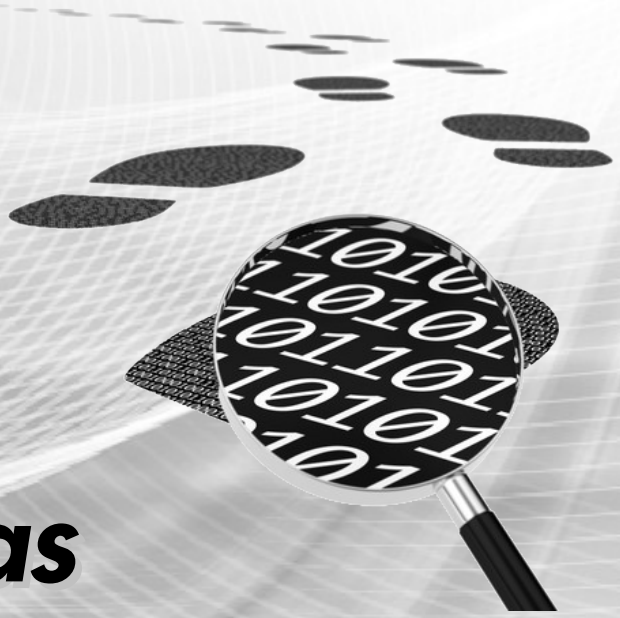
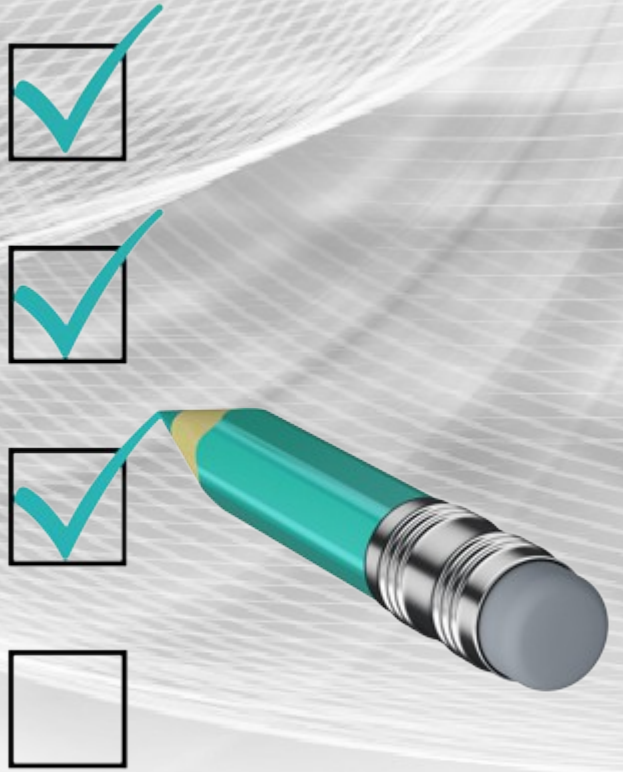


Novos Desafios das Perícias em Sistemas Computacionais

Ricardo Kléber

Roteiro desta apresentação

- A computação forense
- Cenários tradicionais
- Anti-forense computacional
- Novos desafios
- Cenas dos próximos capítulos



A Computação Forense

Ciências Forenses

- Definição
  - Aplicação das ciências físicas ao direito na busca da verdade em matérias cíveis, criminais, sociais e comportamentais a fim de que não sejam cometidas injustiças a nenhum membro da sociedade

- Objetivo
- Determinar o valor probatório da cena do crime e as evidências relacionadas

Computação Forense

- É um conjunto de procedimentos que envolve a preservação, identificação, extração, interpretação e documentação de evidências computacionais, utilizando metodologia adequada, obedecendo requisitos legais, zelando pela integridade, relatando com fidelidade as informações extraídas dos dados a partir de opiniões de especialistas em um tribunal e/ou em processos administrativos, com objetividade.

Computação Forense

- Perícia Forense Computacional
  - Forense Computacional
    - Forense em Informática
      - Forense Digital
        - Perícia Digital
          - Perícia em Informática
            - Perícia em Sistemas Computacionais
              - Perícia Cibernética
                - ~~Perícia Virtual~~ !?

Objetivos da Computação Forense

Em resumo...

- Recuperar, analisar e preservar computadores e materiais relacionados de tal forma que possam ser apresentados como provas em um tribunal de justiça.

- Identificar as evidências rapidamente, estimar o impacto potencial da atividade maliciosa na vítima, e avaliar a intenção e a identidade do agressor (ou coletar evidências que ajudem nesse objetivo).

Questões Legais

A Base para o Início

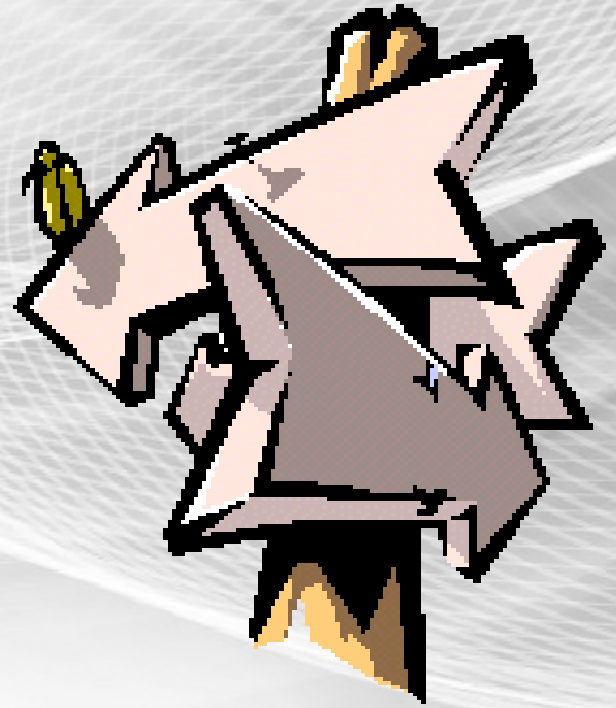
- Artigo 170: "Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas“.

- Artigo 171: "Nos crimes cometidos com destruição ou rompimento de obstáculo a subtração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado".

Computação Forense

Pontos Chave

- Aquisição
- Preservação
- Identificação
- Extração
- Recuperação
- Análise
- Apresentação (documentação)



Computação Forense

Termos Específicos Mais Relevantes

- Cadeia de Custódia
- Ordem de Volatilidade
- Perícia “In Loco” x “Post Mortem”
- Mídia de Origem x Mídia de Destino
- Assinatura Hash
- Duplicação Pericial
- Tipificação Específica ou por Analogia

Cenários Tradicionais

Cenários Tradicionais

Ferramentas e técnicas específicas para cada caso

- Dados Não-Voláteis
  - Mídias (discos rígidos, pendrives, cds/dvds, ...)
    - Duplicação + Hash + Extração + Recuperação
- Dados Voláteis
  - Memória
    - Dump de memória + File Carving
  - Tráfego de Rede
    - Grampo + Análise de Cabeçalhos + File Carving

Cenários Tradicionais

Mobile (um capítulo à parte)

Mobile Forensics "Tradicional"

- Cabos adequados (conexão para acesso aos dados)
- Conhecimentos sobre restrições de acesso ("rootear" / jailbreak / ...)
- Duplicação + Hash + Extração + Recuperação
  - Informações (tipo/localização/restrições) variam de acordo com aparelho/S.O.
  - Onde estão os dados "mais importantes" ???
  - Você tem, realmente, tempo para fazer dessa forma? Ou "é o jeito"?

Cenários Tradicionais

Mobile (um capítulo à parte)

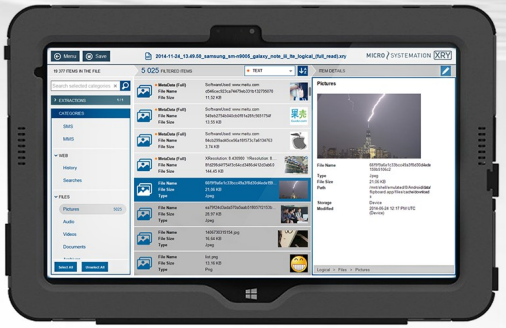
Mobile Forensics

- Soluções comerciais = pague e use :)

Mobile Forensics

Soluções Comerciais

.XRY



https://www.msab.com/products/

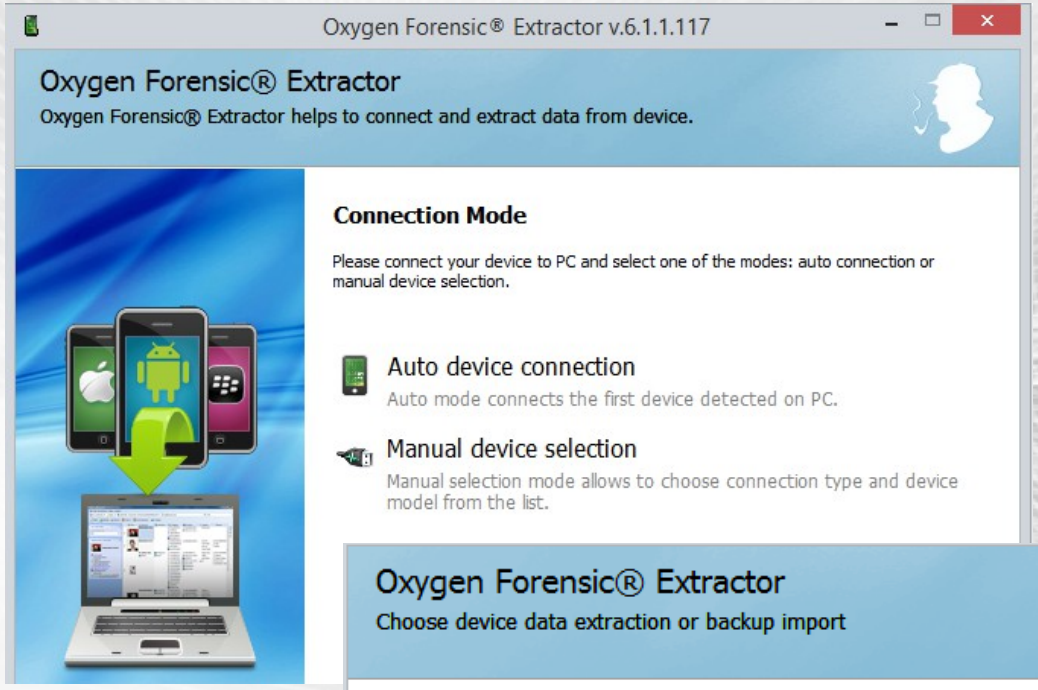
Mobile Forensics

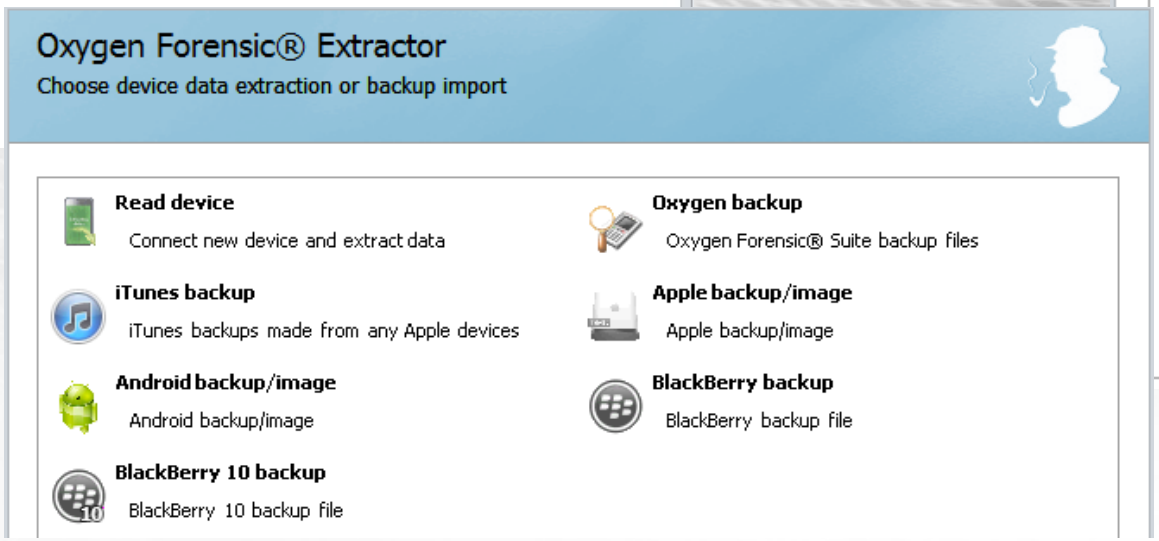
Soluções Comerciais

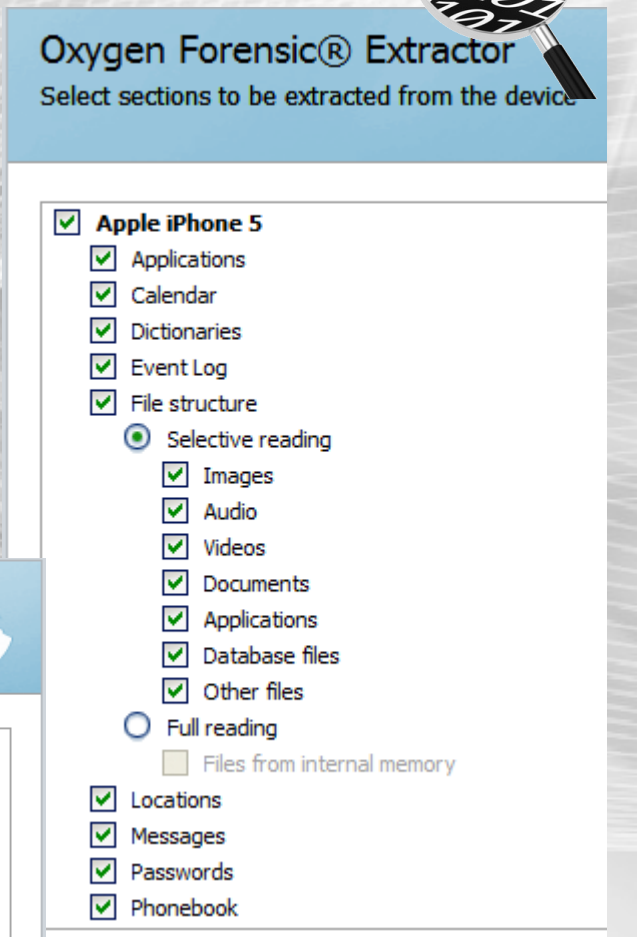
cellebrite
UFED

http://www.cellebrite.com/mobile-forensics

Mobile Forensics
Soluções Comerciais





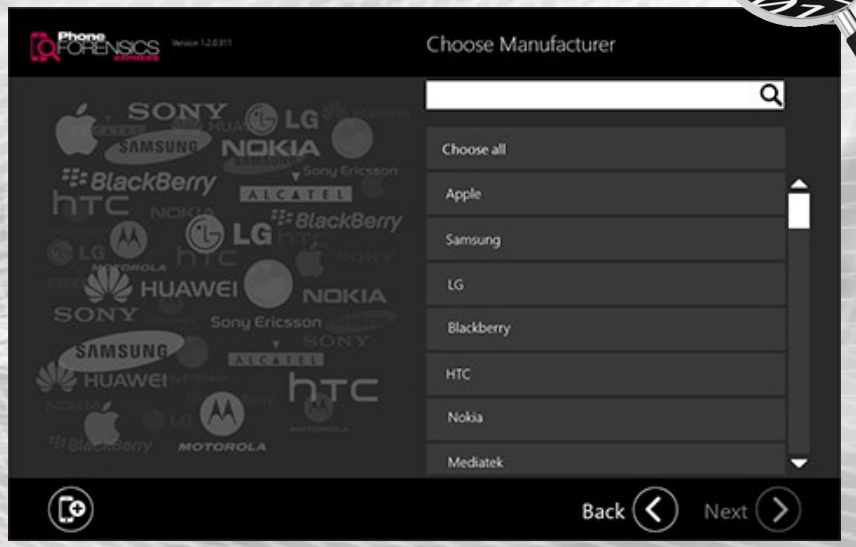


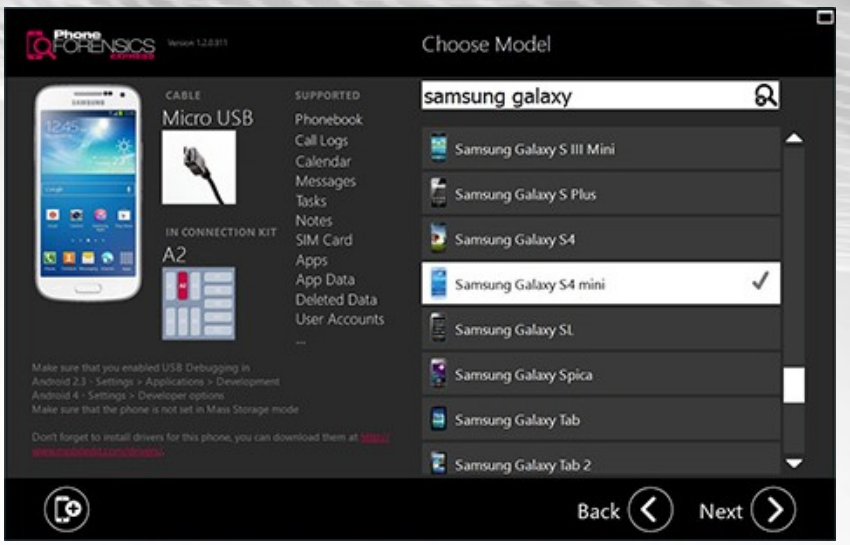
www.oxygen-forensic.com/en/products/oxygen-forensic-extractor/for-mobile-devices

Mobile Forensics

Soluções Comerciais

MOBILedit





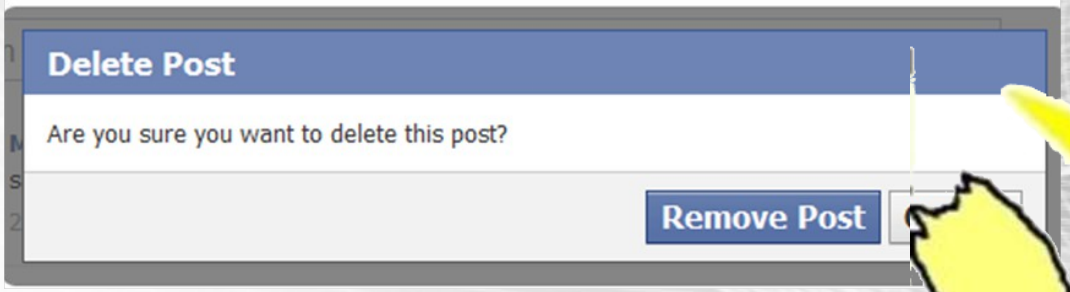
http://www.mobiledit.com/forensic

Anti Forense Computacional

Anti Forense Computacional

Técnicas que dificultam o trabalho pericial

Volatilidade



- Adequação e cooperação de provedores de conteúdo
- Ata Notarial (“assunto do momento”)

Anti Forense Computacional

Técnicas que dificultam o trabalho pericial

Criptografia

DATADEC online

	MD5 (AMD R9 290)				
	digitos	minúsculas	min + may	min + may + dig	min + may + dig + sim
1 caracter	0 seg	0 seg	0 seg	0 seg	0 seg
2 caracteres	0 seg	0 seg	0 seg	0 seg	0 seg
3 caracteres	0 seg	0 seg	0 seg	0 seg	0 seg
4 caracteres	0 seg	0 seg	0 seg	0 seg	0 seg
5 caracteres	0 seg	0 seg	0 seg	0 seg	1 seg
6 caracteres	0 seg	0 seg	3 seg	10 seg	2 min
7 caracteres	0 seg	2 seg	3 min	10 min	3 horas
8 caracteres	0 seg	39 seg	2 horas	10 horas	12 dias
9 caracteres	0 seg	15 min	5 dias	27 dias	3,3 años
10 caracteres	2 seg	7 horas	9 meses	4 años	> 10 años
11 caracteres	21 seg	7 dias	> 10 años	> 10 años	> 10 años
12 caracteres	3 min	6 meses	> 10 años	> 10 años	> 10 años
13 caracteres	31 min	> 10 años	> 10 años	> 10 años	> 10 años
14 caracteres	5 horas	> 10 años	> 10 años	> 10 años	> 10 años

Esterilização (Wipe)

```
# wipe -q /dev/sda1
```

```
# wipe -Q 1000 /dev/sda1
```

```
# wipe -rf /home/conta_criminosa/
```

USB Kill

http://github.com/hephaest0s/usbkill

- « usbkill » is an anti-forensic kill-switch that waits for a change on your USB ports and then immediately shuts down your computer.
- To run:
  - **sudo python usbkill.py**
- **--no-shut-down:** Execute all the (destructive) commands you defined in settings.ini, but don't turn off the computer.

Novos Desafios

Novos Desafios

DVRs (Sistemas de CFTV)

"Primeira" Geração

- Arquivos H.264/AVI
- Sist.Arquivos: FAT/NTFS/EXT3

- Extração Simples
- Recuperação (Carving)

Novos Desafios

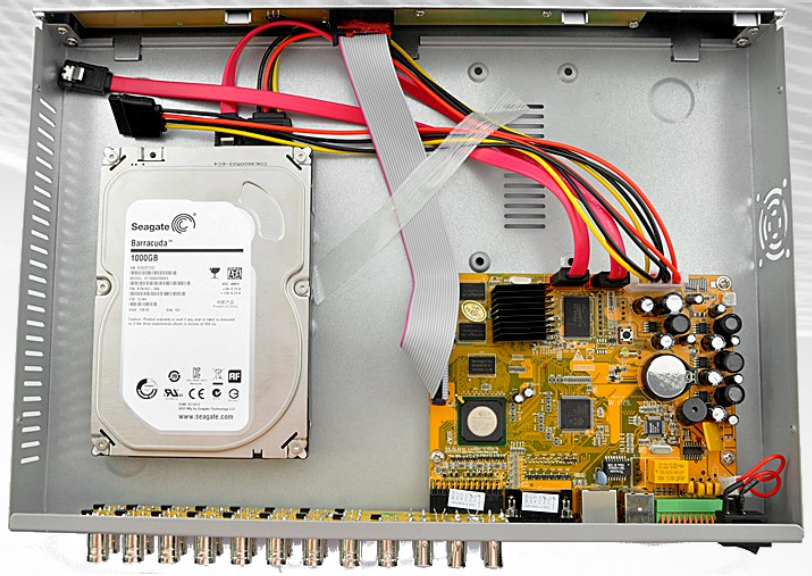
DVRs (Sistemas de CFTV)

"Nova" Geração

- Sistema Operacional (Embutido): Linux (modificado)
- Formato dos Vídeos: H.264
- Sistemas de Arquivos: DAHUA / MEIHDFS / DHFS / WFS

  (Surveillance video encrypted)

  - Procedimentos (Perícia Forense):
    - Duplicação do Disco Rígido
      - ~~Extração Simples~~
      - ~~Recuperação (Carving)~~



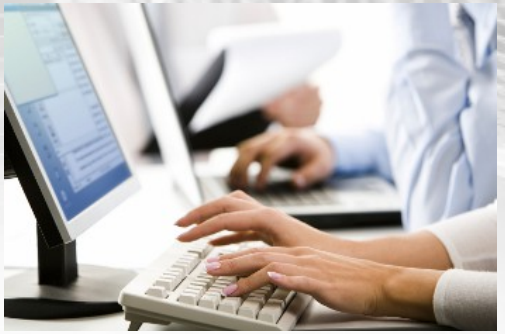
Novos Desafios

DVRs (Sistemas de CFTV)

"Nova" Geração

- Necessário conhecer:
  - Tipo de criptografia utilizada
  - Chave (sim, o padrão tem sido utilizar uma chave "mestra")
  - Métodos de identificação dos vídeos (formatos/cabeçalhos)

Arquivo de Imagem
(Disco do DVR)



Software Específico
- Script !?
- Framework !?
- Ferramentas tradicionais (atualizadas)!?

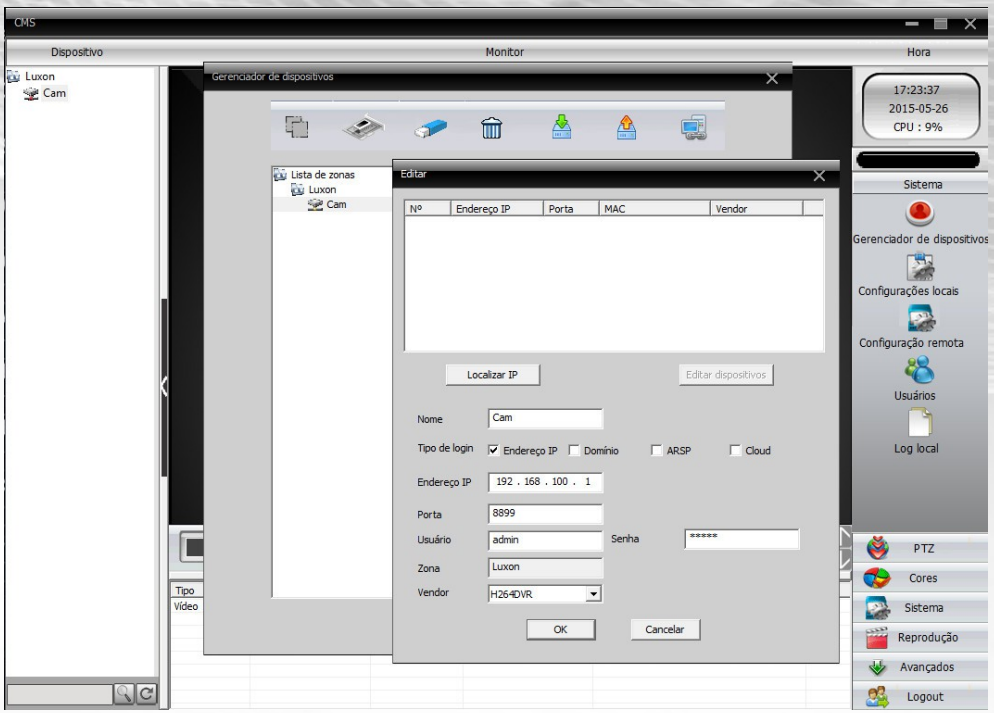
Vídeos
Extraídos/Recuperados

Novos Desafios

DVRs (Sistemas de CFTV)

"Nova" Geração

- Suporte dos fabricantes não ajuda
  - Oferece softwares para visualizar arquivos exportados a partir do próprio equipamento



Novos Desafios

DVRs (Sistemas de CFTV)

"Nova" Geração

- Soluções disponíveis para "fazer na unha"
  - Pioneer DVR Harddrive Recovery Tools
    - Mike Knoop
    - **http://mikeknoop.com/pioneer-dvr-harddrive-recovery-tools**
    - Scripts Python:
      - **Extract.py** – Extrai sequências MPEG de uma imagem de disco de um DVR Pioneer (modelos DVR-633H e DVR545H)
      - **Combine.py** – Concatena/combina múltiplos arquivos MPEG
      - **Split.py** – Divide (split) arquivos manualmente

https://code.google.com/p/pioneer-rec/

Novos Desafios

DVRs (Sistemas de CFTV)

"Nova" Geração

- Soluções disponíveis para "fazer na unha"
  - Projeto "ampliado" para mais modelos de DVRs
    - Stefan Haller
    - **https://github.com/haliner/dvr-recover**
    - Modelos PANASONIC
      - DMR-EH55 / DMR-EH56 / DMR-EH57 / DMR-EX77 / DMR-EX85 / DMR-XW300 / DVM-E80H
      - **python dvr-recover.py [parâmetros]**

https://code.google.com/p/panasonic-rec/

Novos Desafios

DVRs (Sistemas de CFTV)

"Nova" Geração

- Soluções comerciais = pague e use :)

Novos Desafios

DVRs (Sistemas de CFTV)

"Nova" Geração

- Soluções comerciais = pague e use :)
  - Huaxin Data Recovery (HX-Recovery for DVR)
  - Frombyte Recovery For DVR
  - **www.hxsjhf.com | www.frombyte.com/Recovery**
  - Windows XP, Windows 2000, Windows 2003, Windows 7, Windows 2008...
  - Opera diretamente sobre a imagem do disco do DVR
  - Suporte a: Dahua, DHFS v4.0 ou 4.1, WFS v 0.2, 0.3 ou 0.4
  - Extrai/Restaura e exporta em formatos H.264 ou AVI
  - U$ 680 (permanent version) | U$ 168 (one-time version)

Novos Desafios

DVRs (Sistemas de CFTV)

"Nova" Geração

- HX-Recovery for DVR

HX-Recovery for DVR(unregistered) V2.1

File About

Start Scan | Stop | Exit — New Task

Save Task | Load Task — Save&Load the Tast

Recover All | Recover Checked — Recovery

Check All | Reverse Check | Uncheck All — Select

Create Image — Image

F:\imagem_hd_dvr.dd
- 2015.02.03
- Unkown date
- 2015.02.06
- 2015.01.24
- 2015.01.25
- 2015.01.26
- 2015.01.27
- 2015.01.13
- 2015.01.28
- 2015.01.17
- 2015.01.29

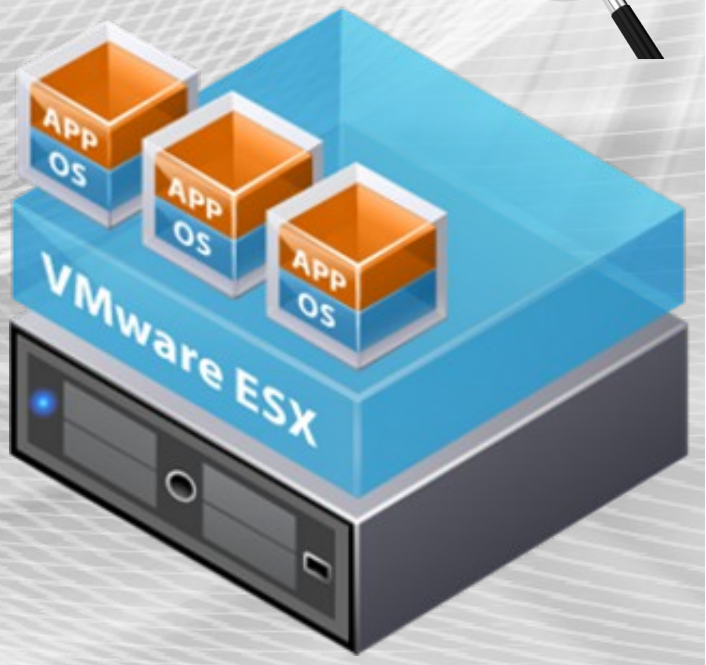
ID	Cam	Start date	End date	File size(MB)
1	0	2015.02.03 05.36.00	2015.02.03 05.59.59	4
2	0	2015.02.03 05.36.26	2015.02.03 05.59.59	80
3	0	2015.02.03 05.45.18	2015.02.03 05.59.59	50
4	0	2015.02.03 05.36.24	2015.02.03 05.59.59	80
5	0	2015.02.03 05.36.24	2015.02.03 05.59.59	80
6	0	2015.02.03 05.36.24	2015.02.03 05.59.59	82
7	0	2015.02.03 05.36.24	2015.02.03 05.59.59	80
8	0	2015.02.03 05.36.24	2015.02.03 05.59.59	80
9	0	2015.02.03 05.36.24	2015.02.03 05.59.59	82
10	0	2015.02.03 05.46.30	2015.02.03 05.59.59	46
11	0	2015.02.03 05.36.24	2015.02.03 05.59.59	82
12	0	2015.02.03 05.36.24	2015.02.03 05.59.59	82
13	0	2015.02.03 05.36.24	2015.02.03 05.59.59	82
14	0	2015.02.03 05.36.24	2015.02.03 05.59.59	234
15	0	2015.02.03 05.36.24	2015.02.03 06.00.00	230
16	0	2015.02.03 05.45.16	2015.02.03 05.59.59	52
17	0	2015.02.03 06.00.00	2015.02.03 06.59.59	10
18	0	2015.02.03 06.00.00	2015.02.03 06.59.59	202
19	0	2015.02.03 06.00.00	2015.02.03 06.59.59	204
20	0	2015.02.03 06.00.00	2015.02.03 06.59.59	206
21	0	2015.02.03 06.46.56	2015.02.03 06.59.59	46
22	0	2015.02.03 06.00.00	2015.02.03 06.59.59	202
23	0	2015.02.03 06.00.00	2015.02.03 06.59.59	606
24	0	2015.02.03 06.00.00	2015.02.03 06.59.59	204
25	0	2015.02.03 06.00.00	2015.02.03 06.59.59	208
26	0	2015.02.03 06.00.00	2015.02.03 06.59.59	206
27	0	2015.02.03 06.00.00	2015.02.03 06.59.59	206
28	0	2015.02.03 06.29.21	2015.02.03 06.59.59	106

Date	Information
20/03/2015 01:34:32	Scan type: Scan all space
20/03/2015	Scaning...

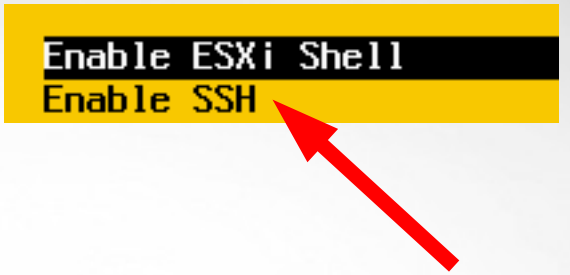
979842304/1953525168-27 总共发现2728个文件，大小为464,43GB

Servidor de Máquinas Virtuais

- O importante é não esquecer das “regras”
  - Não acessar diretamente a mídia original !!!
  - Acessar o (S.O. do) Servidor ESXi não altera dados das mídias originais (servidores virtuais)



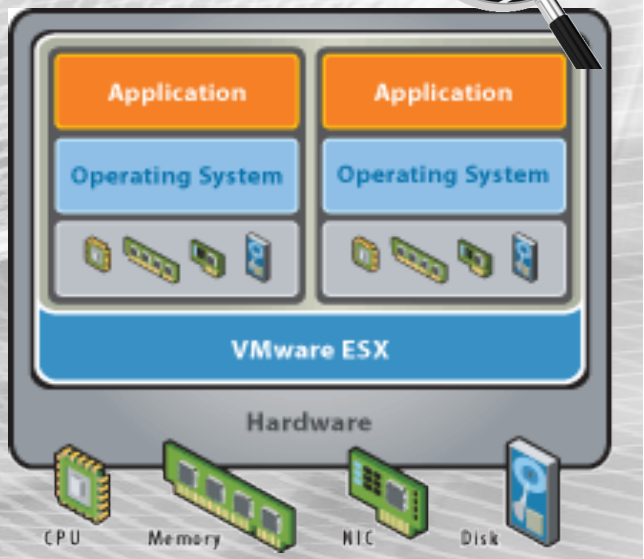
OU



Servidor de Máquinas Virtuais

- Procedimentos para cópia de evidências (Mvs)
  - Copiar arquivos de cada diretório (/vmfs/volumes/)
  - Calcular e registrar hashes → Cadeia de Custódia
  - Analisar informações de arquivos complementares
  - Manipular cópia do arquivo de imagem do disco (VMDK) normalmente
    - A imagem pode ser "montada" e analisada como um disco
      - Procedimentos de análise e extração simples
    - A imagem pode ser analisada diretamente (com ferramentas forenses)
      - Procedimentos de recuperação / carving de arquivos

Servidor de Máquinas Virtuais



- Arquivos relevantes:
  - **Nome_da_MV.vmx**
    - Arquivo de configuração principal da MV
    - Detalha componentes físicos e lógicos da MV
  - **Nome_da_MV.vmxf** :: Arquivo de configuração complementar
  - **Nome_da_MV.vmdk** :: Conteúdo (completo) dos discos da máquina virtual
  - **Nome_da_MV.vmsd** :: Informações e metadados da MV
  - **Nome_da_MV.nvram** :: BIOS da MV
  - **vmware(-*).log** :: Logs das atividades da MV

Novos Desafios
Máquinas Virtuais

- Exemplo de manipulação / análise de arquivos .VMDK:


```
/vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01

# du -khs /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/*

50.0G    /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/SRV_01-flat.vmdk
1.0M     /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/SRV_01.nvram
0        /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/SRV_01.vmdk
0        /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/SRV_01.vmsd
8.0K     /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/SRV_01.vmx
0        /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/SRV_01.vmxf
1.0M     /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/vmware-1.log
1.0M     /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_01/vmware.log

# fdisk -l SRV_01-flat.vmdk

Disk SRV_01-flat.vmdk: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders, total 104857600 sectors
Units = setores of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0001c5f4

Dispositivo       Boot      Start         End      Blocks   Id  System
SRV_01-flat.vmdk1   *        2048   100663295    50330624   83  Linux
SRV_01-flat.vmdk2       100665342   104855551     2095105    5  Estendida
SRV_01-flat.vmdk5       100665344   104855551     2095104   82  Linux swap / Solaris
```

Novos Desafios

Máquinas Virtuais

- Exemplo de manipulação / análise de arquivos .VMDK:


```
/vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_02

# du -khs /vmfs/volumes/5305c92a-d3816e70-b5f7-001a3fb1453a/SRV_02/*

1.8T /vmfs/volumes/5321a1c4-d93116e0-a6bc-001a3fb1453a/SRV_02/SRV_02-flat.vmdk
1.0M /vmfs/volumes/5321a1c4-d93116e0-a6bc-001a3fb1453a/SRV_02/SRV_02.nvram
0    /vmfs/volumes/5321a1c4-d93116e0-a6bc-001a3fb1453a/SRV_02/SRV_02.vmdk
0    /vmfs/volumes/5321a1c4-d93116e0-a6bc-001a3fb1453a/SRV_02/SRV_02.vmsd
8.0K /vmfs/volumes/5321a1c4-d93116e0-a6bc-001a3fb1453a/SRV_02/SRV_02.vmx
0    /vmfs/volumes/5321a1c4-d93116e0-a6bc-001a3fb1453a/SRV_02/SRV_02.vmxf
1.0M /vmfs/volumes/5321a1c4-d93116e0-a6bc-001a3fb1453a/SRV_02/vmware.log

# fdisk -l SRV_02-flat.vmdk

Disk SRV_02-flat.vmdk: 1979.1 GB, 1979120929792 bytes
255 heads, 63 sectors/track, 240614 cylinders, total 3865470566 sectors
Units = setores of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x9a3f5eb9512 bytes / 512 bytes
Disk identifier: 0x0001c5f4

Dispositivo       Boot      Start         End      Blocks   Id  System
SRV_02-flat.vmdk1   *        2048      206847      102400    7  HPFS/NTFS/exFAT
SRV_02-flat.vmdk2          206848   225279999   112536576    7  HPFS/NTFS/exFAT
SRV_02-flat.vmdk3       225280000  3865466879  1820093440    7  HPFS/NTFS/exFAT
```

Servidor de Máquinas Virtuais

- Soluções comerciais = pague e use :)

www.frombyte.com/Recovery/2012/1108/5.html

Cenas dos próximos capítulos

Cenas dos Próximos Capítulos

Ou não?

Cenas dos Próximos Capítulos

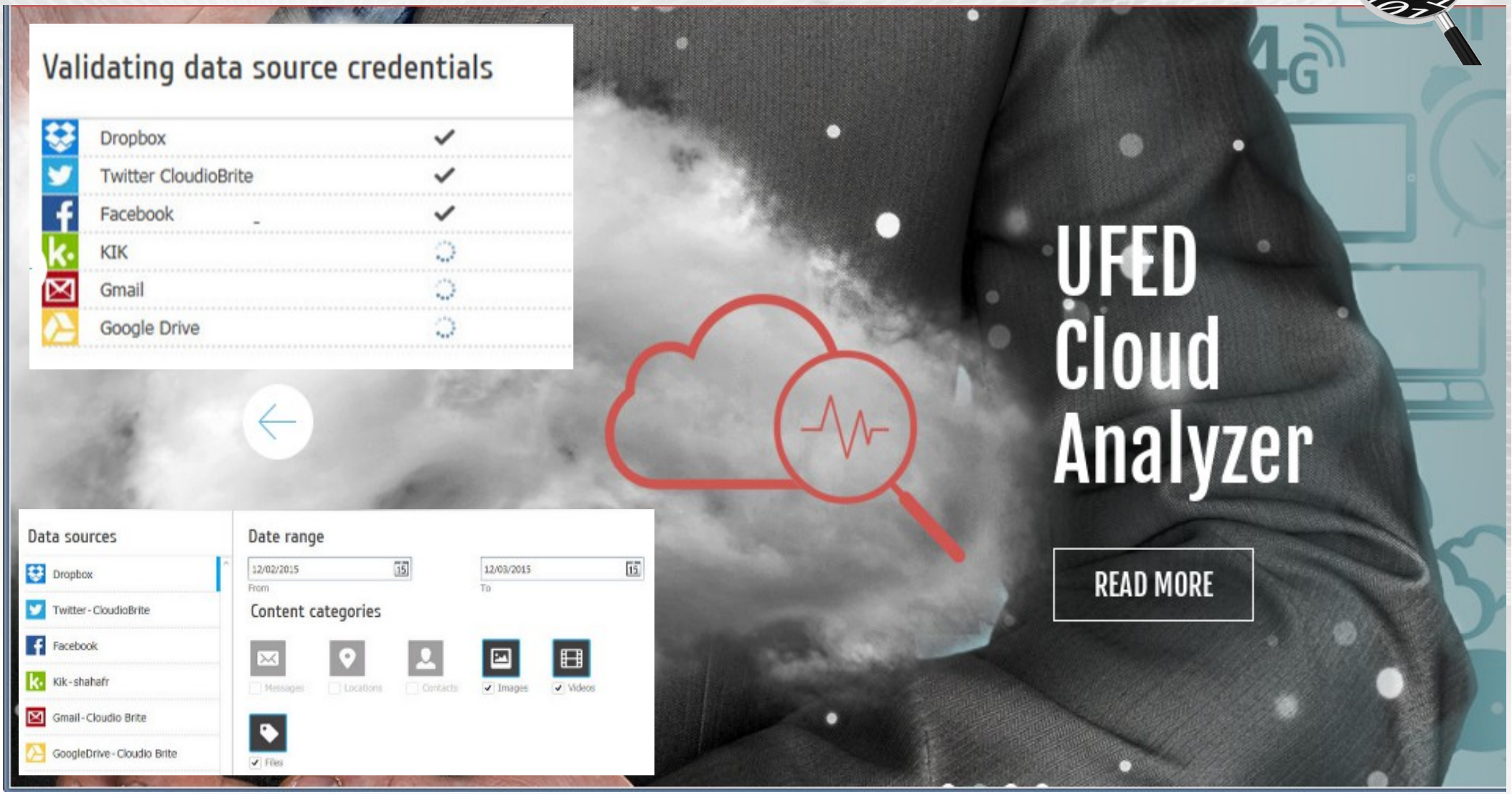
Ou não?

Computação Forense nas Nuvens

- Soluções comerciais = pague e use :)

Computação Forense nas Nuvens

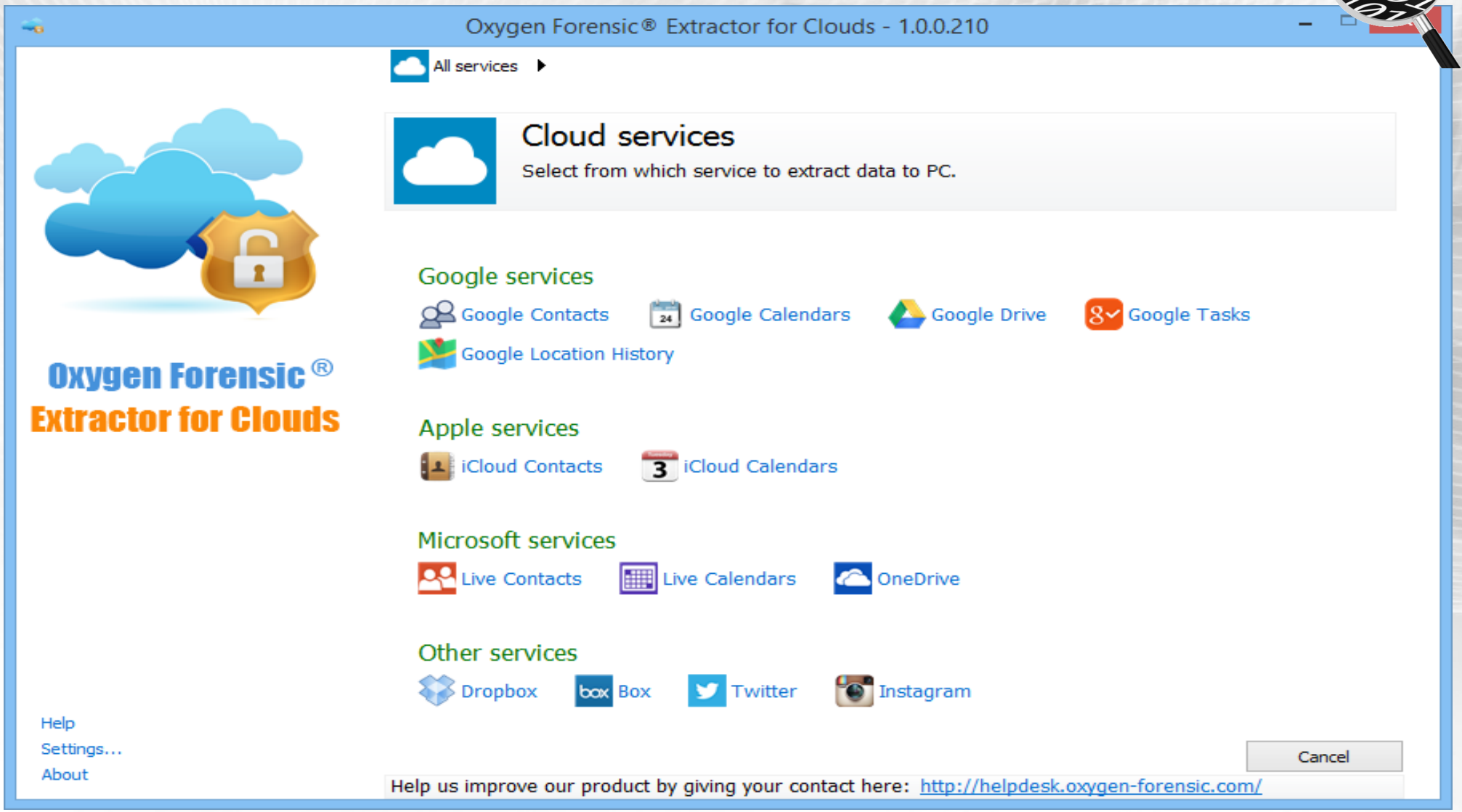
Soluções comerciais



www.cellebrite.com/mobile-forensics/applications/UFED-Cloud-Analyzer

Computação Forense nas Nuvens

Soluções comerciais



www.oxygen-forensic.com/en/products/oxygen-forensic-extractor/for-clouds

GTER 39 | GTS 25

Novos Desafios das Perícias em Sistemas Computacionais

ricardokleber@ricardokleber.com

@ricardokleber | @segurancaderede

www.segurancaderedes.com.br

www.youtube.com/segurancaderedes