    Opções    Ajuda    0 / 12298

Id	Score	Marcarador	Nome	Tipo	Tamanho (14...)	Deletado	Categoria
1	1%		SMIR		512	false	Outros Arquivos
2	1%		Unalloc_3_0_32256		32,256	true	Não Alocado
3	1%		SFAT1		3,139,584	false	Outros Arquivos
4	1%		SFAT2		3,139,584	false	Outros Arquivos
5	1%		2918063365piupsah sqLite-w...	sqLite...	0	true	Outros Arquivos   Tama...
6	1%		818200132aebmooount sqLite...	sqLite...	0	true	Outros Arquivos   Tama...
7	1%		places sqLite-wal	sqLite...	0	true	Outros Arquivos   Tama...
8	1%		update.test	test	0	true	Outros Arquivos   Tama...
9	1%		/		4,096	false	Pastas
10	1%		WINDOWS		4,096	false	Pastas
11	1%		system32		28,672	false	Pastas
12	1%		config		4,096	false	Pastas
13	1%		drivers		4,096	false	Pastas
14	1%		media		4,096	false	Pastas
15	1%		Fonts		12,288	false	Pastas
16	1%		bin		4,096	false	Pastas

Marcaradores    Item Pai    Duplicatas

Marcaradores

- [Sem Marcaradores]

O visualizador pode conter erros. Clique 2 vezes sobre o arquivo para abri-lo.    Fixar Visualizador

Hex    Texto    Metadados    Pré-visualização

### Ajuda

**Busca por Palavras-chave:**

Para realizar buscas por palavras-chave, execute a aplicação "IPED-SearchApp" na raiz da mídia óptica ou, em um terminal, execute o comando "java -Xms512M -jar indexador/lib/iped-search-app.jar". É necessário possuir instalado o Java JRE, preferencialmente de 64bits, disponível em [www.java.com](http://www.java.com). Ao realizar a busca diretamente a partir do disco óptico, as buscas podem ficar lentas. Para torná-las mais rápidas, copie todo o conteúdo do CD/DVD para uma pasta local do computador, a partir da qual o relatório deve ser acessado.

# Android

Em Julho de 2005 o Google comprou a Android, uma *startup* que fazia um pequeno sistema para celulares;

Em 5 de Novembro de 2007 o Google anunciou o nascimento do Android como uma plataforma e criou a *Open Handset Alliance (OHA)*.

AUGUST 3, 2013  
#481920  
LOG: 0

JUL 11, 2013  
#453201  
LOG: 1



# Android

AUGUST 3, 2013  
#481920  
LOG: 0



# Perícia Digital no Android

Preservação, aquisição, análise e apresentação.

Para quê? Investigação interna, criminais, litígios, segurança nacional, análise de malware.



# Perícia Digital no Android

Soluções comerciais:

Cellebrite;

X-Ray;

Oxygen;

ViaForensics.



All-inclusive Mobile Forensic Solution

New  
Platform



# Perícia Digital no Android

Mas tudo pode se resumir ao SDK!!!

```
root@forense: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@forense:~# adb shell
root@android:/ # mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /mnt/asec tmpfs rw,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,relatime,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
/dev/block/mtdblock1 /system yaffs2 ro,relatime 0 0
/dev/block/mtdblock5 /data yaffs2 rw,nosuid,nodev,relatime 0 0
/dev/block/mtdblock6 /persist yaffs2 rw,nosuid,nodev,relatime 0 0
/dev/block/mtdblock2 /cache yaffs2 rw,nosuid,nodev,relatime 0 0
/dev/block/vold/179:1 /mnt/sdcard vfat rw,dirsync,nosuid,nodev,noexec,relatime,uid=1000,gid=1015,fmask=0707,dmask=0707,allow_utime=0020,codepage=cp437,icharset=iso8859-1,shortname=mixed,utf8,errors=remount-ro 0 0
/dev/block/vold/179:1 /mnt/secure/asec vfat rw,dirsync,nosuid,nodev,noexec,relatime,uid=1000,gid=1015,fmask=0707,dmask=0707,allow_utime=0020,codepage=cp437,icharset=iso8859-1,shortname=mixed,utf8,errors=remount-ro 0 0
tmpfs /mnt/sdcard/.android_secure tmpfs ro,relatime,size=0k,mode=000 0 0
root@android:/ #
```

JULY 9, 2013  
#453201  
LOG: 1



# Perícia Digital no Android

## Evidências

Preferências compartilhadas: arquivos XML.

Armazenamento interno: arquivos criados pelo dispositivo, não acessível por nenhuma aplicação ou usuário, exceto root.

Armazenamento externo: cartão SD (FAT32).

SQLite: permite armazenar uma base de dados num único arquivo.

# Perícia Digital no Android

Informações \$ adb pull <arquivo>

Dados	Localização
Contatos	/data/data/com.android.providers.contacts/
Calendário	/data/data/com.android.providers.calendar/
SMS	/data/data/com.android.providers.telephony/
Downloads	/data/data/com.android.providers.downloads/
Dados do Browser	/data/data/com.android.providers.browser/
Gmail	/data/data/com.google.android.providers.gmail/
Cache de GeoLocalização	/data/data/com.google.android.location/

# Perícia Digital no Android

Aquisição Lógica

Acesso com root.

Modo Depuração USB.

Princípio de Locard.

Ferramentas: AFLogical OSE.

JULY 9, 2013  
#453201  
LOG: 1



AFLogical  
OSE

AFLogical OSE

Available providers:

- CallLog Calls
- Contacts Phones
- MMS
- MMSParts
- SMS

Select All

Deselect All

Capture

# Perícia Digital no Android

## Aquisição Física

dd:

```
$ dd if=/dev/mtd/mtd2 of=/sdcard/cache.img bs=2048
```

## Imagem NAND completa

nandump: file carving (scalpel), strings,  
editor hexa, sqlite, The Sleuth Kit  
(mactime)

# Perícia Digital no Android

ARE (Android Reverse Engineering)

OSAF (Open Source Android Forensics)

ViaExtract  
Santoku



# Perícia Digital no Android

## Avilla Forensics

The screenshot displays the Avilla Forensics 3.6 software interface. The main window is titled "Avilla Forensics 3.6 - ATTENTION: THIS TOOL IS FREE - Vesion 1\_0\_0\_295". The interface features a top toolbar with icons for various data sources (Android collections, iOS collections) and a central workspace. On the left, there is a sidebar with "Miscellaneous Tools" including icons for search, file operations, and communication. The central workspace shows a "NEW CASE" button and a large "Avilla FORENSICS" logo with a green Android robot character. Below the logo, the "Path of Acquisition" is set to "C:\Forensics-3-6\acquisitions\Case-10-11-2023-11-00-49". The bottom status bar indicates the software was developed by Daniel Hubscher Avilla in 2023 and provides contact information: [daniel.avilla@policiacivil.sp.gov.br](mailto:daniel.avilla@policiacivil.sp.gov.br), <https://www.linkedin.com/in/daniel-a-avilla-0987/>, and <https://www.avillaforensics.com.br>.

# O que mais?!

Meld / diff

Octave / Scilab

ImageJ / Fiji / Bio7

Praat

Audacity

OpenCV

R / R Studio

AUGUST 3, 2013  
#481920  
LOG: 0

JULY 9, 2013  
#453201  
LOG: 1



# Perguntas?! Cursos gratuitos

Pré-inscrição no curso EaD gratuito  
"Introdução à Forense Computacional"

<https://abre.ai/hfPz>

Pré-inscrição no curso EaD gratuito  
"Introdução à Forense Computacional em  
Dispositivos Móveis"

<https://abre.ai/hfPD>

[www.lamarca.eng.br](http://www.lamarca.eng.br)

AUGUST 3, 2013  
#481920  
LOG: 0

JULY 9, 2013  
#453201  
LOG: 1