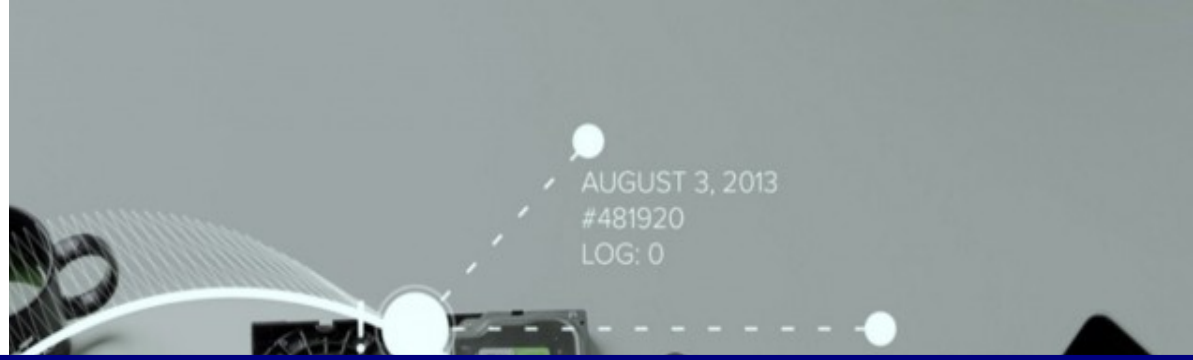


Forense Computacional com Software Livre: do desktop aos dispositivos móveis!

Palestrante:

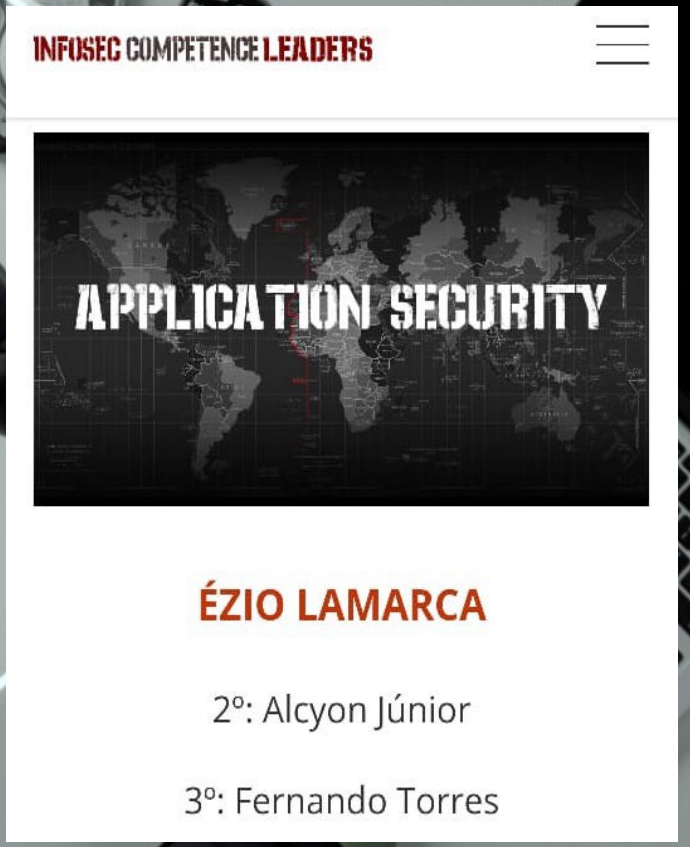
Eng. Ézyo Lamarca da Silva

5º CAFÉ

COM SOFTWARE LIVRE

11 DE NOVEMBRO

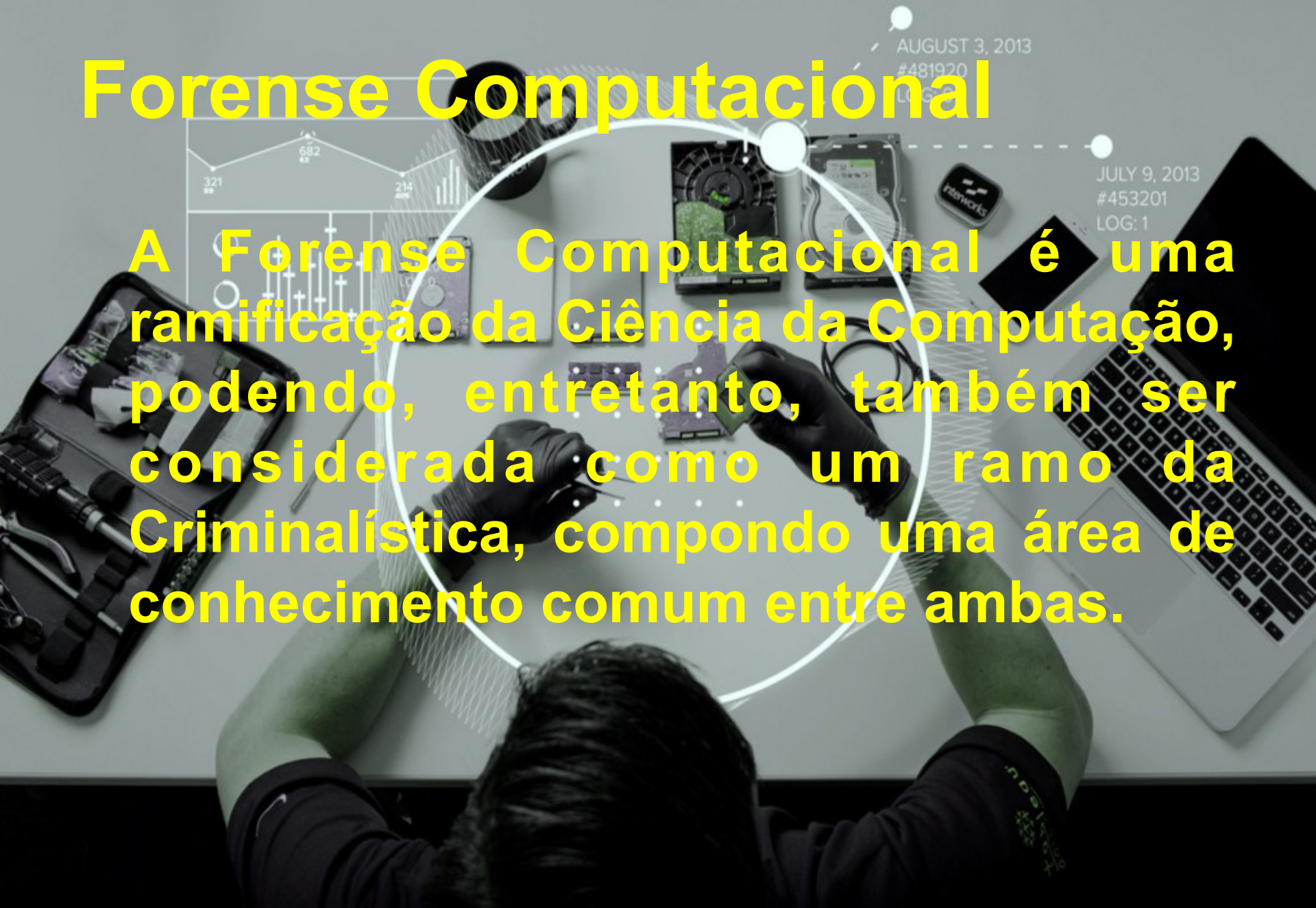
Ézyo Lamarca da Silva



Ézyo Lamarca da Silva

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 Correcional na Divisão de Investigação Correcional 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

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.

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.

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.

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.

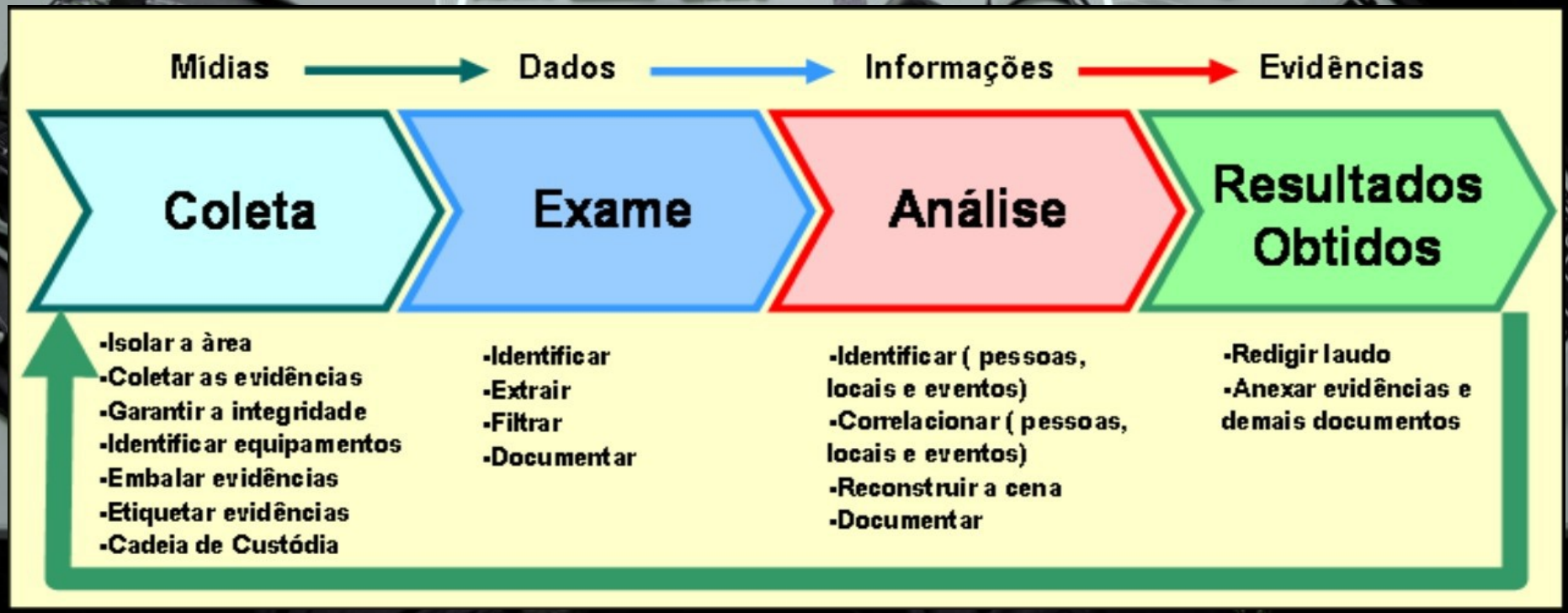
Forense Computacional

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



Forense Computacional

Software Livre

Fases	Descrição	FDTK
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

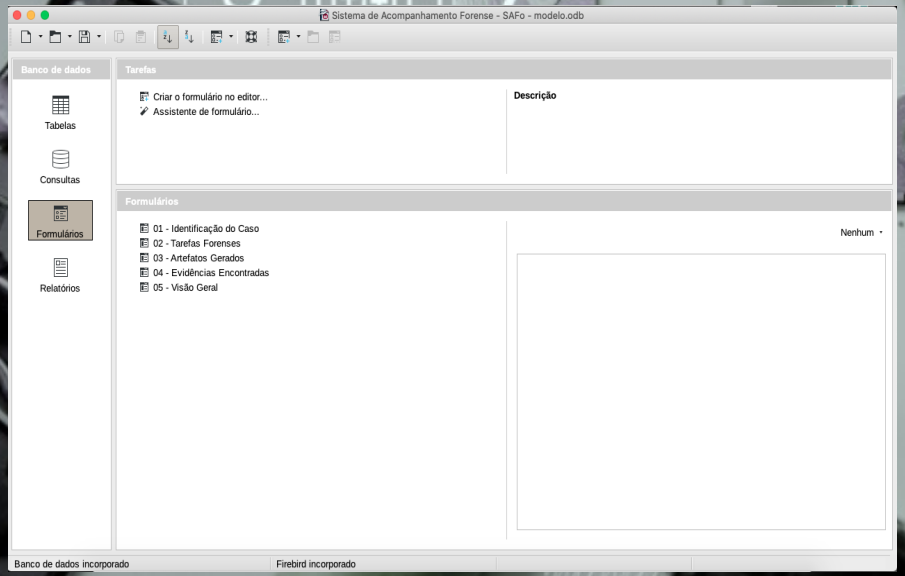
Forense Computacional

Software Livre

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
	Detecção 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

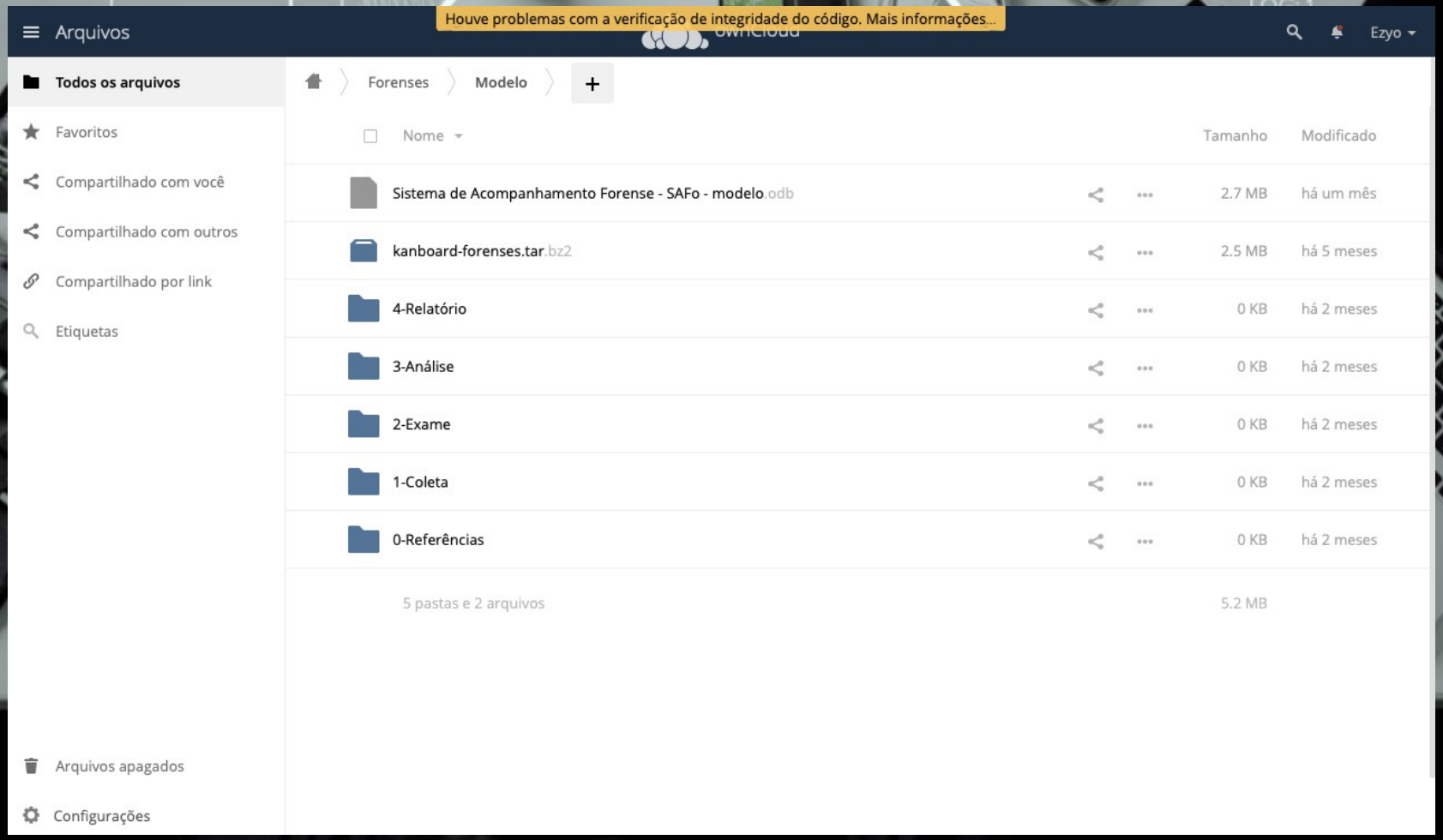


Forense Computacional

Kanboard

Forense Computacional

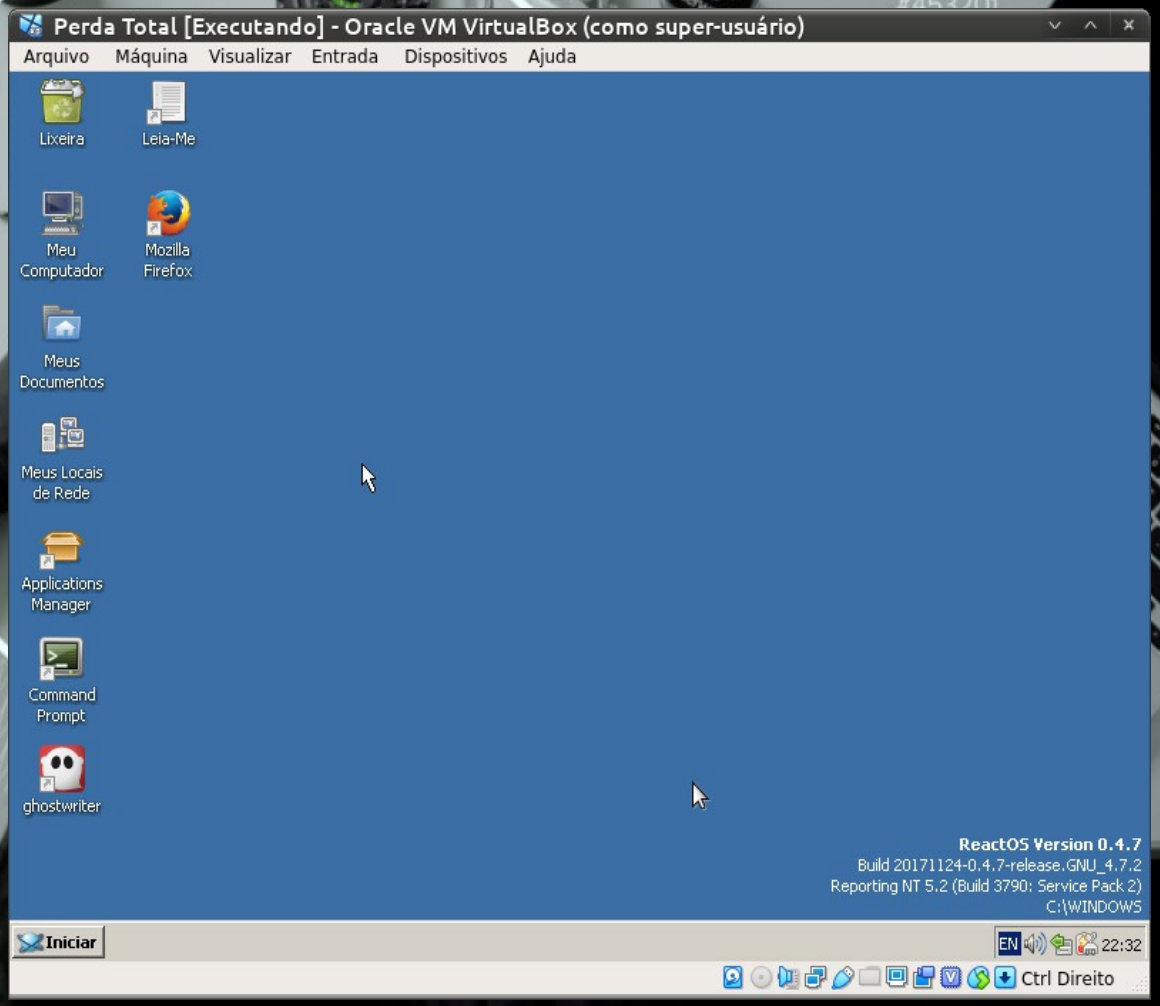
ownCloud



Forense Computacional

VirtualBox

- ReactOS



Forense Computacional

Comandos: mount, grep, strings

```
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/NOsT
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
```

timeline.csv - LibreOffice Calc

Arquivo Editar Exibir Inserir Formatar Estilos Planilha Dados Ferramentas Janela Ajuda

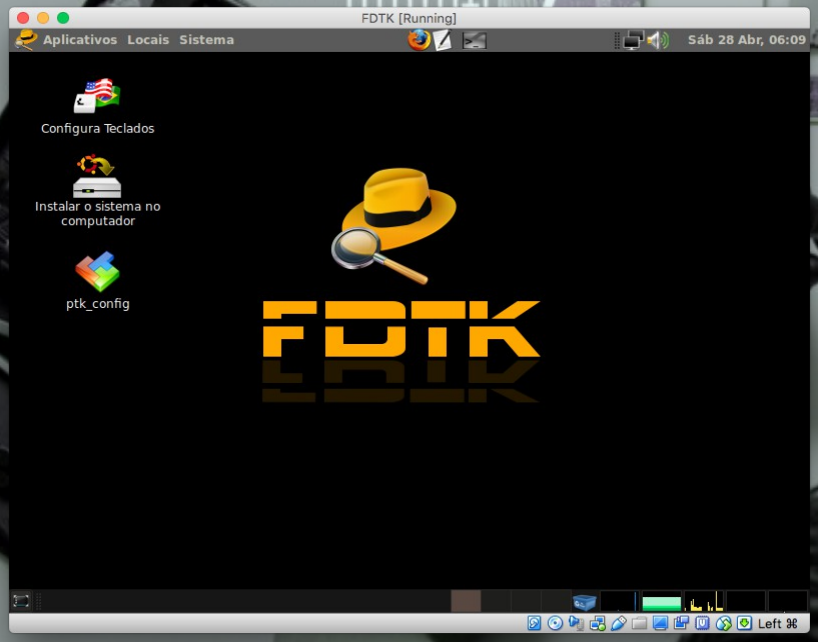
	A	B	C	D	E	F	G	H
6314	Sat Feb 10 2018 23:17:02	4257197	..b	r/rwxrwxrwx	0	0	37561114	/Arquivos de programas/7-Zip/_oneca.zip (deleted)
6315	Sat Feb 10 2018 23:17:12	4257197	m...	r/rwxrwxrwx	0	0	35945862	/RECYCLED/Dc0.zip
6316	Sun Feb 11 2018 00:00:00	736547	a...	r/rwxrwxrwx	0	0	33222409	/Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-back114947.jpg (deleted)
6317	Sun Feb 11 2018 00:00:00	1209051	a...	r/rwxrwxrwx	0	0	33222413	/Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)
6318	Sun Feb 11 2018 00:00:00	531424	a...	r/rwxrwxrwx	0	0	33222419	/Documents and Settings/Administrator/Meus Documentos/stockvault-art-and-nature89657.jpg
6319	Sun Feb 11 2018 00:00:00	4899755	a...	r/rwxrwxrwx	0	0	33222431	/Documents and Settings/Administrator/Meus Documentos/stockvault-artistic-nude111056.jpg
6320	Sun Feb 11 2018 00:00:00	1011257	a...	r/rwxrwxrwx	0	0	33222436	/Documents and Settings/Administrator/Meus Documentos/stockvault-close-up-nude-body-woman175094.jpg
6321	Sun Feb 11 2018 00:00:00	1869728	a...	r/rwxrwxrwx	0	0	33222441	/Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111901.jpg (deleted)
6322	Sun Feb 11 2018 00:00:00	1967942	a...	r/rwxrwxrwx	0	0	33222446	/Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111903.jpg (deleted)
6323	Sun Feb 11 2018 00:00:00	2431415	a...	r/rwxrwxrwx	0	0	33222451	/Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111904.jpg (deleted)
6324	Sun Feb 11 2018 00:00:00	28	a...	r/rwxrwxrwx	0	0	50179978	/Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.ini.lock (deleted)
6325	Sun Feb 11 2018 00:00:00	2302	a...	r/rwxrwxrwx	0	0	50179981	/Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.ini
6326	Sun Feb 11 2018 00:00:00	2302	a...	r/rwxrwxrwx	0	0	50179984	/Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.ini.mDR876 (deleted)
6327	Sun Feb 11 2018 00:00:00	21	a...	r/rwxrwxrwx	0	0	51168775	/Documents and Settings/Administrator/Meus Documentos/boneca/senha_boneca.txt (deleted)
6328	Sun Feb 11 2018 03:39:08	21	..b	r/rwxrwxrwx	0	0	51168775	/Documents and Settings/Administrator/Meus Documentos/boneca/senha_boneca.txt (deleted)
6329	Sun Feb 11 2018 03:40:24	21	m...	r/rwxrwxrwx	0	0	51168775	/Documents and Settings/Administrator/Meus Documentos/boneca/senha_boneca.txt (deleted)
6330	Sun Feb 11 2018 03:40:28	28	m..b	r/rwxrwxrwx	0	0	50179978	/Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.ini.lock (deleted)
6331	Sun Feb 11 2018 03:40:28	2302	m..b	r/rwxrwxrwx	0	0	50179981	/Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.ini
6332	Sun Feb 11 2018 03:40:28	2302	m..b	r/rwxrwxrwx	0	0	50179984	/Documents and Settings/Administrator/Dados de aplicativos/ghostwriter/ghostwriter.ini.mDR876 (deleted)
6333	Sun Feb 11 2018 03:41:24	1869728	m...	r/rwxrwxrwx	0	0	33222441	/Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111901.jpg (deleted)
6334	Sun Feb 11 2018 03:41:54	1209051	m...	r/rwxrwxrwx	0	0	33222413	/Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)
6335	Sun Feb 11 2018 03:42:14	736547	m...	r/rwxrwxrwx	0	0	33222409	/Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-back114947.jpg (deleted)
6336	Sun Feb 11 2018 03:44:30	736547	..b	r/rwxrwxrwx	0	0	33222409	/Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-back114947.jpg (deleted)
6337	Sun Feb 11 2018 03:44:30	1209051	..b	r/rwxrwxrwx	0	0	33222413	/Documents and Settings/Administrator/Meus Documentos/stockvault-baby-doll-front114945.jpg (deleted)
6338	Sun Feb 11 2018 03:44:32	1869728	..b	r/rwxrwxrwx	0	0	33222441	/Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111901.jpg (deleted)
6339	Sun Feb 11 2018 03:44:32	1967942	..b	r/rwxrwxrwx	0	0	33222446	/Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111903.jpg (deleted)
6340	Sun Feb 11 2018 03:44:34	2431415	..b	r/rwxrwxrwx	0	0	33222451	/Documents and Settings/Administrator/Meus Documentos/stockvault-plastic-doll-figure111904.jpg (deleted)
6341	Thu May 02 2019 00:00:00	12	a...	r/rwxrwxrwx	0	0	190	/WINDOWS/bootstat.dat
6342	Thu May 02 2019 00:00:00	155648	a...	r/rwxrwxrwx	0	0	33208491	/Documents and Settings/LocalService/ntuser.dat
6343	Thu May 02 2019 00:00:00	155648	a...	r/rwxrwxrwx	0	0	33220523	/Documents and Settings/Network Service/ntuser.dat

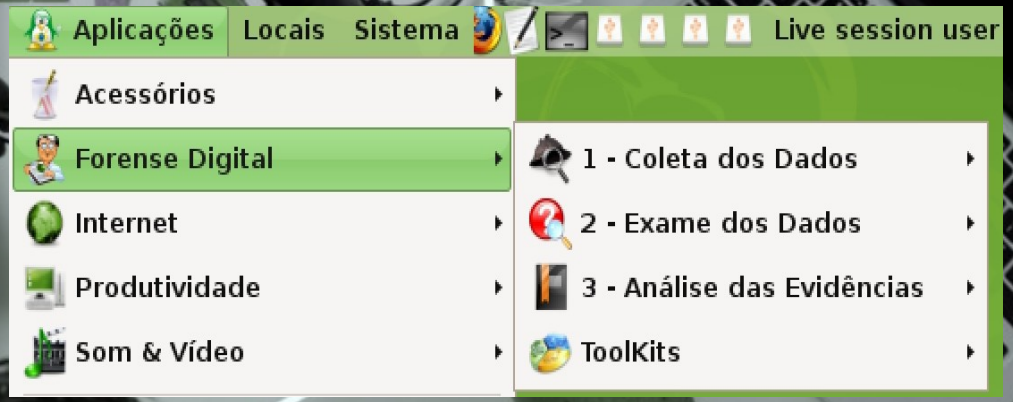
timeline

Planilha 1 de 1 | Padrão | Português (Brasil) | Média: ; Soma: 0 | 100%

Forense Computacional

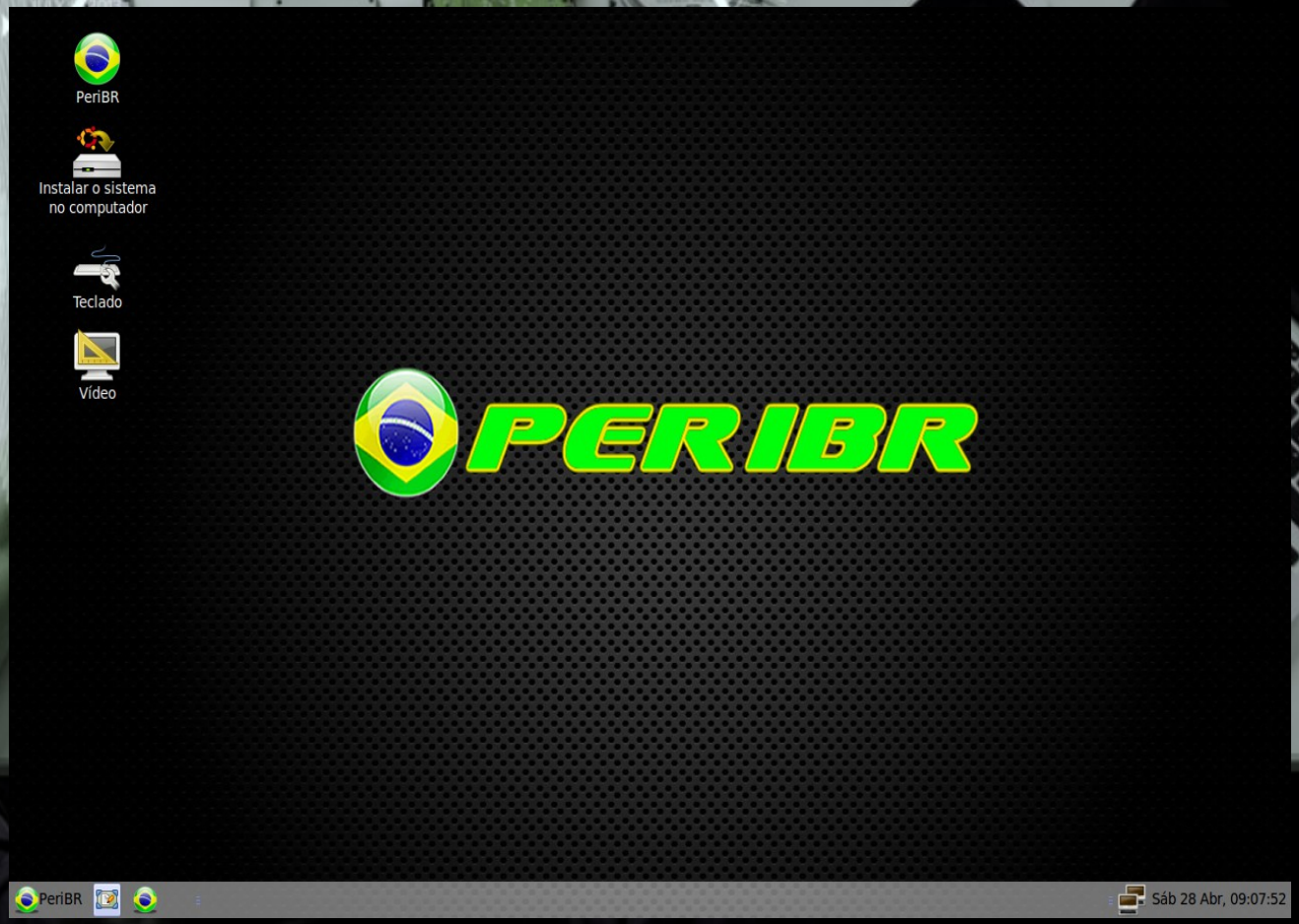
FDTK





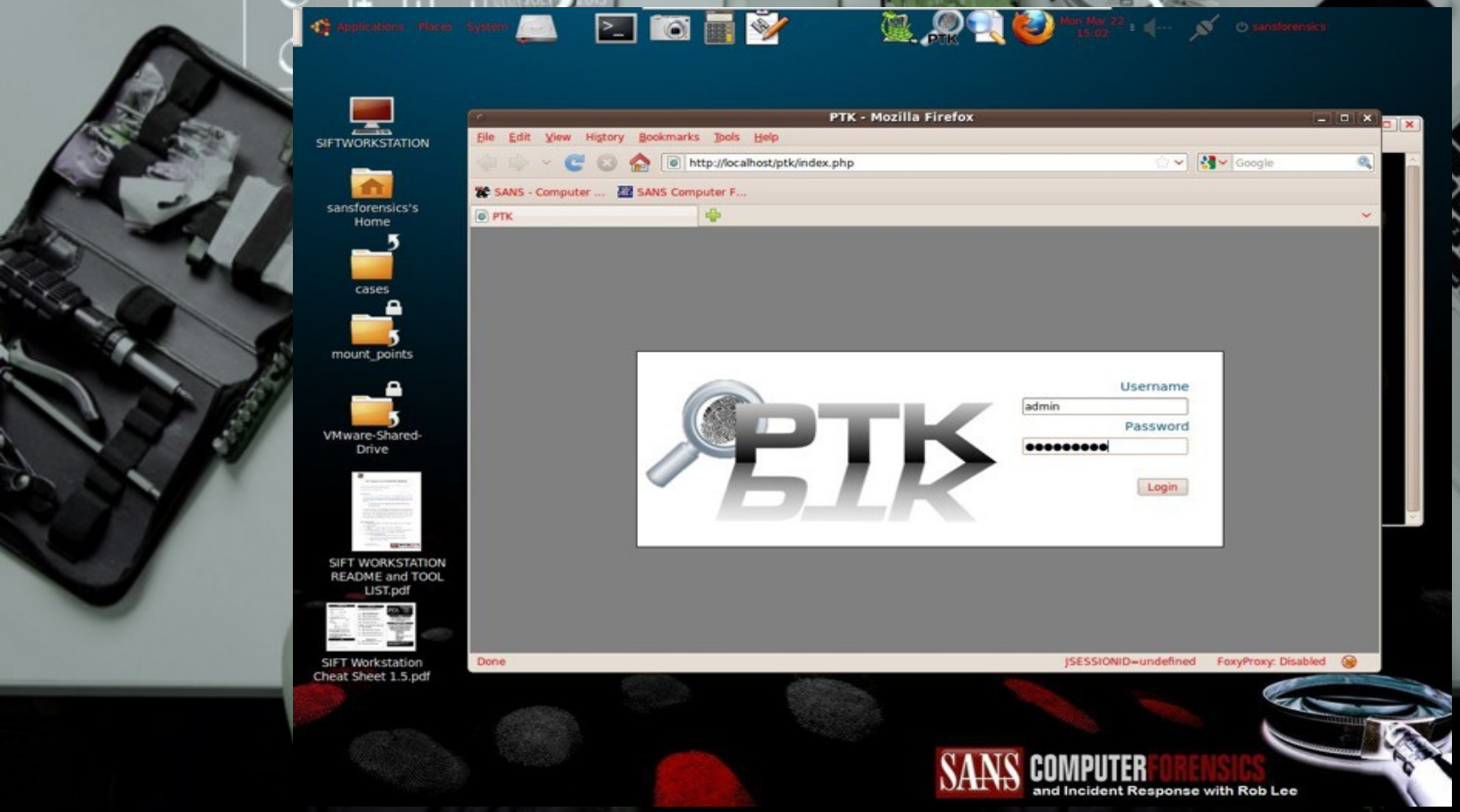
Forense Computacional

PeriBR



Forense Computacional

SIFT (SANS Investigate Forensic Toolkit)



Forense Computacional

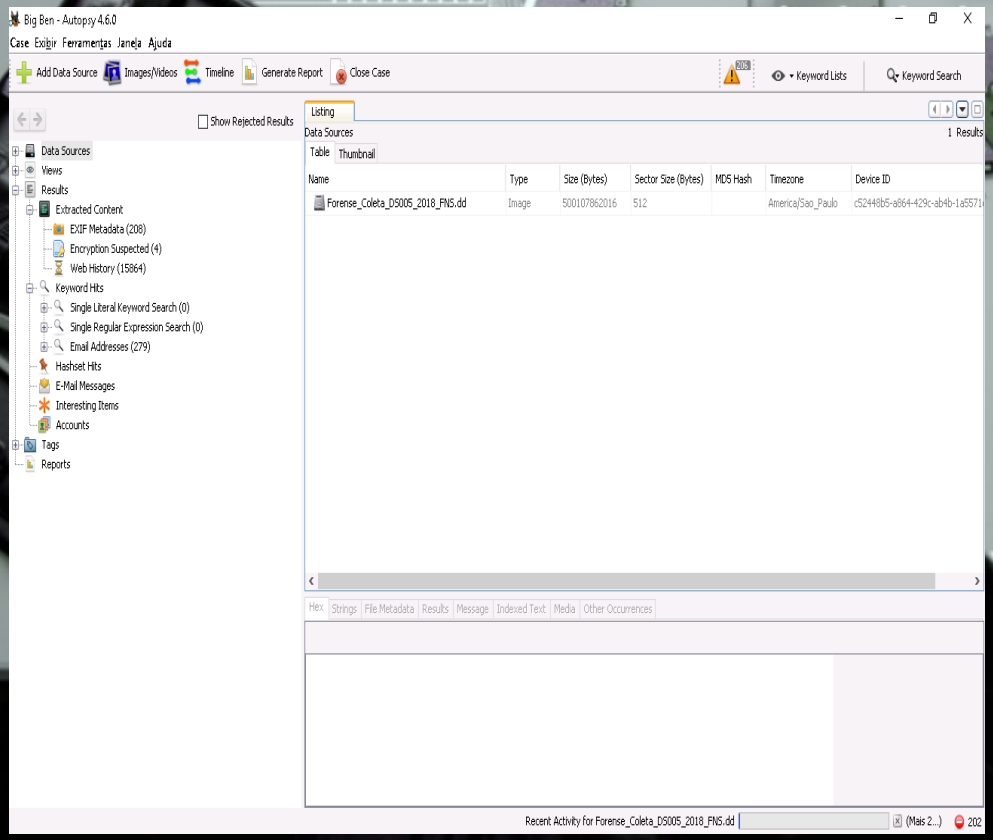
DEFT (Digital Evidence & Forensic Toolkit)

Forense Computacional

CAINE (Computer Aided Investigative Environment)

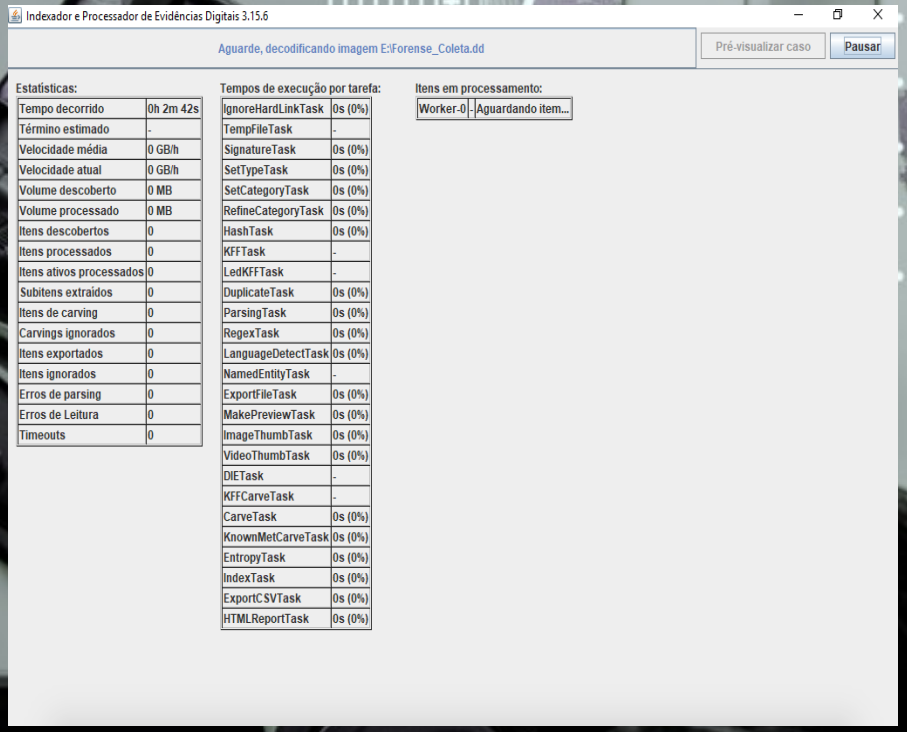
Forense Computacional

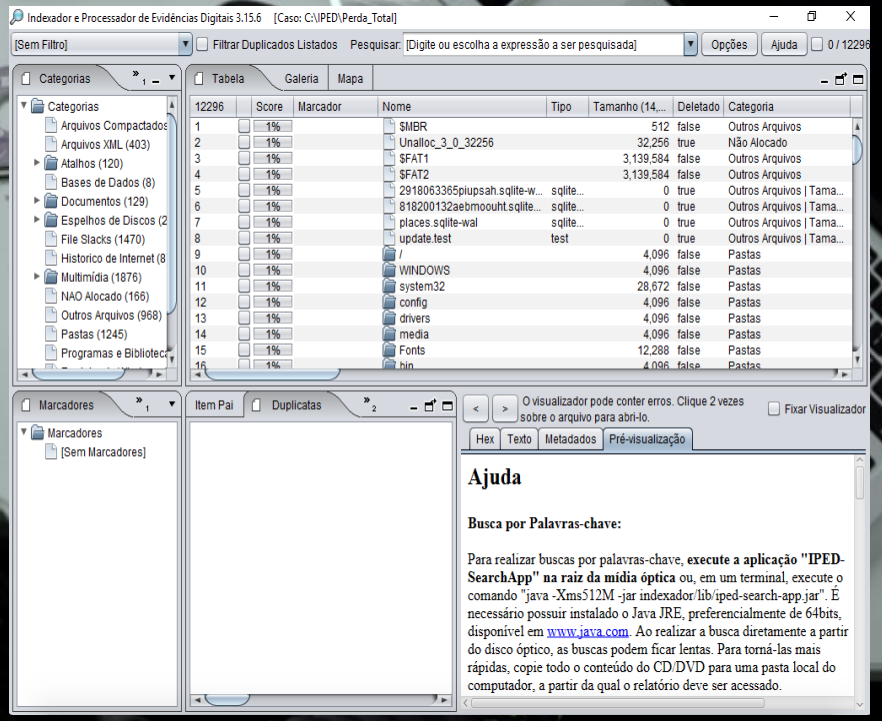
Autopsy



Forense Computacional

IPED

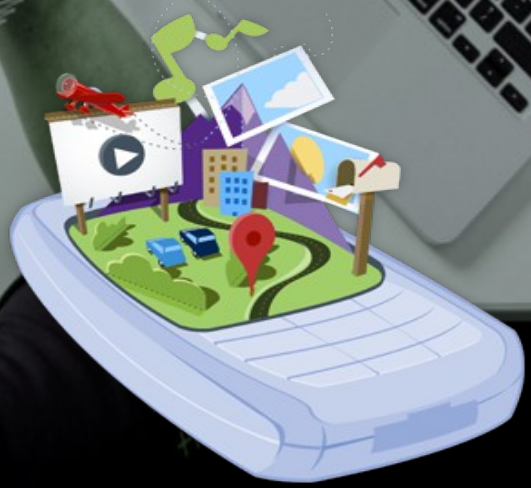




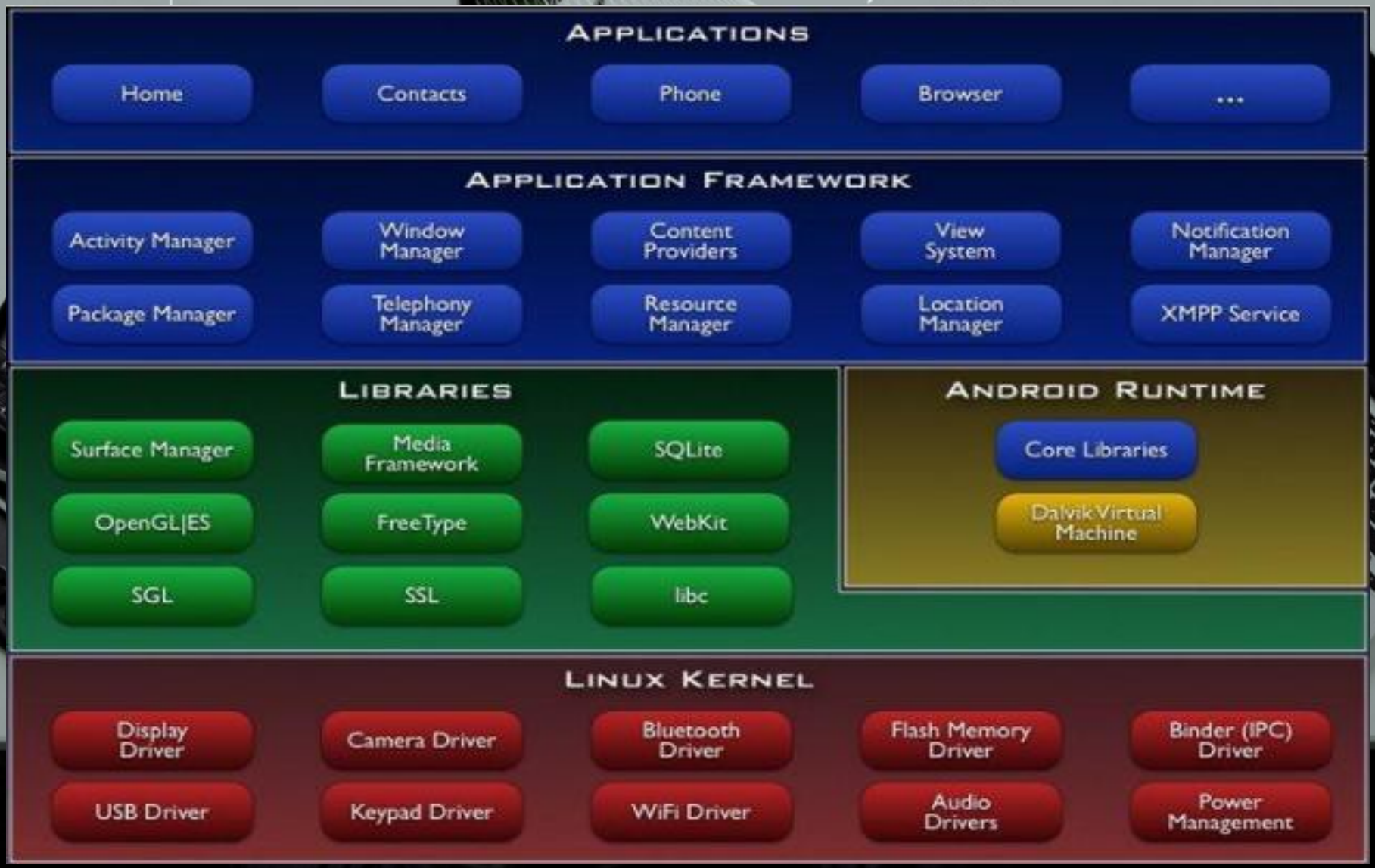
Android

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).



Android


Applications
Home
Contacts
Phone
Browser
...
Application Framework
Activity Manager
Window Manager
Content Providers
View System
Notification Manager
Package Manager
Telephony Manager
Resource Manager
Location Manager
XMPP Service
Libraries
Surface Manager
Media Framework
SQLite
OpenGL|ES
FreeType
WebKit
SGL
SSL
libc
Android Runtime
Core Libraries
Dalvik Virtual Machine
Linux Kernel
Display Driver
Camera Driver
Bluetooth Driver
Flash Memory Driver
Binder (IPC) Driver
USB Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

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;

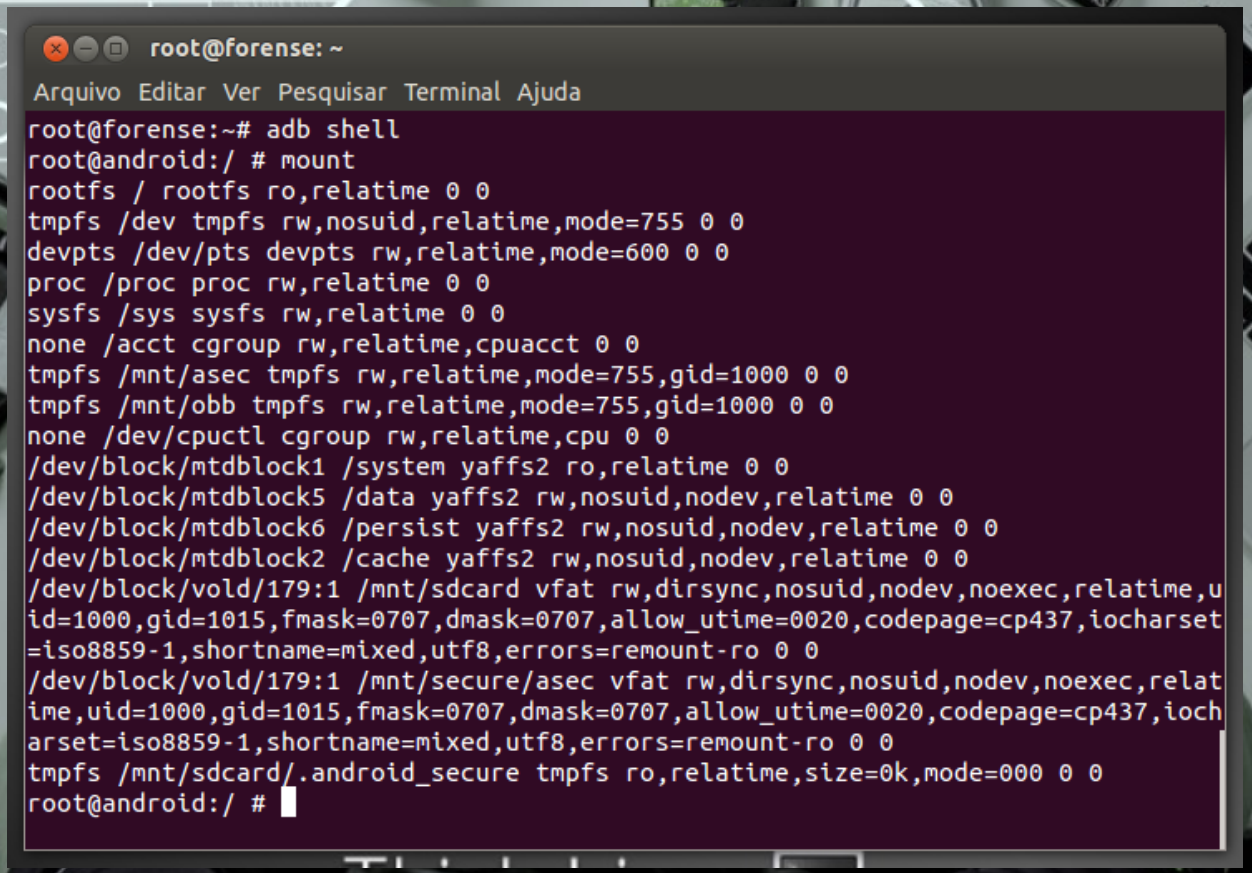
X-Ray;

Oxygen;

ViaForensics.

Perícia Digital no Android

Mas tudo pode se resumir ao SDK!!!



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.co**
Calendário	**/data/data/com.android.providers.calendar/**
SMS	**/data/data/com.android.providers.telephon**
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/ google.android.location/**

Perícia Digital no Android

Aquisição Lógica

Acesso com root.

Modo Depuração USB.

Principio de Locard.

Ferramentas: AFLogical OSE.

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

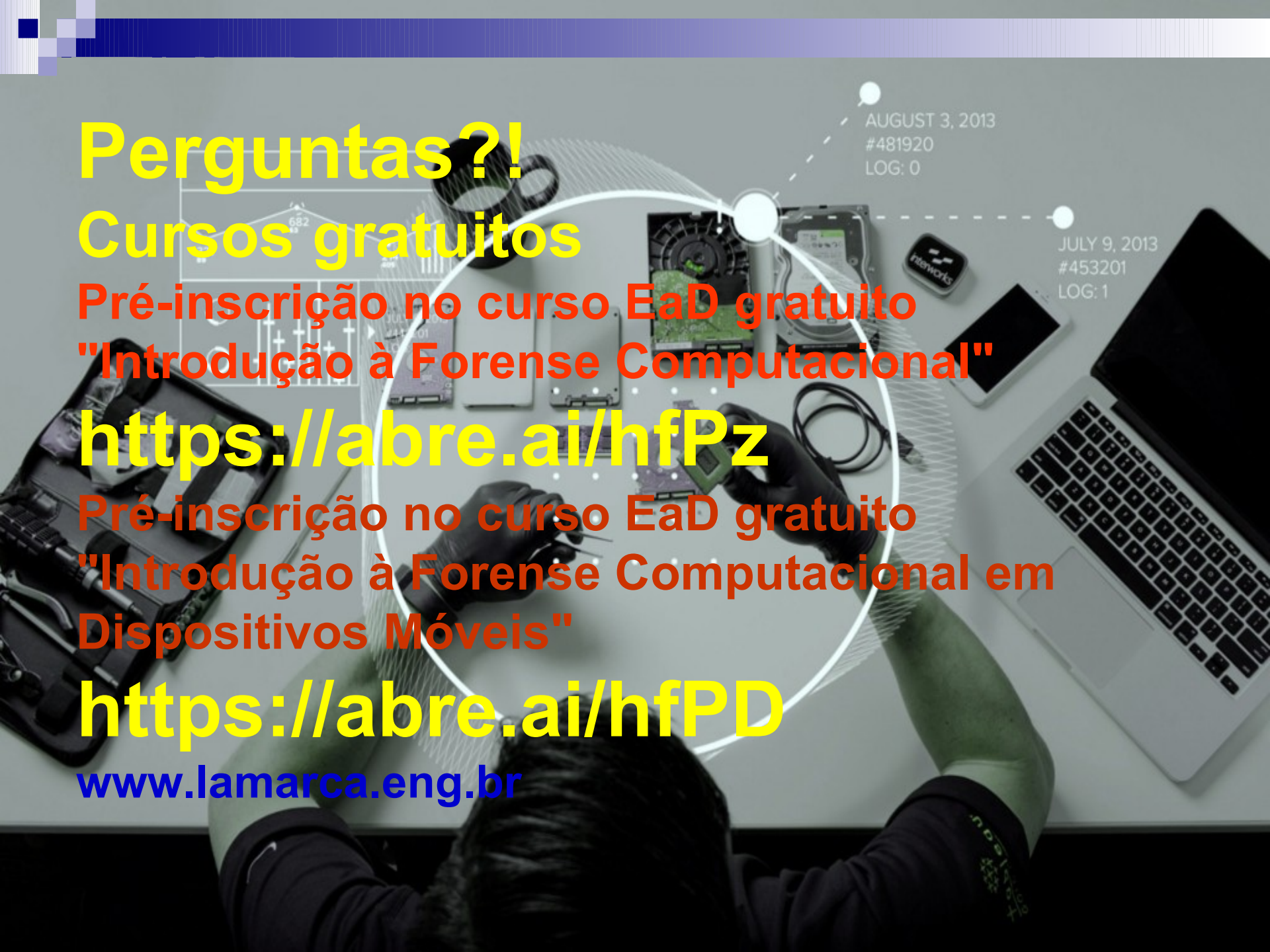
Santoku

Perícia Digital no Android

Avilla Forensics

O que mais?!

- Meld / diff
- Octave / Scilab
- ImageJ / Fiji / Bio7
- Praat
- Audacity
- OpenCV
- R / R Studio



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