

Índice

I.	Introdução a Computação Forense	
	a. Processo de investigação.....	
	b. Características de uma evidência.....	
II.	Manipulação de Evidências	
	a. Hashing de arquivos.....	
	b. Comparação de arquivos.....	
	c. Criação e montagem de imagens de discos.....	
	d. Preservação de disco.....	
	e. Hashing de diretórios.....	
	f. Comparação de diretórios.....	
III.	Busca de Diretórios	
	a. Visualização gráfica.....	
	b. Visualização em árvore.....	
	c. Filtragem por características.....	
	d. Busca de esteganografia.....	
IV.	Análise de Arquivos	
	a. Análise de meta-dados.....	
	b. Cabeçalhos hexadecimais.....	
V.	Auditoria no Windows.....	
	a. Averiguação de hardware.....	
	b. Análise manual do registro.....	
	c. Busca de evidências de uso.....	
	d. Análise de processos e tarefas.....	
VI.	Recuperação de Arquivos	
	a. Programas de recuperação.....	
	b. Suíte de análise.....	
VII.	Análise de Criptografia	
	a. Detecção de criptografia por padrão	
	b. Quebra de cifra de substituição.....	
	c. Análise e quebra de hash.....	
VIII.	Análise de Esteganografia	
	a. Análise por meta-dados.....	
	b. Busca por programas conhecidos.....	
	c. Detecção de alterações.....	
IX.	Quebra de Senhas	
	a. Métodos de ataque.....	
	b. Recuperação de senha de usuário.....	
	c. Criação de wordlists.....	
	d. Ataques de força bruta.....	
X.	Auditoria no Android	
	a. Auditoria do aparelho.....	
XI.	Busca Reversa	
	a. Busca utilizando critérios do Google.....	
	b. Busca por data.....	
	c. Busca de imagens.....	
	d. Busca de vídeos.....	

Prefácio

Olá! É com grande satisfação que apresento mais esse curso de computação feito pelo canal Fábrica de Noobs. Nesta apostila, abordaremos um tema de extrema importância no mundo atual, principalmente na área policial: a computação forense.

A computação forense pode ser definida pelo conjunto de práticas adotadas para a preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais que possuam validade em juízo.

Tais evidências podem ser úteis para o levantamento de provas a respeito da ocorrência ou não de crimes virtuais, e devem ser analisadas de acordo com procedimentos que impeçam a sua deterioração. A computação forense é útil na solução de crimes como invasões, fraudes financeiras, pornografia ilegal, quebra de direitos autorais, spam, cyberbulling, entre outros.

Este curso tem por objetivo apresentar de forma simples, informal e acessível os princípios da computação forense através de experiências práticas com programas do ramo. Não visa a formação profissional, mas sim a introdução de pessoas iniciantes e interessadas no ramo.

Todos os programas apresentados são relacionados a seus respectivos links de download e estão disponíveis em versão grátis (completa ou demo). Eles também podem ser encontrados na biblioteca do MEGA (<https://mega.nz#F!fQcV2IqR!e8iOoBMpVmitVq4ocajL4A>) e no pack que acompanha esta apostila.

Para melhor entendimento do curso, recomendo dispor de alguns materiais para serem usados como “cobaias” por você para testar as ferramentas apresentadas nele. Principalmente unidades de memória, como HD’s e cartões de memória. Caso esteja animado o bastante, vasculhar um lixo de uma loja de informática pode dar bons resultados.

Também é interessante (mas não obrigatório) possuir os cabos e conversores para a análise desses materiais. Um conjunto de cabos USB e um kit de conversão IDE/SATA deverá ser suficiente.



Dispondo ou não dos materiais adequados, é fundamental que você procure se aprofundar por conta nos tópicos apresentados, explorar outras ferramentas e testar recursos novos daquelas já apresentadas.

Espero que esse curso lhe traga uma experiência positiva e sirva para adquirir novos conhecimentos. Confira também as vídeo-aulas a serem gravadas no canal, e sinta-se livre para sugerir novos conteúdos.

I. Introdução à Computação Forense

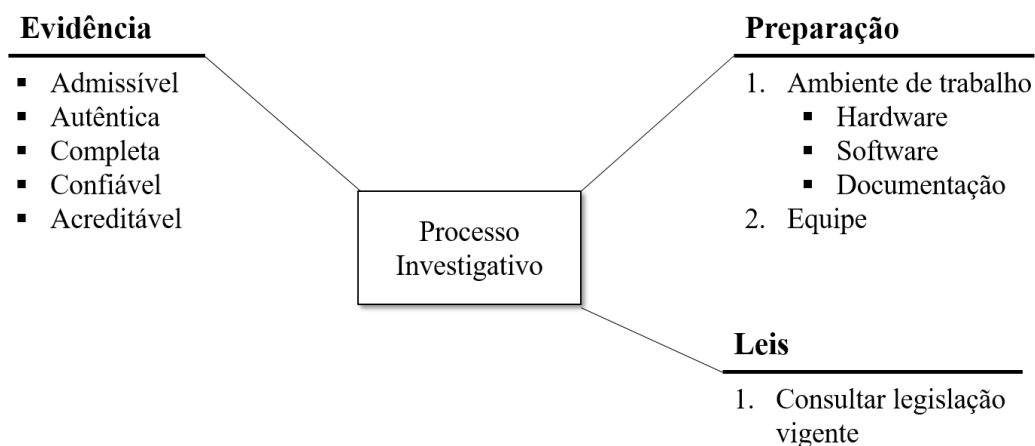
Passos Básicos

Identificação	{	1. Ocorrência do crime
		2. Identificação da cena do crime
Preservação	{	3. Autorização da investigação
		4. Busca por evidências
		5. Apreensão
		6. Transporte
Extração	{	7. Cópias
		8. Certificação de autenticidade
		9. Cadeia de custódia
		10. Armazenamento
Interpretação	{	11. Análise
Documentação	{	12. Relatório
Apresentação	{	13. Tribunal

O processo de investigação forense começa com a ocorrência de um crime e a constatação da existência de evidências digitais, como discos rígidos, computadores, unidades USB, celulares, entre outros.

Uma vez autorizado, deve-se inicia-lo a partir da busca e da apreensão de tais evidências, seguida pela produção de cópias das mesmas e autenticação, visando garantir a originalidade de tais cópias em relação à evidência original.

Após tais procedimentos, inicia-se a investigação em si, na qual as evidências devem ser analisadas utilizando uma gama de programas do gênero. Todas as descobertas feitas nessa fase devem ser registradas em um relatório, que será posteriormente apresentado em julgamento.

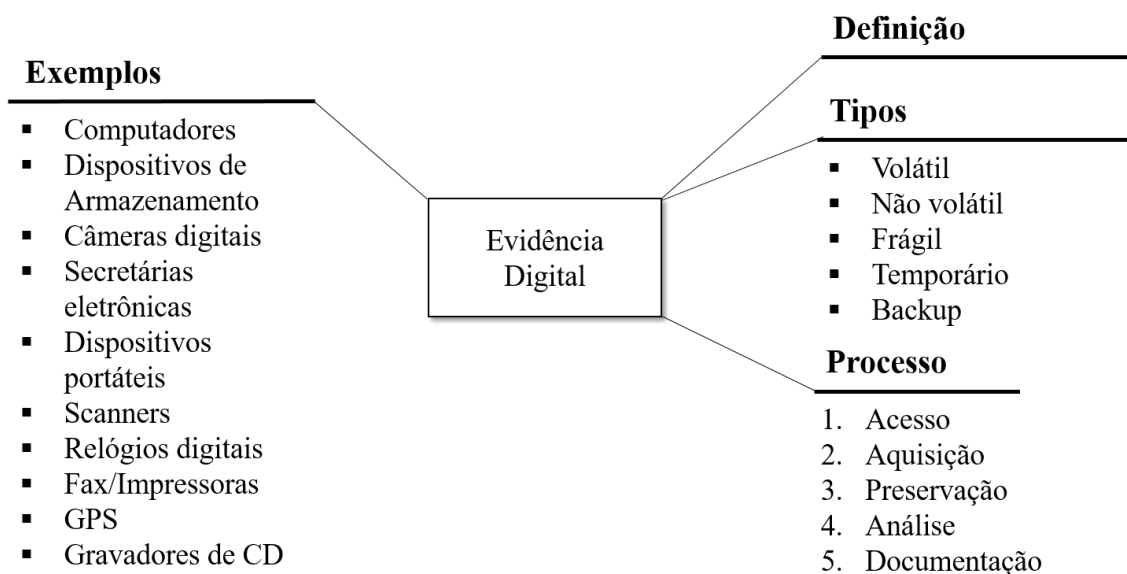


O processo de investigação envolve não só a análise das evidências, mas também a montagem de um ambiente de trabalho equipado com os recursos de software (programas de computação forense) e hardware (cabos e adaptadores) necessários para o caso.

Também é preciso definir se a investigação será feita individualmente ou em equipe, e a mesma deverá estar em conformidade com a legislação vigente.

Uma evidência deverá, obrigatoriamente, apresentar as seguintes características:

- **Admissível:** deverá reunir condições de ser apresentadas em um tribunal;
- **Completa:** não é suficiente coletar evidência que fornece apenas uma perspectiva do fato;
- **Autêntica:** evidências autênticas são aquelas que apresentam nexo de causalidade com o fato investigado de forma relevante;
- **Confiável:** os procedimentos de coleta e análise não devem causar dúvidas de sua autenticidade e veracidade;
- **Acreditável:** a evidência deve ser clara, fácil de entender e que faça com que um júri acredite nela.



Por definição, evidência digital é uma informação de valor probatório armazenada ou transmitida em formato digital e que pode ser utilizada em um processo judicial. Ela pode estar presente em quase todos os tipos de dispositivos eletrônicos, como mostra o diagrama acima;

Além disso, podemos classificá-las principalmente em função de sua volatilidade: quanto mais volátil uma evidência, maior a possibilidade de ser perdida ou alterada durante a investigação. Cache e memórias de curto prazo entram nessa categoria. Já discos rígidos e CD's são considerados evidências não-voláteis.

II. Manipulação de Evidências

Uma vez em posse da evidência, é necessário iniciar sua análise. Em uma investigação real, jamais deve-se realizar procedimentos na evidência original, mas sim em uma cópia bit-a-bit da mesma. Porém, antes de entender o procedimento de cópia, será necessário entender a autenticação das mesmas.

Vale ressaltar que o processo citado abaixo é absolutamente desnecessário em uma situação informal, como uma tentativa de recuperar arquivos deletados acidentalmente de um disco rígido.

É possível se certificar de que um arquivo é uma cópia exata de outro através da comparação de hash. Uma hash é uma sequência de caracteres que corresponde ao produto da inserção do arquivo sobre um algoritmo. Dessa forma, se apenas um bit for alterado do arquivo original, a hash resultante será diferente.

Caso queira estudar mais sobre funções hash, recomendo assistir ao seguinte vídeo <https://www.youtube.com/watch?v=ZTJEWeWRUkc>.

Podemos comparar hashes de arquivos utilizando o [QuickHash-Windows-v2.6.9.2](https://sourceforge.net/projects/quickhash/?source=typ_redirect), que pode ser baixado de forma gratuita em https://sourceforge.net/projects/quickhash/?source=typ_redirect.








A hash de um arquivo pode ser obtida na aba **File**. Basta escolher o algoritmo desejado e observar sua hash correspondente.

The screenshot displays the QuickHash-Windows-v2.6.9.2 application window. The 'File' tab is selected in the top menu bar. On the left, under 'Hash Algorithm', the 'MD5' radio button is selected. The main area, titled 'Single File Hashing', shows a 'Select File' button, the status 'Complete.', and the start time 'Started at : 24/09/16 14:32:36'. Below this, it indicates '(or "drag and drop" a file here)' and shows the time taken as 'Time taken : 00:00:00'. The file path 'C:\Users\Natanael\Desktop\A Cyberpunk Manifesto.docx' is displayed in a text box. Below the file path, the computed MD5 hash 'ABE69AD521DC20E462610DDEC6CB281' is shown in a larger text box. At the bottom, there is a field for 'Expected Hash Value (paste from other utility)' which is currently empty, and a status bar at the very bottom that reads 'RECOMPUTED NEW HASH VALUE.'

É possível também obter a hash de todos os arquivos presentes em um diretório utilizando a aba **FileS**, com funcionamento de forma semelhante.

C:\Users\Natanael\Desktop\Arquivos				
	File Name	Path	Hash Value	File Size (on Disk)
1	Redes da Deep Web - Freenet.pdf	C:\Users\Natanael\Desktop\Arquivos\	2E2B5ED23A3025641A58C839964B1A44	359816 bytes (351,38 KiB)
2	Redes da Deep Web - Galet.pdf	C:\Users\Natanael\Desktop\Arquivos\	684B6606ADD4ECB0C6EA31F2B96E0E8	304059 bytes (296,93 KiB)
3	Redes da Deep Web - Globaleaks.pdf	C:\Users\Natanael\Desktop\Arquivos\	53B13D6CF29608F399F96124EC7D4879	742402 bytes (725 KiB)
4	Redes da Deep Web - Hyperboria.pdf	C:\Users\Natanael\Desktop\Arquivos\	C622160E4362ED987BA012ADF3F1044E	181429 bytes (177,18 KiB)
5	Redes da Deep Web - I2P.pdf	C:\Users\Natanael\Desktop\Arquivos\	05912611A82F02DBAAE8E0D03528FFAB	87852 bytes (85,79 KiB)
6	Redes da Deep Web - Onion.pdf	C:\Users\Natanael\Desktop\Arquivos\	CD651531C0014F726DF6C1A1760D451D	332974 bytes (325,17 KiB)
7	Redes da Deep Web - Perfect Dark.pdf	C:\Users\Natanael\Desktop\Arquivos\	FE3937C623CF280072D95869B8564783	493206 bytes (481,65 KiB)
8	Redes da Deep Web - StealthNet.pdf	C:\Users\Natanael\Desktop\Arquivos\	1AC676F1D68973C307FBF368E5F8AA4C	346756 bytes (338,63 KiB)

Essa ferramenta pode ser útil para encontrar um arquivo diferente dos demais em um diretório repleto de arquivos aparentemente iguais, como no exemplo abaixo.

Nome	Data de modificaç...	Tipo	Tamanho
 A Cyberpunk Manifesto - Copia (2)	24/09/2016 14:32	Documento do Mi...	16 KB
 A Cyberpunk Manifesto - Copia (3)	24/09/2016 14:32	Documento do Mi...	16 KB
 A Cyberpunk Manifesto - Copia (4)	24/09/2016 14:32	Documento do Mi...	16 KB
 A Cyberpunk Manifesto - Copia (5)	24/09/2016 14:32	Documento do Mi...	16 KB
 A Cyberpunk Manifesto - Copia (6)	24/09/2016 14:32	Documento do Mi...	16 KB
 A Cyberpunk Manifesto - Copia (8)	24/09/2016 14:32	Documento do Mi...	16 KB
 A Cyberpunk Manifesto - Copia (9)	24/09/2016 14:32	Documento do Mi...	16 KB

O programa conseguiu facilmente reconhecer o arquivo modificado com base no valor de sua hash.

C:\Users\Natanael\Desktop\Cópias			
	File Name	Path	Hash Value
39	A Cyberpunk Manifesto - Copia (7).docx	C:\Users\Natanael\Desktop\Cópias\	2685715707732F193381EFACCE9DD08E837226
29	A Cyberpunk Manifesto - Copia (36).docx	C:\Users\Natanael\Desktop\Cópias\	F85D055A58FBCB669019BE8C2FB03FCE66A3:
28	A Cyberpunk Manifesto - Copia (35).docx	C:\Users\Natanael\Desktop\Cópias\	F85D055A58FBCB669019BE8C2FB03FCE66A3:

A aba **Compare Two Files** permite comparar arquivos e verificar se eles são exatamente os mesmos através de sua hash. Observe a seguir dois resultados diferentes.

Choose two files and click 'Compare Files'

Select File A C:\Users\Natanael\Desktop\A Cyberpunk Manifesto.docx
F85D055A58FBCB669019BE8C2FB03FCE66A33F7E

Select File B C:\Users\Natanael\Desktop\Cópias\A Cyberpunk Manifesto - Copia (9).docx
F85D055A58FBCB669019BE8C2FB03FCE66A33F7E

Compare Files Result: **MATCH!**

Choose two files and click 'Compare Files'

Select File A C:\Users\Natanael\Desktop\A Cyberpunk Manifesto.docx
F85D055A58FBCB669019BE8C2FB03FCE66A33F7E

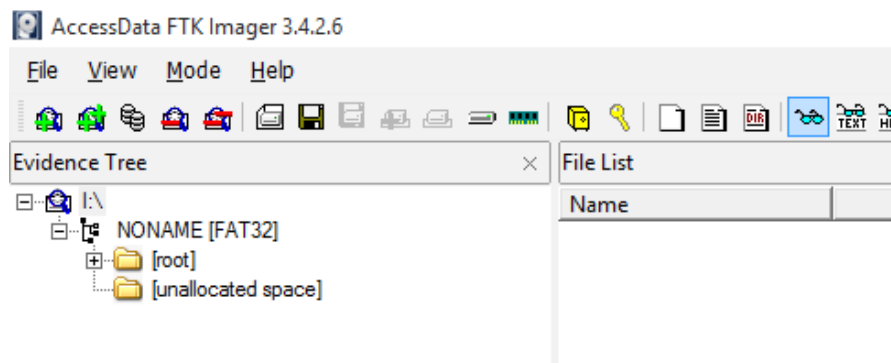
Select File B C:\Users\Natanael\Desktop\Cópias\A Cyberpunk Manifesto - Copia (7).docx
2685715707732F193381EFACCE9DD08E83722662

Compare Files Result: **MIS-MATCH!**

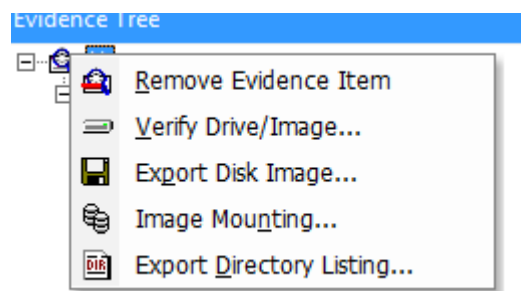
Temos ainda a opção **Compare Directories**, que pode ser usada para comparar dois diretórios entre si e procurar por diferenças de hash ou número de arquivos.

Status:		
There is a hash mis-match between the two directories.		
	File Path and Name (Dir A)	Hash Value
39	C:\Users\Natanael\Desktop\Cópias\A Cyberpunk Manifesto - Copia (7).docx	2685715707732F193381EFACCE9DD08E83722662
29	C:\Users\Natanael\Desktop\Cópias\A Cyberpunk Manifesto - Copia (36).docx	F85D055A58FBCB669019BE8C2FB03FCE66A33F7E
28	C:\Users\Natanael\Desktop\Cópias\A Cyberpunk Manifesto - Copia (35).docx	F85D055A58FBCB669019BE8C2FB03FCE66A33F7E
32	C:\Users\Natanael\Desktop\Cópias\A Cyberpunk Manifesto - Copia (39).docx	F85D055A58FBCB669019BE8C2FB03FCE66A33F7E
31	C:\Users\Natanael\Desktop\Cópias\A Cyberpunk Manifesto - Copia (38).docx	F85D055A58FBCB669019BE8C2FB03FCE66A33F7E
	File Path and Name (Dir B)	Hash Value
39	C:\Users\Natanael\Desktop\Cópias 2\A Cyberpunk Manifesto - Copia (7).docx	2685715707732F193381EFACCE9DD08E83722662
14	C:\Users\Natanael\Desktop\Cópias 2\A Cyberpunk Manifesto - Copia (22).docx	65C2043A5F869FE779793D6108D5B3FC05611721
28	C:\Users\Natanael\Desktop\Cópias 2\A Cyberpunk Manifesto - Copia (35).docx	F85D055A58FBCB669019BE8C2FB03FCE66A33F7E
29	C:\Users\Natanael\Desktop\Cópias 2\A Cyberpunk Manifesto - Copia (36).docx	F85D055A58FBCB669019BE8C2FB03FCE66A33F7E

Caso queiramos obter a hash de um conjunto de arquivos, seja ele uma pasta, diretório ou unidade inteira, podemos fazê-lo utilizando o **AccessData FTK Imager**, que pode ser baixado gratuitamente em <http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.2>.



De posse do programa, podemos inserir evidências (que podem ser pastas, discos físicos ou partições lógicas) e obter suas hashes através da função **Verify Drive/Image**.

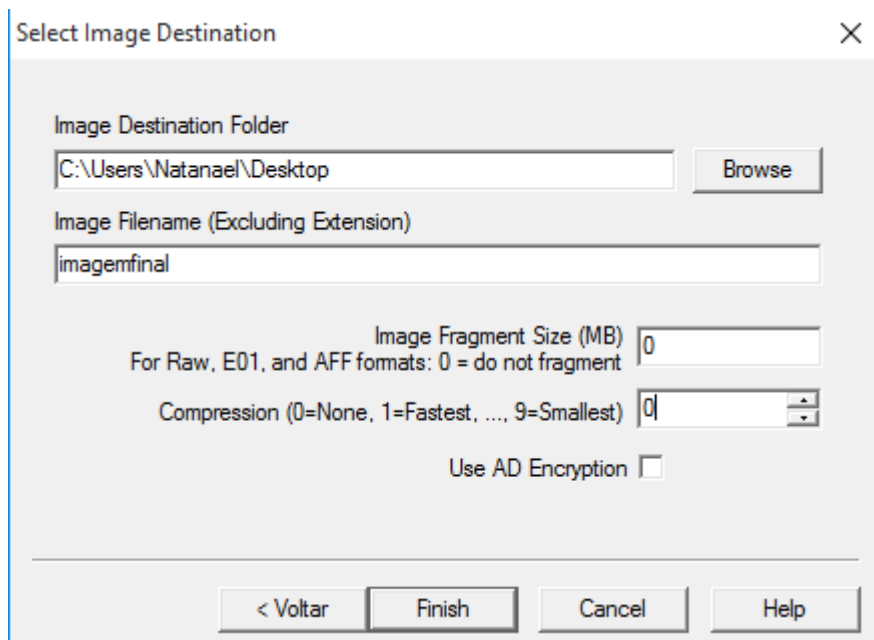


O processo pode demorar para unidades maiores, e retorna suas respectivas hashes ao final do processo.

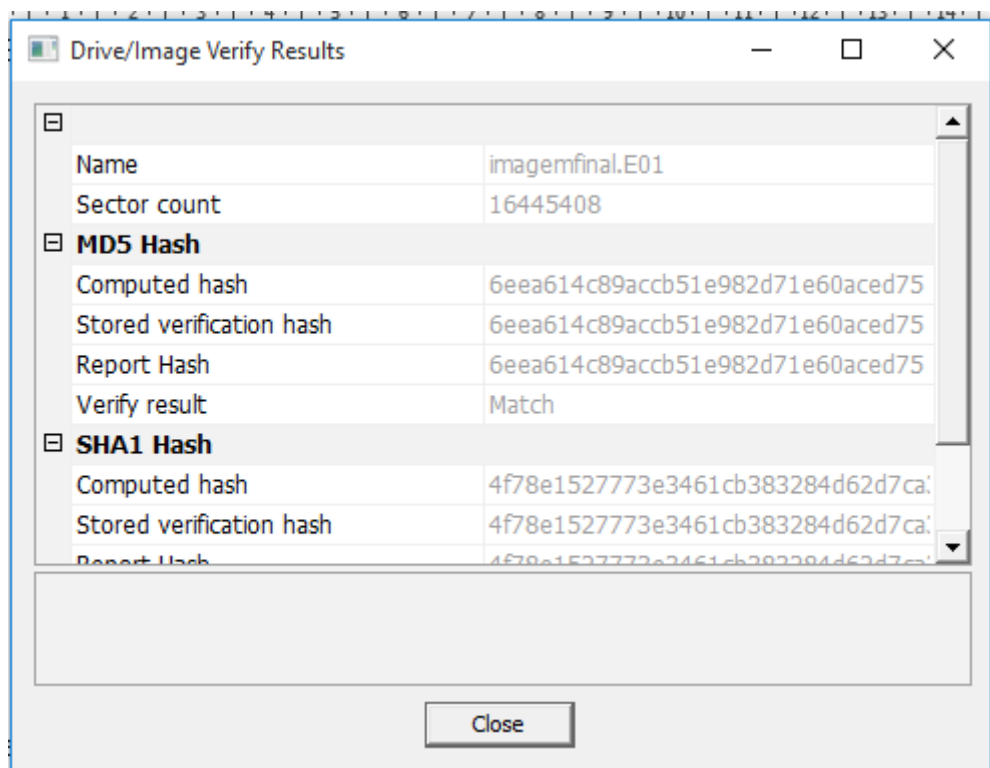
Name	I:\
Sector count	16445408
MD5 Hash	
Computed hash	5839729ec2074bf2d0c2317044cb7de2
SHA1 Hash	
Computed hash	4b1420ac60f25b9209a8b124011902baba9
Bad Sector List	
Bad sector(s)	No bad sectors found

O mesmo programa também pode ser usado para realizar cópias bit-a-bit de unidades. É importante relevar que uma cópia bit-a-bit difere de uma cópia comum no quesito de dados copiados: a segunda opção irá copiar apenas os arquivos visíveis e manipuláveis, enquanto que a primeira copiará todos os bits do volume.

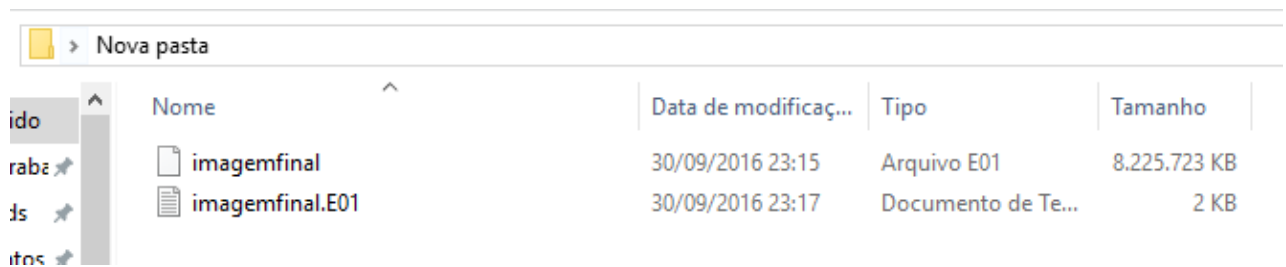
Podemos fazer isso utilizando a opção Create Disk Image e inserindo a unidade desejada. Por questões de compatibilidade com outras ferramentas (o Autopsy é realmente fresco nesse sentido), recomendo utilizar o formato E01 e não fragmentar a imagem, conforme o exemplo.



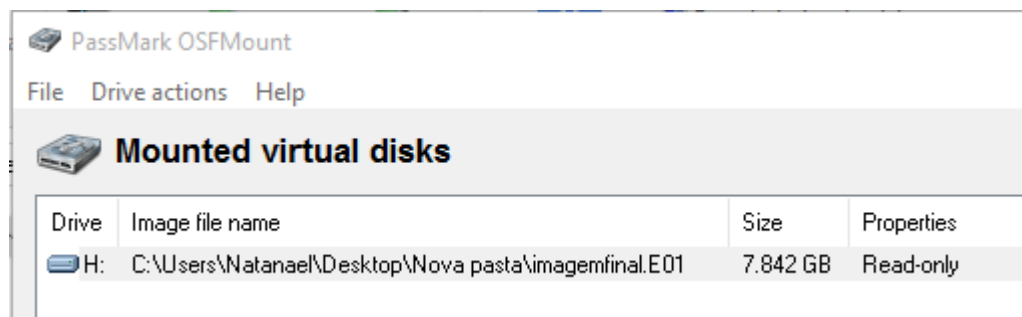
O processo também tende a demorar, e ao final deve gerar uma cópia exata dos bits presentes na unidade original. Lembre-se de comparar as hashes com futuras cópias da evidência.



Após a criação da imagem, são gerados dois arquivos: a imagem em si e um log, contendo informações valiosas sobre sua procedência. É importante que os dois sejam guardados no sistema.



Caso desejarmos explorar o conteúdo de uma imagem, podemos montá-la como uma mídia removível através de programas como o [OSFMount](http://www.osforensics.com/tools/mount-disk-images.html), que pode ser baixado em <http://www.osforensics.com/tools/mount-disk-images.html>. A montagem é intuitiva e a unidade montada apresentará a mesma aparência da unidade original.



Ainda porém, em uma situação na qual seja necessário o uso direto da unidade USB, podemos nos certificar que nenhum byte seja alterado através do [USB Write Blocker for ALL Windows](https://sourceforge.net/projects/usbwriteblockerforwindows8/) (<https://sourceforge.net/projects/usbwriteblockerforwindows8/>). O programa realiza algumas mudanças no registro que impedem o computador de realizar qualquer alteração em qualquer unidade USB, garantindo a integridade da evidência.

```
C:\Windows\system32\cmd.exe

The USB Write Blocker is - ON

USB Write Blocker for ALL Windows by Securite Multi-Secteurs - Version 1.3

Start the write blocker before connecting the USB Flash Drive and do not
change the settings when a USB Flash Drive is connected.
-----
If you have any questions send an email to - support@securitemulti-secteurs.ca

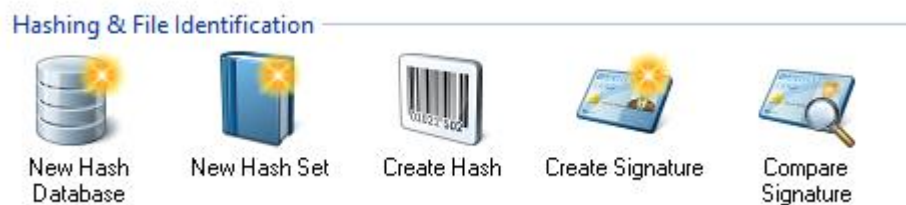
1. Enable the USB Write Blocker - ON
2. Disable the USB Write Blocker - OFF
3. Exit

Type the number and press Enter:
```

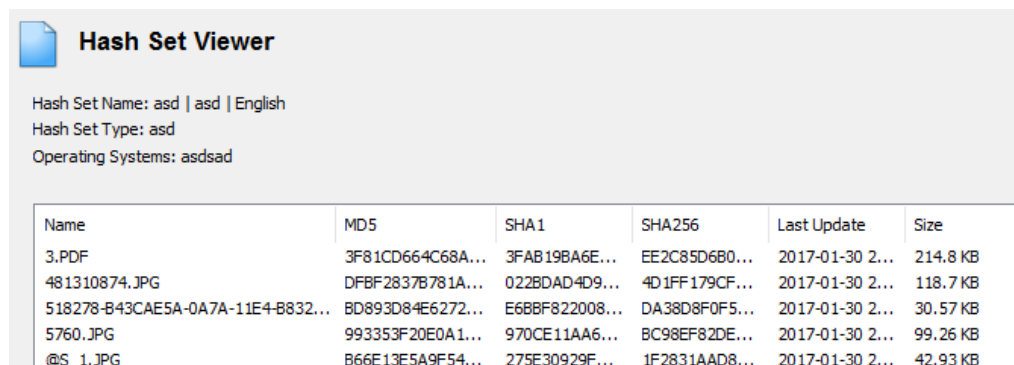
Quando a manipulação da evidência terminar, lembre-se de retirar a unidade USB e só então rativar a permissão para realizar mudanças. Lembre-se também de ler o manual do desenvolvedor, pois contém informações importantes.

Outro programa que permite tal análise é o **OSForensics**, que apesar de pago, possui uma demo disponível para download em <http://www.osforensics.com/download.html>.

A sua categoria Hashing & File Identification permite realizar as operações de documentação de evidências na forma de hash.



A primeira e segunda ferramentas nos permitem montar um índice com todas as hashes presentes em um diretório.

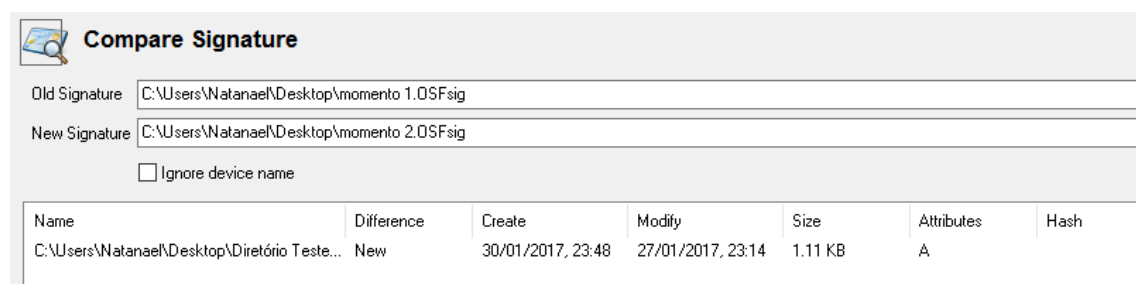


Hash Set Name: asd | asd | English
Hash Set Type: asd
Operating Systems: asdsad

Name	MD5	SHA1	SHA256	Last Update	Size
3.PDF	3F81CD664C68A...	3FAB198A6E...	EE2C85D6B0...	2017-01-30 2...	214.8 KB
481310874.JPG	DFBF2837B781A...	022BDAD4D9...	4D1FF179CF...	2017-01-30 2...	118.7 KB
518278-B43CAE5A-0A7A-11E4-B832...	BD893D84E6272...	E6BBF822008...	DA38D8F0F5...	2017-01-30 2...	30.57 KB
5760.JPG	993353F20E0A1...	970CE11AA6...	BC98EF82DE...	2017-01-30 2...	99.26 KB
@S_1.JPG	B66E13E5A9F54...	275E30929F...	1F2831AAD8...	2017-01-30 2...	42.93 KB

Já a terceira retorna o valor em hash de um único arquivo, da mesma forma que já fizemos anteriormente.

A quarta permite criarmos uma assinatura de um diretório ou disco inteiro. Caso façamos o processo em dois momentos diferentes, podemos compará-los a fim de procurar por eventuais mudanças, utilizando a quinta ferramenta.



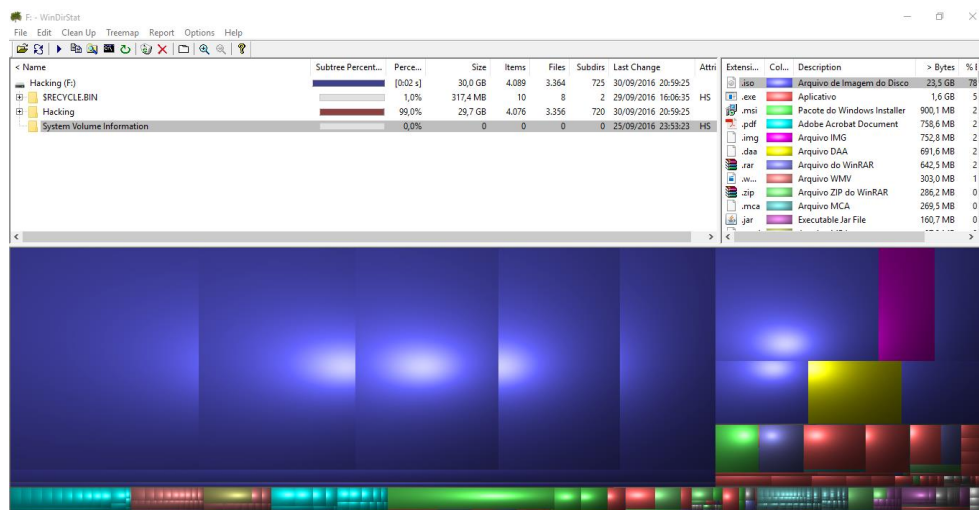
Neste processo, todos os arquivos adicionados, alterados ou removidos serão exibidos.

III. Busca de Diretórios

Durante uma investigação, é comum nos depararmos com uma unidade repleta de diretórios para serem analisados, nos quais é preciso buscar apenas por determinados arquivos. Por exemplo, imagine que temos um HD suspeito de armazenar pornografia infantil e precisamos localizar apenas os arquivos de mídia (imagem e vídeo) para posteriormente classificá-los em provas do crime ou arquivos comuns.

Sem o uso de ferramentas adequadas, essa tarefa pode se tornar árdua – ainda mais considerando a existência de várias pastas e diretórios.

O WinDirStat é uma ferramenta grátis (<https://sourceforge.net/projects/windirstat/>) que nos dá uma representação gráfica dos arquivos que mais ocupam espaço num diretório e pode ser extremamente útil para busca de arquivos suspeitos.



O gráfico na parte inferior mostra sua distribuição, na qual cada cor é relacionada com uma extensão de arquivo exibido no canto superior esquerdo.

Extensi...	Col...	Description	> Bytes	% t
.iso		Arquivo de Imagem do Disco	23,5 GB	78
.exe		Aplicativo	1,6 GB	5
.msi		Pacote do Windows Installer	900,1 MB	2
.pdf		Adobe Acrobat Document	758,6 MB	2
.img		Arquivo IMG	752,8 MB	2
.daa		Arquivo DAA	691,6 MB	2
.rar		Arquivo do WinRAR	642,5 MB	2
.wmv		Arquivo WMV	303,0 MB	1
.zip		Arquivo ZIP do WinRAR	286,2 MB	0
.mca		Arquivo MCA	269,5 MB	0
.jar		Executable Jar File	160,7 MB	0

Clicando em um deles, somos imediatamente direcionados para a visualização do arquivo em questão.

desktop.ini	0,0%	104 bytes				02/10/20
Microsoft Office	74,4%	5,6 GB	14	13	1	18/05/20
<Files>	100,0%	5,6 GB	7	7	0	14/12/20
desktop.ini	0,0%	101 Bytes				29/09/20
Microsoft Office 2010 Profissional Português-br x6...	12,6%	719,5 MB				10/11/20
Microsoft Office 2010 Profissional Português-br x8...	11,3%	642,0 MB				10/11/20
OfficeProfessionalPlus_x64_pt-br.daa	12,2%	691,6 MB				06/10/20
OfficeProfessionalPlus_x64_pt-br.imn	13,2%	752,8 MB				03/10/20

Outra forma interessante de listar arquivos é com os comandos `tree` e `dir` no Prompt de Comando do Windows. O primeiro exibe todos os arquivos presentes em um diretório na forma de árvore, onde podemos ver claramente a organização de pastas.

```
C:\>F:

F:\>tree
Listagem de caminhos de pasta para o volume Hacking
O número de série do volume é 00000043 4009:6980
F:.
├── Hacking
│   ├── Biblioteca
│   │   ├── Biblioteca Hacking
│   │   │   └── Computer Power User - Ano 2014
│   │   ├── Conteúdo Genérico
│   │   ├── Engenharia Social
│   │   ├── Forense
│   │   ├── Forense digital toolkit
│   │   ├── Google Hacking
│   │   ├── Kali Linux
│   │   ├── Linguagem Batch
│   │   ├── Linguagem C
│   │   │   └── Linguagem C para Hackers Iniciantes Marco A T
│   │   ├── Phyton
│   │   ├── Redes
│   │   │   └── Apostila de Redes
│   │   ├── Senhas
│   │   ├── SQL Injection
│   │   ├── Visual Basic
│   │   ├── Vírus
│   │   ├── Web Hacking
│   │   ├── Wireless Hacking
│   │   │   └── Curso Wireless Hacking
│   └── Criptomoedas
│       ├── Arquivos Batch
│       ├── Backups
│       ├── Mineradores
│       │   └── ccminer-1.7.5-blake2s-32-bit
```

Já o último exibe todas as pastas de um diretório de uma forma um pouco mais compacta.


```
F:\>cd Hacking

F:\Hacking>dir
O volume na unidade F é Hacking
O Número de Série do Volume é 4009-6980

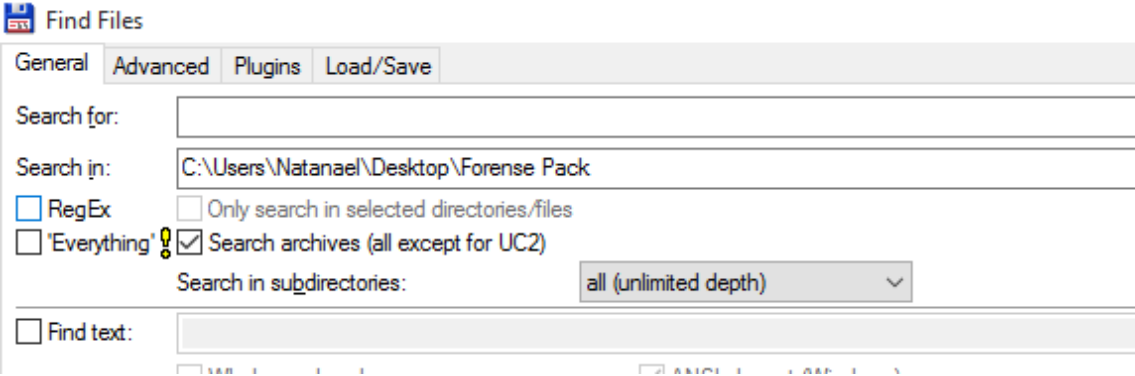
Pasta de F:\Hacking

11/09/2016  22:08    <DIR>          .
11/09/2016  22:08    <DIR>          ..
24/09/2016  15:01    <DIR>          Biblioteca
18/05/2016  15:35    <DIR>          Criptomoedas
24/09/2016  15:01    <DIR>          Feitos
21/09/2016  15:26    <DIR>          Formatação
28/09/2016  20:31             1.476 Prompt de Comando.lnk
24/09/2016  15:01    <DIR>          Páginas para Deface
27/08/2016  11:51    <DIR>          Páginas para Phishing
24/09/2016  15:01    <DIR>          Scans
20/09/2016  14:19    <DIR>          Scripts e Tools
                1 arquivo(s)          1.476 bytes
                10 pasta(s)      49.912.459.264 bytes disponíveis

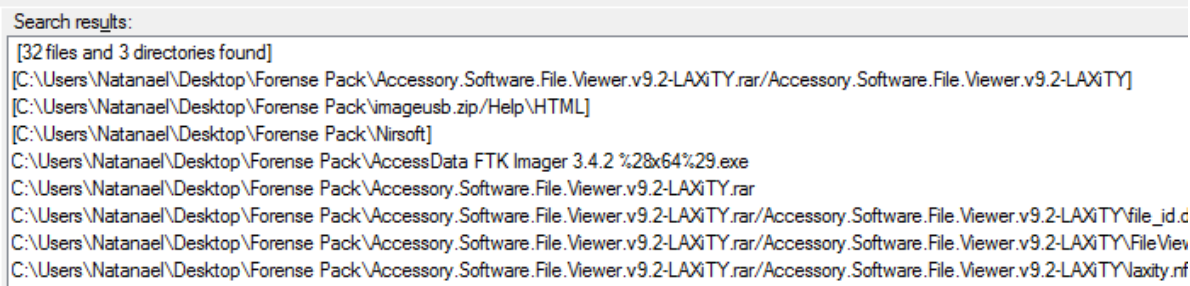
F:\Hacking>
```

Existem ainda mais duas ferramentas com funções semelhantes que podem ser utilizadas para exploração de diretórios.

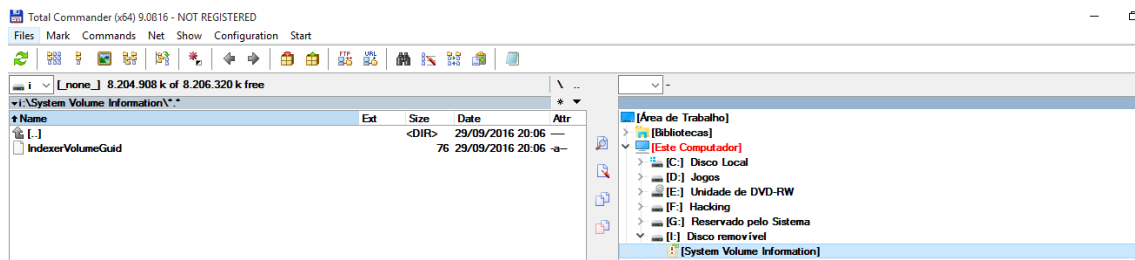
A primeira delas é o **Total Commander** (<https://www.ghisler.com>), que permite buscarmos arquivos em diretórios conforme filtros de data, tamanho, atributos e tipos de arquivo.



Basta configurarmos os filtros corretos e iniciar a busca para que os programas enquadrados neles sejam listados na tela.



O programa ainda nos fornece duas janelas de operação, o que permite uma busca mais rápida e funcional.



Outra ferramenta interessante é o [File Viewer 9.2](#), que apesar de ser um projeto descontinuado, pode ser encontrado no pack que acompanha este curso.

Ele nos permite buscar arquivos conforme sua extensão, o que pode economizar uma quantidade considerável de trabalho braçal.



Basta definir os critérios de busca e aguardar até que os arquivos desejados sejam exibidos na barra inferior.

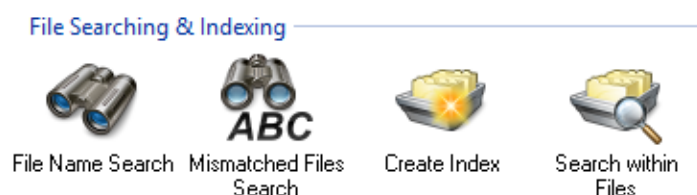


Podemos ainda usar a Copiadora 666 (<https://sourceforge.net/projects/copiadora-666/>) para copiar arquivos de determinado tipo entre diretórios.

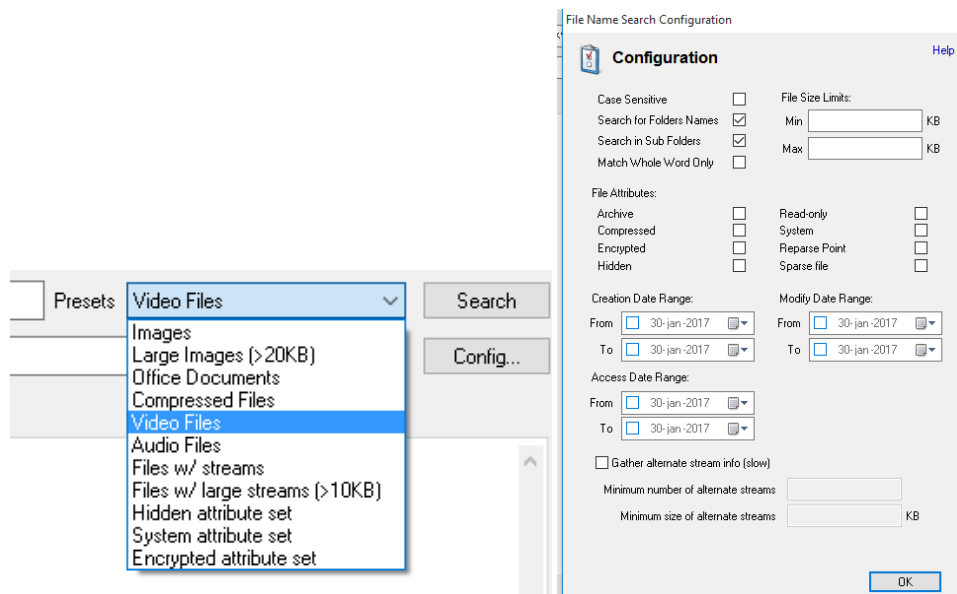
```
O que deseja fazer?7
Qual diretorio deseja copiar (insira o diretorio completo)?F
Para qual diretorio ou unidade (insira o diretorio completo)?C
Deseja adicionar outros parametros? Se nao, deixe com um espaco.

1 - Tudo
2 - Imagens (png,jpg,jpeg,gif,ico,svg,bmp)
3 - Videos (mp4,avi,mkv,vmv,vma,mpg,mpeg,asf)
4 - Musicas (mp3,wav,flac,aac)
5 - Textos (txt,docx,pdf,doc,docm)
6 - Office (doc,docx,docm,xlsx,xlsm,xltx,pptx,ppsx,potx,accdb,mdb )
  6.1 - Word (doc,docx,docm)
  6.2 - Excel (xlsx,xlsm,xltx)
  6.3 - Power Point (pptx,ppsx,potx)
  6.4 - Access (accdb,mdb)
7 - Web (html, htm,php,js,aspx,css,cpp)
8 - Design (psd,indd,pdf,svg,cdr,ai,aep,aepx,ppj)
9 - Sistema (dll,reg,jar)
10 - Compactados (zip,rar)
11 - Outro (inserir)
```

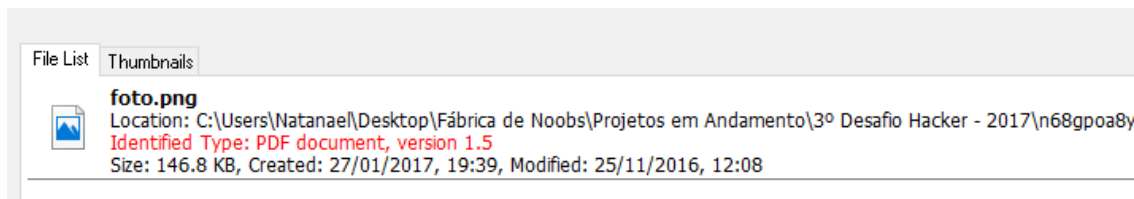
O OSForensics também possui ferramentas interessantes neste quesito. A aba **File Searching & Indexing** nos permite realizar busca de arquivos dentro de um disco investigado.



A primeira opção permite que essa busca seja realizada com base em filtros de tipo de arquivo, data, tamanho e outros atributos. Pode ser uma ferramenta extremamente útil quando procuramos por alguma prova que deve apresentar determinado formato (vídeos de pornografia ilegal, por exemplo).



Já a segunda tem uma aplicação interessante em busca de arquivos contendo esteganografia. Ela procura por arquivos que possuam um conteúdo diferente do que sua extensão representa.



Para obter maiores informações sobre o assunto, consulte o capítulo VIII, que aborda a análise de esteganografia.

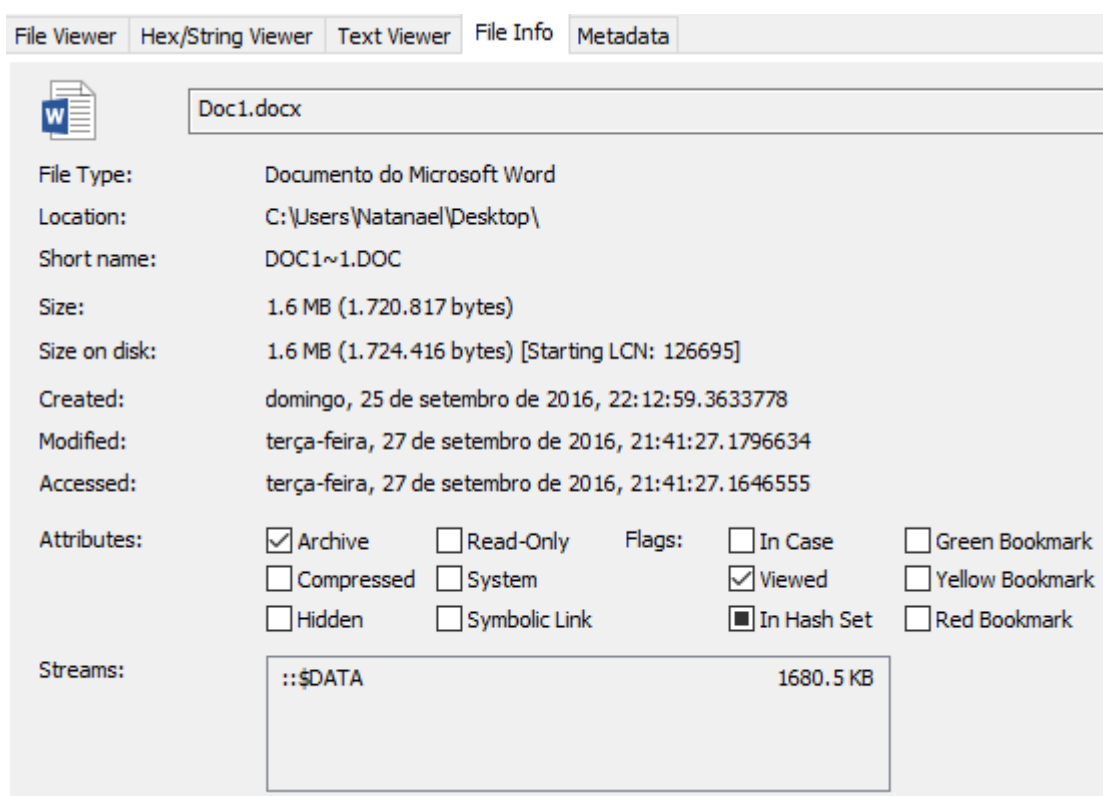
As outras duas possuem ferramentas que permitem a catalogação e procura de arquivos com determinadas características na forma de índice.

IV. Análise de Arquivos

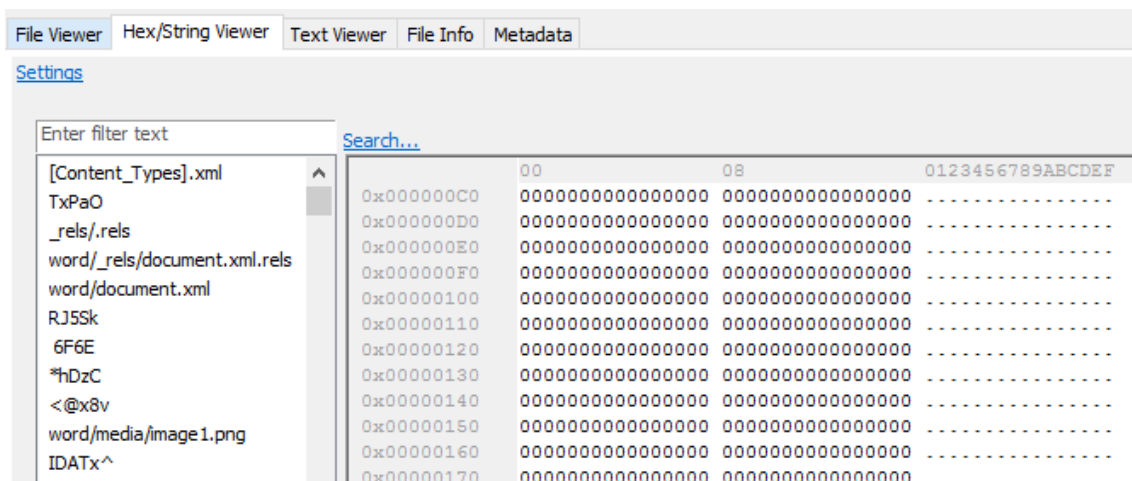
Arquivos, além de serem provas de eventuais crimes, podem também ser fontes de informações valiosas.

Aqui, o OSForensics também possui grande utilidade neste tipo de análise.

A opção **File Viewer** nos permite obter informações sobre a data na qual um arquivo foi criado, acessado e modificado, além de detalhes sobre seus atributos.

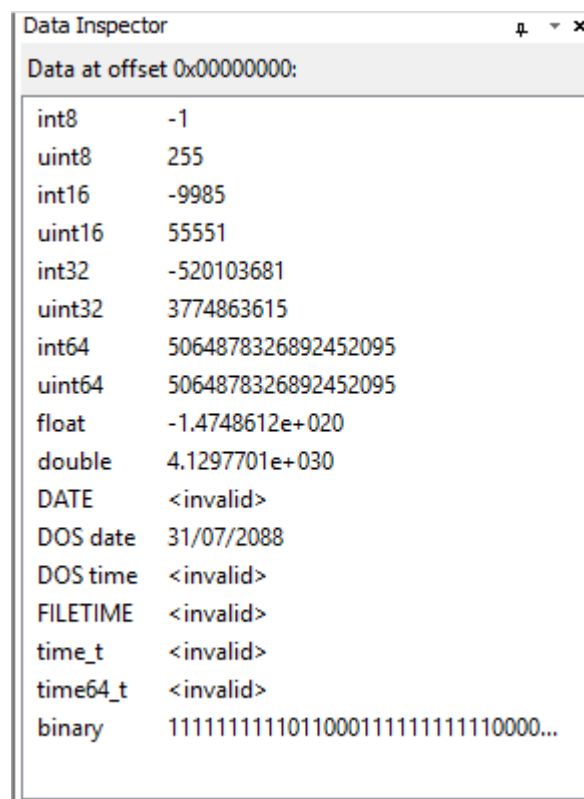


Podemos também usar a visão em hexadecimal para extrair partes de texto que podem ser relevantes em uma investigação forense, como caminhos de arquivos, nomes de programas utilizados e URL's.



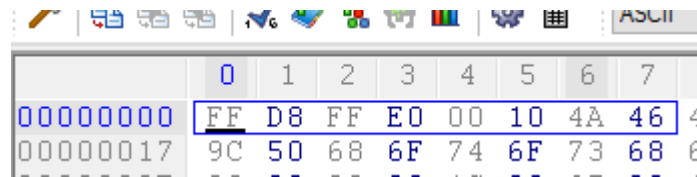
Caso não disponha de um programa como o OSForensic, também é possível obter essas informações manualmente utilizando um editor hexadecimal como o [Hex Workshop Hex Editor](http://www.hexworkshop.com), disponível para download em <http://www.hexworkshop.com>.

Ao abrir um arquivo com o programa, temos acesso ao seu código hexadecimal e também a um inspetor de valores, presente na coluna à esquerda.



Essa parte em especial pode fornecer alguns detalhes importantes, como o header do arquivo.

O header é uma sequência de caracteres em hexadecimal que indica a extensão de determinado arquivo. Cada extensão (jpg, png, docx, etc) possui seu próprio header. No exemplo, ele está presente nos valores associados com o campo **binary**.



Segue uma tabela com os headers dos principais tipos de arquivo encontrados. Note também que sempre é possível pesquisar pelo código em hexadecimal para descobrir sua correspondência.

Filetype	Start	Start ASCII Translation
ani	52 49 46 46	RIFF
au	2E 73 6E 64	snd
bmp	42 4D F8 A9	BM
bmp	42 4D 62 25	BMp8
bmp	42 4D 76 03	BMv
cab	4D 53 43 46	MSCF
dll	4D 5A 90 00	MZ
Excel	D0 CF 11 E0	
exe	4D 5A 50 00	MZP (inno)
exe	4D 5A 90 00	MZ
flv	46 4C 56 01	FLV
gif	47 49 46 38 39 61	GIF89a
gif	47 49 46 38 37 61	GIF87a
gz	1F 8B 08 08	
ico	00 00 01 00	
jpeg	FF D8 FF E1	
jpeg	FF D8 FF E0	JFIF
jpeg	FF D8 FF FE	JFIF
Linux bin	7F 45 4C 46	ELF
png	89 50 4E 47	PNG
msi	D0 CF 11 E0	
mp3	49 44 33 2E	ID3
mp3	49 44 33 03	ID3
OFT	4F 46 54 32	OFT2
PPT	D0 CF 11 E0	
PDF	25 50 44 46	%PDF
rar	52 61 72 21	Rar!
sfw	43 57 53 06/08	cws
tar	1F 8B 08 00	
tgz	1F 9D 90 70	
Word	D0 CF 11 E0	
wmv	30 26 B2 75	
zip	50 4B 03 04	PK

Buscar por headers específicos em um código hexadecimal também pode ser útil para detectar e quebrar alguns métodos simples de esteganografia.

V. Auditoria em Windows

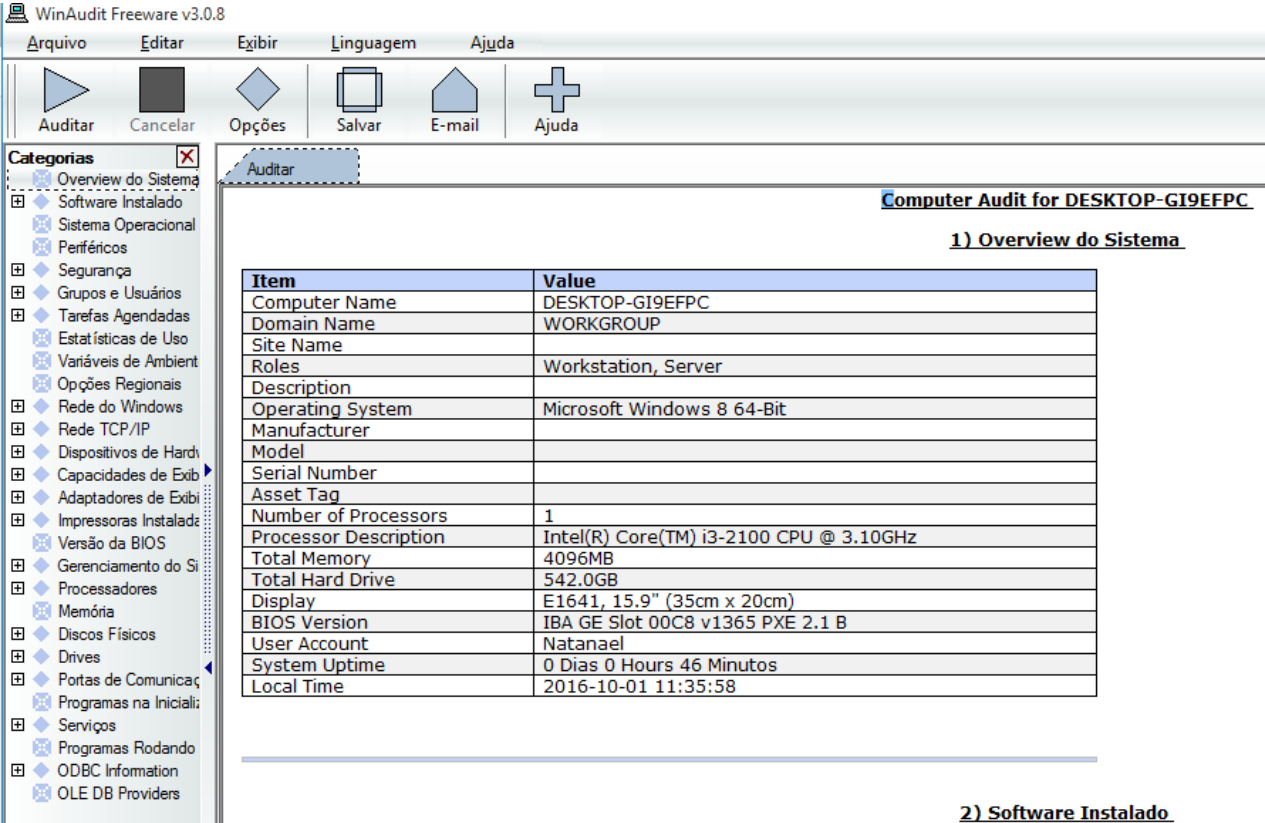
São diversas as situações em que ocorre a apreensão de um computador e é necessário analisá-lo não só no quesito dos arquivos armazenados, mas também dos processos que estão sendo executados na máquina.

É nesse contexto que entram os programas que permitem procurar por dados úteis em um sistema operacional, como chaves de registro, senhas armazenadas, histórico de navegação, entre outros.

Por se tratar de dados voláteis, é importante que os programas forenses sejam executados a partir de uma unidade externa, de forma a realizar o mínimo possível de modificações no sistema investigado.

Um dos primeiros passos é fazer um levantamento completo do hardware do computador, incluindo placas de vídeo, rede, processadores e dispositivos periféricos.

Felizmente, existem programas que realizam todo o serviço automaticamente, como o **WinAudit** (<https://winaudit.codeplex.com>). Basta executá-lo e aguardar o processo de auditoria.



The screenshot displays the WinAudit Freeware v3.0.8 application window. The interface includes a menu bar (Arquivo, Editar, Exibir, Linguagem, Ajuda) and a toolbar with icons for Auditar, Cancelar, Opções, Salvar, E-mail, and Ajuda. A left sidebar lists various system categories for auditing, such as Software Instalado, Sistema Operacional, Periféricos, and Hardware. The main window area shows the 'Computer Audit for DESKTOP-GI9EFPC' results under the '1) Overview do Sistema' section. This section contains a table with system details.

Item	Value
Computer Name	DESKTOP-GI9EFPC
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server
Description	
Operating System	Microsoft Windows 8 64-Bit
Manufacturer	
Model	
Serial Number	
Asset Tag	
Number of Processors	1
Processor Description	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz
Total Memory	4096MB
Total Hard Drive	542.0GB
Display	E1641, 15.9" (35cm x 20cm)
BIOS Version	IBA GE Slot 00C8 v1365 PXE 2.1 B
User Account	Natanael
System Uptime	0 Dias 0 Hours 46 Minutos
Local Time	2016-10-01 11:35:58

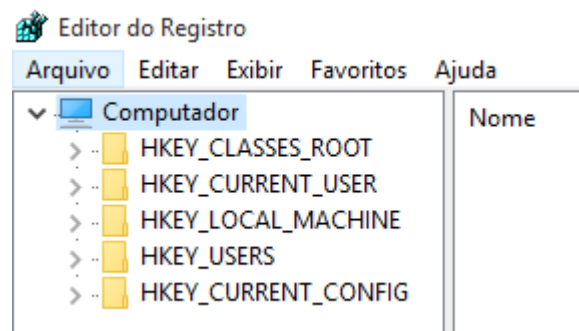
Below the table, the '2) Software Instalado' section is partially visible.

Uma vez terminado, basta navegar no menu para obter todo tipo de informação sobre o computador analisado.

Também é importante salvar o resultado da auditoria como um arquivo HTML para futuras consultas.

O registro do Windows é um banco de dados do sistema que armazena todas as configurações dos aplicativos que instalamos. Qualquer alteração feita nele será salva no registro, o que o torna uma importante fonte de informação para a computação forense.

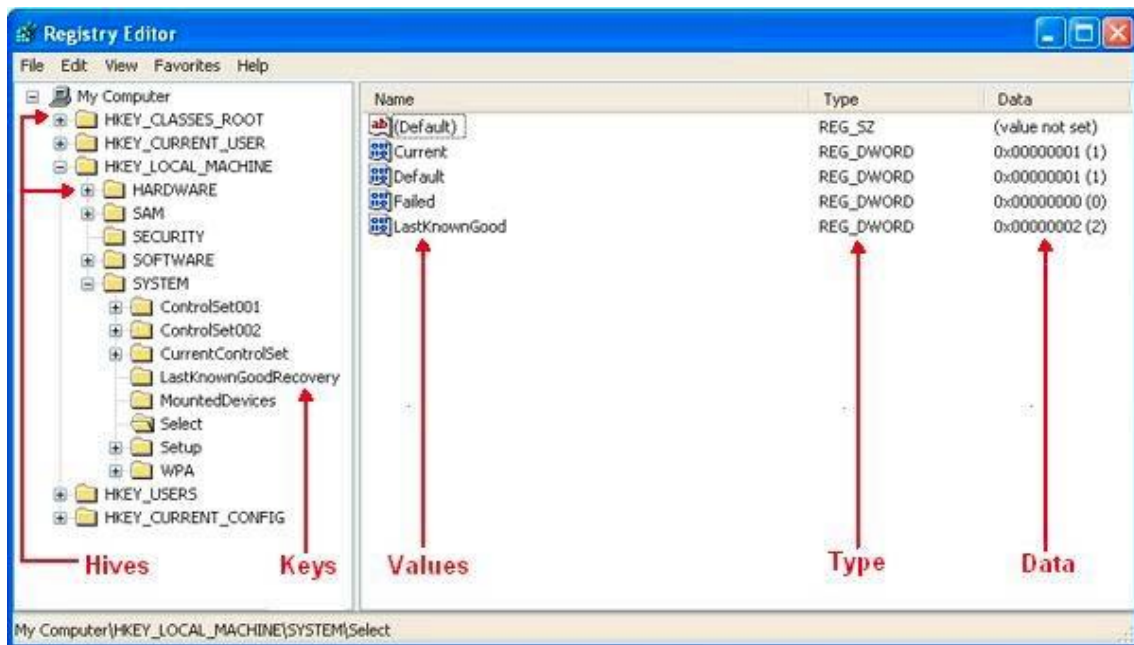
Ele pode ser facilmente acessado pelo comando regedit e é composto de 5 classes de valores.



São elas:

- HKEY_CLASSES_ROOT (HKCR): armazena informações que garantem que o programa correto seja iniciado quando clicado pelo Windows Explorer. Também possui detalhes sobre atalhos.
- HKEY_CURRENT_USER (HKCU): contém informações sobre o usuário logado atualmente no sistema.
- HKEY_LOCAL_MACHINE (HKLM): contém informações de hardware sobre máquina em questão, cuja maioria já pode ser obtida a partir da auditoria.
- HKEY_USERS (HKU): contém informações a respeito de todos os usuários presentes na máquina, como programas, configurações e definições visuais.
- HKEY_CURRENT_CONFIG (HCU): armazenas informações sobre a atual configuração do sistema.

O registro do Windows é basicamente organizado nos seguintes valores:



Por exemplo, podemos encontrar os programas configurados para se auto executar no momento da inicialização do Windows em localizações como:

HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce

HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

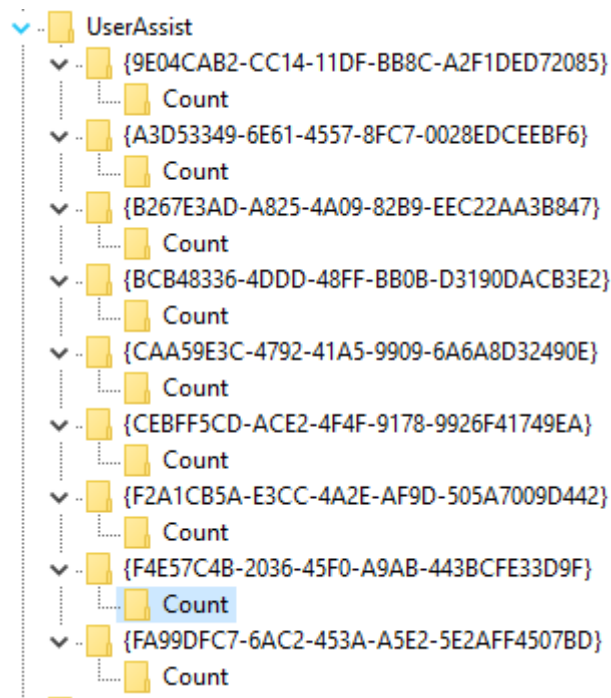
HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Essas informações nos permitirão deduzir quais programas são iniciados automaticamente com o Windows.

ajuda

Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
AdobeAAMUpd...	REG_SZ	"C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe"
Fences	REG_SZ	"C:\Program Files (x86)\Stardock\Fences\Fences.exe" /startup

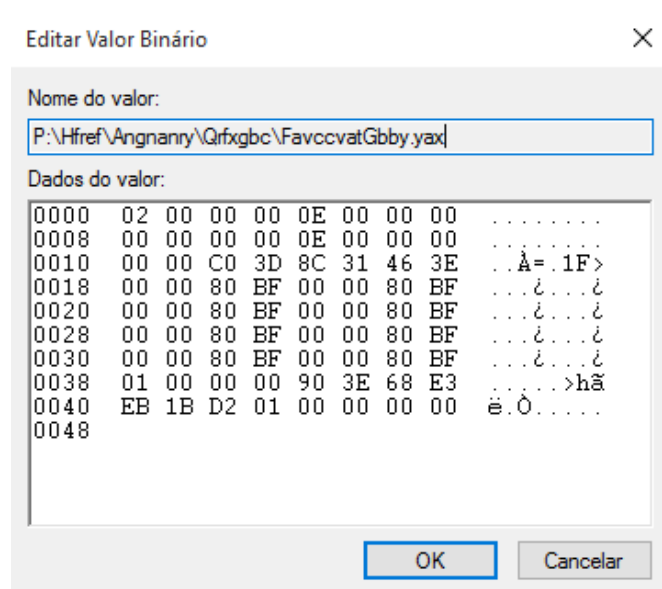
Em HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist, podemos encontrar valores relativos aos processos iniciados na máquina por determinado usuário. Para tanto, basta expandir as pastas e clicar nos valores Count.



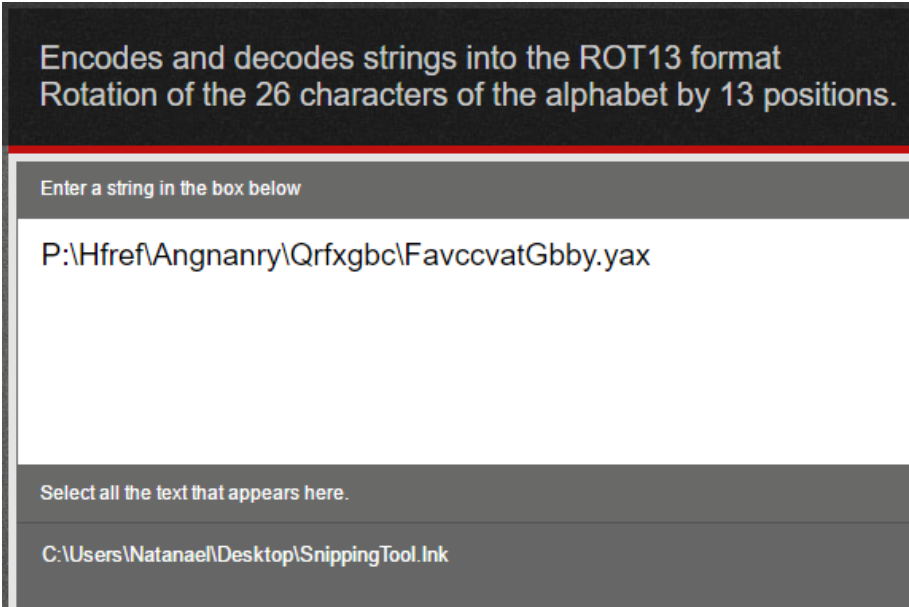
Cada um deles deverá revelar um conjunto de valores.

Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
{0139Q44R-6NSR-49S2-8690-...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
{0139Q44R-6NSR-49S2-8690-...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
{0139Q44R-6NSR-49S2-8690-...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
{0139Q44R-6NSR-49S2-8690-...	REG_BINARY	02 00 00 00 01 00 00 00 00 00 00 00 00 01 00 00
{0139Q44R-6NSR-49S2-8690-...	REG_BINARY	02 00 00 00 01 00 00 00 00 00 00 00 00 01 00 00
{0139Q44R-6NSR-49S2-8690-...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
{0139Q44R-6NSR-49S2-8690-...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

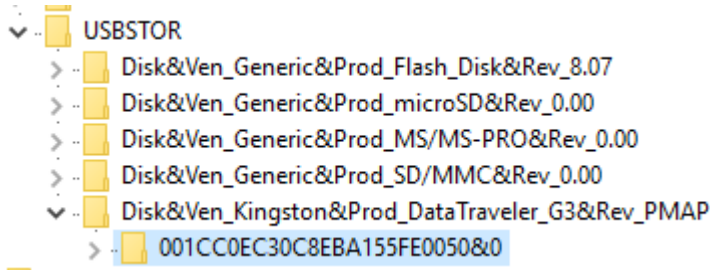
Escolhendo um valor arbitrário, receberemos a seguinte janela:



O texto do campo **Nome do valor** está encriptado em ROT13 e ao ser traduzido pode revelar informações interessantes.



Podemos encontrar detalhes sobre os dispositivos USB que foram contactados no computador na seção **HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR**.



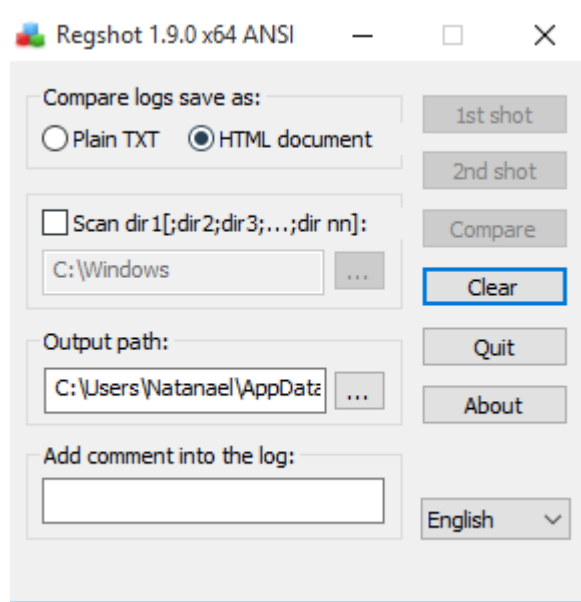
Clicar em uma das chaves nos retorna valores sobre o dispositivo.

Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{fe7d53c2-79aa-5a0d-be2f-5f2b3817b1f0}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0006
FriendlyName	REG_SZ	Kingston DataTraveler G3 USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskKingstonDataTraveler_G3_PMAP USE
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk driv
Service	REG_SZ	disk

Também podemos verificar as regras de Firewall e encontrar detalhes sobre as aplicações executadas na máquina em `HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules`.

Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
{01724322-F8F7-43BC-9AAD...	REG_SZ	v2.24 Action=Allow Active=TRUE Dir=In Profile=Domain Profile=Private Name=@{Microsoft.MicrosoftEdge_2
{04962834-EF86-4783-BFB2-E...	REG_SZ	v2.24 Action=Allow Active=TRUE Dir=In Protocol=17 Profile=Public App=C:\Program Files (x86)\Microsoft Of
{05220A64-073F-48BD-9DD8...	REG_SZ	v2.24 Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public Name=@{Microsoft
{11AA8C16-7B44-4A32-823A...	REG_SZ	v2.24 Action=Block Active=TRUE Dir=Out App=%ProgramFiles% (x86)\TechSmith\Camtasia Studio 8\Camtas
{16AD77C6-B7F9-4F95-885A...	REG_SZ	v2.24 Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public Name=@{Microsoft

Outra ferramenta interessante é o **Regshot** (<https://sourceforge.net/projects/regshot/>), que permite tirar uma “fotografia” do registro naquele momento, e depois comparar com outra. É uma função interessante para estudar as alterações que determinados procedimentos no Windows podem exercer no registro, e facilitar a busca por determinadas evidências.












Existem alguns programas que facilitam nossa busca por informações de relevância conhecida e que requerem uma procura mais complexa se forem levantadas através do regedit, como os presentes no kit da **Nirsoft**. Cada programa pode ser baixado individualmente em http://www.nirsoft.net/password_recovery_tools.html e tem funções próprias. É possível ainda realizar o download de toda a ferramenta em <http://launcher.nirsoft.net/downloads/index.html>.

Recomendo gastar algum tempo se familiarizando com todas as suas funções. Além disso, o projeto está em constante desenvolvimento e novas funções são atualizadas a cada semana.

NirLauncher - NirSoft Utilities












File Edit View Options Launcher Packages Help

Password Recovery Utilities	Network Monitoring Tools	Web Browser Tools	Video/Audio Related Utilities	Internet R
Outlook/Office Utilities	Programmer Tools	Disk Utilities	System Utilities	Othe
Name	Description	Version	Updated On	Web Page URL
 Password Security Scanner	Displays security information about passwords st...	1.40	26/09/2016 10:22:00	http://www.nirs
 ImageCacheViewer	Displays images stored in the cache of your Web ...	1.12	25/09/2016 06:51:30	http://www.nirs
 PasswordFox	View passwords stored in Firefox Web browser.	1.57	24/09/2016 12:33:02	http://www.nirs
 BrowsingHistoryView	View browsing history of popular Web browsers	1.90	22/09/2016 17:18:50	http://www.nirs
 ShadowCopyView	View shadow copies on your system	1.03	22/09/2016 08:20:02	http://www.nirs
 HashMyFiles	Calculate the MD5/SHA1 hashes of your files	2.20	21/09/2016 05:29:04	http://www.nirs
 VaultPasswordView	Decrypts passwords stored in Windows Vault	1.00	20/09/2016 04:52:24	http://www.nirs
 ChromePass	Password recovery tool for Google Chrome Web ...	1.41	19/09/2016 02:52:02	http://www.nirs
 WakeMeOnLan	Turn on one or more computers remotely by sen...	1.78	16/09/2016 15:13:32	http://www.nirs

Com eles é possível, por exemplo, ter acesso à todas as senhas armazenadas no computador.

WebBrowserPassView








File Edit View Options Help

URL	Web Browser	User Name	Password
 http://cocada3301.mipropia.com/	Vivaldi		
 http://www.acdlabs.com/account/regist...	Vivaldi		
 https://accountrecovery.mercadolivre.co...	Vivaldi		
 https://accounts.google.com/ServiceLog...	Vivaldi		
 https://accounts.google.com/signin/cha...	Vivaldi		
 https://login.proboards.com/login/6311...	Vivaldi		
 https://my.dogechain.info/	Vivaldi		
 https://pass.chemaxon.com/activate/fab...	Vivaldi		
 https://twitter.com/	Vivaldi		
 https://www.cybrary.it/wp-login.php	Vivaldi		
 https://www.fuvest.com.br/portal/fuvest...	Vivaldi		

Ou ao histórico de navegação de páginas da web e arquivos.

BrowsingHistoryView

File Edit View Options Help

URL	Title	Visit Time	Visit
 https://www.youtube....	FULL: Donald Trump vs ...	28/09/2016 14:55:57	2
 https://www.youtube....	FULL: Donald Trump vs ...	28/09/2016 14:55:56	2
 https://www.youtube....	Criptografia - Funções ...	30/09/2016 23:18:07	1
 https://www.youtube....	Nirvana - Smells Like Te...	29/09/2016 19:24:09	2
 https://www.youtube....	Nirvana - Smells Like Te...	29/09/2016 19:23:19	2
 https://www.youtube....	YouTube NextUp	22/09/2016 20:23:26	1
 https://www.youtube....		22/09/2016 20:23:29	1

Ou ainda à um registro das vezes em que o computador foi ligado e desligado, além de várias outras informações improtantes.

TurnedOnTimesView - DESKTOP-GI9EFPC				
File Edit View Options Help				
Startup Time	Shutdown Time	Duration	Shutdown Reason	Shu
11/09/2016 19:18:28	11/09/2016 19:41:23	00:22:55	Operating system issue ...	rei
11/09/2016 19:43:26	11/09/2016 19:51:39	00:08:13	Operating system issue ...	rei
11/09/2016 19:53:04				
17/09/2016 17:26:03				
20/09/2016 14:36:48				
20/09/2016 16:04:39	21/09/2016 22:26:28	1 Days + 06:21:49		
22/09/2016 13:03:10	22/09/2016 22:20:08	09:16:58		De
23/09/2016 14:44:00				
25/09/2016 10:15:01				

Mais uma vez, o OSForensics também nos fornece ferramentas para realizar seu trabalho. Elas estão presentes na seção System Artifacts & Passwords, em Recent Activity.






Com poucos passos, o programa nos retorna uma lista completa de todas as atividades recentes realizadas no computador.

</

Este capítulo não estaria completo sem abordar a investigação dos processos do Windows. Esse tipo de análise pode ser útil em casos onde é possível ter acesso ao computador na cena do crime ainda funcionando, ou em uma situação doméstica para se erradicar um malware.

Um primeiro reconhecimento pode ser feito pelo próprio **Gerenciador de Tarefas do Windows**, e consiste apenas em analisar os programas em execução na procura de algo suspeito.

Processos em segundo plano (...)

- >  Adobe Acrobat Update Service (...)
-  Adobe CEF Helper (32 bit)
-  Adobe Creative Cloud (32 bit)
- >  Adobe Genuine Software Integrity...
-  Adobe IPC Broker (32 bit)

0%	0,4 MB	0 MB/s	0 Mbps
0%	2,3 MB	0 MB/s	0 Mbps
0%	3,9 MB	0 MB/s	0 Mbps
0%	0,5 MB	0 MB/s	0 Mbps
0%	1,8 MB	0 MB/s	0 Mbps

É possível também obter uma lista de todos os arquivos e diretórios que estão associados com determinado processo utilizando o [handle](https://technet.microsoft.com/en-us/sysinternals/handle.aspx), ferramenta de linha de comando disponível para download no site da Microsoft (<https://technet.microsoft.com/en-us/sysinternals/handle.aspx>).

```

54C: File C:\Windows\Fonts\segoeui1.ttf
-----
vivaldi.exe pid: 7196 DESKTOP-GI9EFPC\Natanael
54: File C:\Windows
5C: Section \Sessions\1\BaseNamedObjects\CrSharedMem_0866f9d45501376be3608d
60: Section \Sessions\1\BaseNamedObjects\CrSharedMem_ea5cc89c7586cb2e82662e
70: File C:\Users\Natanael\AppData\Local\Vivaldi\Application\1.4.589.29
9C: File C:\Users\Natanael\AppData\Local\Vivaldi\Application\1.4.589.29
E0: Section \Sessions\1\BaseNamedObjects\CrSharedMem_0df4694e2a51c6dc717295
E4: Section \Sessions\1\BaseNamedObjects\CrSharedMem_6c1c289138a175804d1416
1A8: File C:\Users\Natanael\AppData\Local\Vivaldi\Application\1.4.589.29

```

Há também outra ferramenta semelhante chamada [listdlls](https://technet.microsoft.com/en-us/sysinternals/bb896656.aspx) (<https://technet.microsoft.com/en-us/sysinternals/bb896656.aspx>) que permite listar todas as DLL's envolvidas com determinado processo.

```

-----
taskhostw.exe pid: 4708
Command line: taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}

Base          Size          Path
0x0000000057660000 0x19000 C:\Windows\system32\taskhostw.exe
0x0000000091f80000 0x1c2000 C:\Windows\SYSTEM32\ntdll.dll
0x0000000091c60000 0xad000 C:\Windows\system32\KERNEL32.DLL
0x000000008ea40000 0x1dd000 C:\Windows\system32\KERNELBASE.dll
0x0000000091950000 0x9d000 C:\Windows\system32\msvcrt.dll

```


VI. Recuperação de Arquivos

Justamente em função de sua ampla utilidade, a área de recuperação de arquivos é uma das mais populares da computação forense, uma vez que não é útil apenas em investigações, mas em qualquer situação na qual seja necessário recuperar arquivos perdidos – proposital ou acidentalmente.

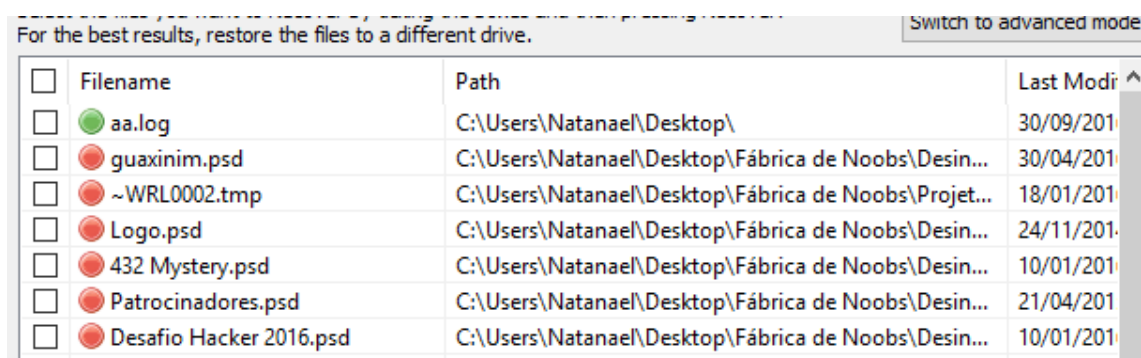
Por essa razão, existe uma ampla gama de programas que recuperam arquivos, desde os voltados para uso doméstico até os profissionais, que contam com funções desnecessárias para o usuário comum.

A recuperação de arquivos só é possível porque, ao deletar um arquivo, o computador não apaga os valores dos bits relativos ao arquivo escolhido, mas apenas os marca como passíveis de serem sobrepostos.

Dessa forma, um arquivo deletado – mesmo a partir de uma formatação de alto nível – ainda pode ser recuperado facilmente com a ajuda de programas simples. Nas próximas páginas, abordarei alguns deles.

O primeiro deles é o **Recuva**, que pode ser baixado gratuitamente em <https://www.piriform.com/recuva/download> e conta com uma interface amigável e funcional.

Pode-se determinar o tipo de arquivo, o diretório procurado e o nível de busca (rápido ou profundo). Os arquivos encontrados devem ser exibidos na tela em seguida, juntamente com sua dificuldade de recuperação. Não é recomendado recuperar um arquivo no mesmo disco em que o arquivo original foi deletado.



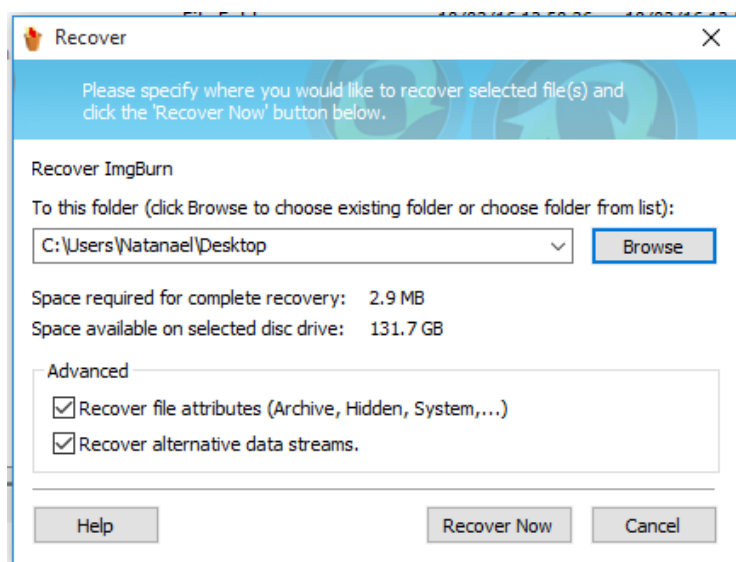
The screenshot shows the Recuva application window. At the top, there is a message: "For the best results, restore the files to a different drive." and a button labeled "Switch to advanced mode". Below this is a table with three columns: "Filename", "Path", and "Last Modified". The table lists several files, each with a checkbox in the first column, a colored circle icon, the filename, the full path, and the last modified date.

<input type="checkbox"/>	Filename	Path	Last Modified
<input type="checkbox"/>	aa.log	C:\Users\Natanael\Desktop\	30/09/201...
<input type="checkbox"/>	guaxinim.psd	C:\Users\Natanael\Desktop\Fábrica de Noobs\Desin...	30/04/201...
<input type="checkbox"/>	~WRL0002.tmp	C:\Users\Natanael\Desktop\Fábrica de Noobs\Projet...	18/01/201...
<input type="checkbox"/>	Logo.psd	C:\Users\Natanael\Desktop\Fábrica de Noobs\Desin...	24/11/201...
<input type="checkbox"/>	432 Mystery.psd	C:\Users\Natanael\Desktop\Fábrica de Noobs\Desin...	10/01/201...
<input type="checkbox"/>	Patrocinadores.psd	C:\Users\Natanael\Desktop\Fábrica de Noobs\Desin...	21/04/201...
<input type="checkbox"/>	Desafio Hacker 2016.psd	C:\Users\Natanael\Desktop\Fábrica de Noobs\Desin...	10/01/201...

Outro programa de funcionalidade semelhante é o Pandora Recovery (<http://www.pandorarecovery.com>), que exibe todos os diretórios de um disco em forma de árvore e destaca os que já foram excluídos.

Name	Size	Type	Date Created	Date Modified
Adobe		File Folder	09/11/16 21:38:34	09/12/16 15:15:06
Audacity		File Folder	09/12/16 16:51:22	09/12/16 16:52:54
Common Files		File Folder	07/10/15 06:05:28	09/28/16 19:23:38
ImgBurn		File Folder	10/02/16 13:50:26	10/02/16 13:50:26
InstallShield Installation Inform...		File Folder	09/20/16 14:26:31	09/20/16 15:58:10
Java		File Folder	09/18/16 11:17:14	09/18/16 11:17:14
MagiISO		File Folder	09/30/16 16:53:18	09/30/16 16:53:18
Microsoft Office		File Folder	09/11/16 21:05:27	09/20/16 04:56:40
NVIDIA Corporation		File Folder	09/11/16 20:06:05	09/28/16 19:23:38
obs-studio		File Folder	09/12/16 15:46:30	09/12/16 15:47:11

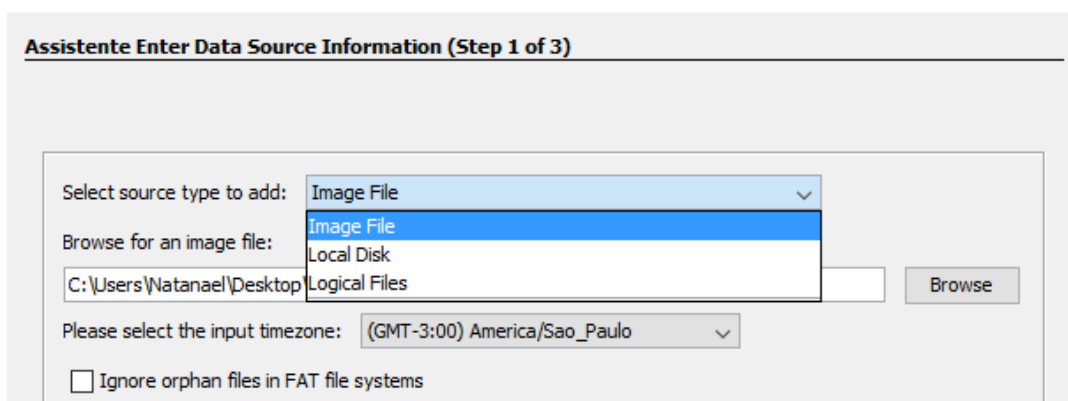
Basta escolher algum e iniciar o processo de recuperação.



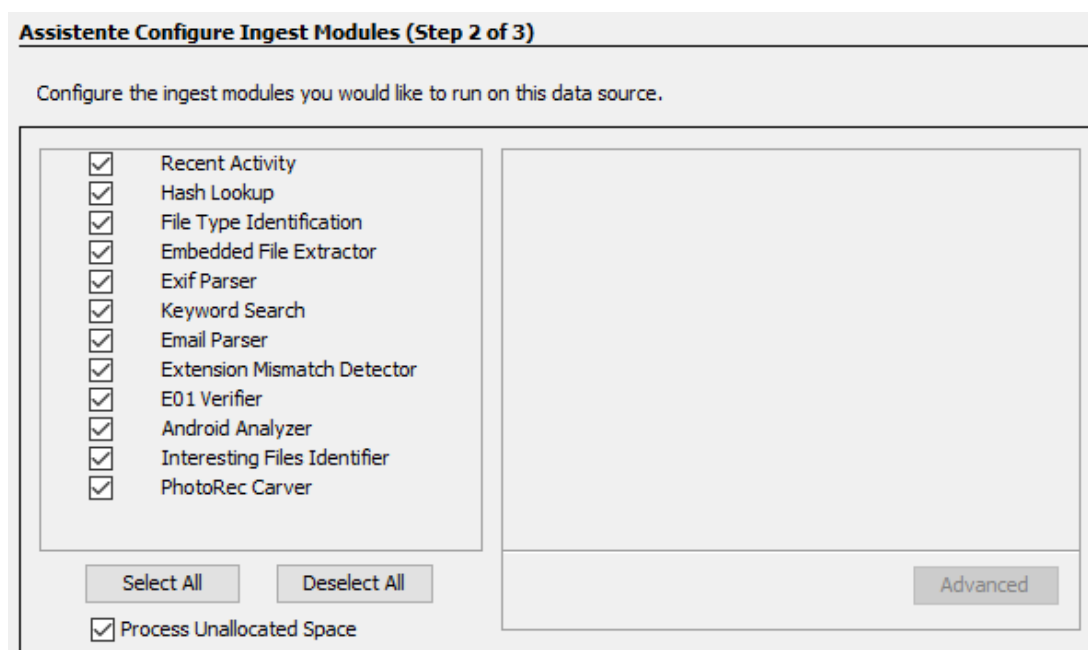
Os programas mostrados acima podem ser extremamente funcionais para usuários domésticos, mas uma investigação forense requer ferramentas mais robustas capazes, por exemplo, procurar arquivos excluídos de uma imagem de disco.

Uma das melhores ferramentas nessa categoria é o [Autopsy](http://www.sleuthkit.org/autopsy/), disponível gratuitamente em <http://www.sleuthkit.org/autopsy/>. Além da busca por arquivos, ele também conta com ferramentas de procura por palavras chave

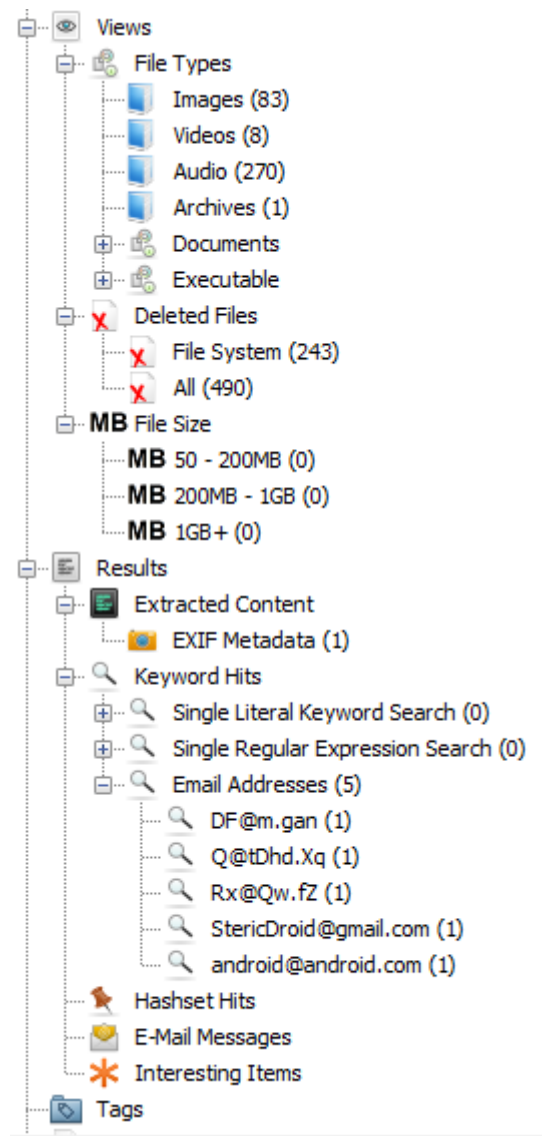
Assim que iniciado, o programa requer a inserção de uma fonte de dados, que pode ser um disco físico, um diretório ou uma imagem. O procedimento padrão é que seja inserido uma imagem, a fim de não danificar a evidência original.



Em seguida, devemos escolher as opções de análise para serem executadas.

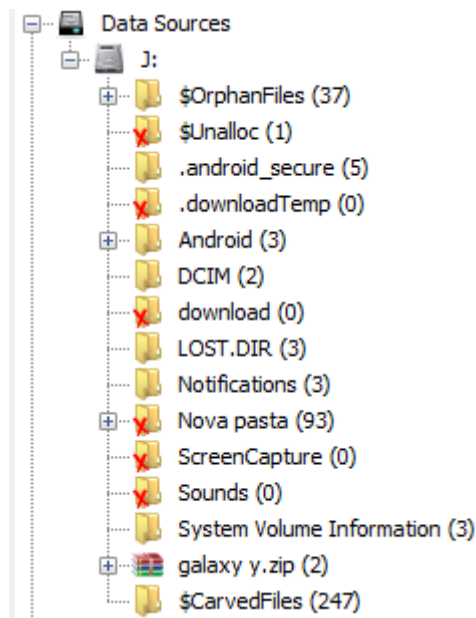


Assim que o disco for analisado, será possível ter acesso a tudo que foi encontrado, incluindo arquivos existentes e deletados, palavras-chave e endereços de e-mail.



Ao navegar por um diretório, os arquivos que foram apagados serão destacados. É possível tentar recuperar cada um deles.

Directory Listing		
Audio		
Table	Thumbnail	
Name	Location	Modified Time
hangout_dingtone.m4a	/img_J;/Notifications/hangout_dingtone.m4a	2011-01-01 0
✗ Alex Goot - Tiffany Alvord - Luke Conard - We	/img_J;/Alex Goot - Tiffany Alvord - Luke Conard - We Are Young (Ly...	2015-12-17 1
✗ 5 Seconds Of Summer - She Looks So Perfect.	/img_J;/Nova pasta/5 Seconds Of Summer - She Looks So Perfect.mp3	2015-12-07 1
✗ 5 Seconds Of Summer - She's Kinda Hot.mp3	/img_J;/Nova pasta/5 Seconds Of Summer - She's Kinda Hot.mp3	2015-12-06 0
✗ A Day To Remember - If it means a lot to you	/img_J;/Nova pasta/A Day To Remember - If it means a lot to you LY...	2015-04-30 1



Em nível de arquivos, o programa também apresenta um editor hexadecimal com retorno de strings.

Hex	Strings	File Metadata	Results	Indexed Text	Media
Page: 1 of 220			Page	Go to Page:	Jump to Offset 0
0x00000000:	49 44 33 04	00 00 00 00	01 13 54 58	58 58 00 00	ID3.....TXXX..
0x00000010:	00 12 00 00	03 6D 61 6A	6F 72 5F 62	72 61 6E 64major_brand
0x00000020:	00 64 61 73	68 00 54 58	58 58 00 00	00 11 00 00	.dash.TXXX.....
0x00000030:	03 6D 69 6E	6F 72 5F 76	65 72 73 69	6F 6E 00 30	.minor_version.0
0x00000040:	00 54 58 58	58 00 00 00	1C 00 00 03	63 6F 6D 70	.TXXX.....comp
0x00000050:	61 74 69 62	6C 65 5F 62	72 61 6E 64	73 00 69 73	atible_brands.is
0x00000060:	6F 36 6D 70	34 31 00 54	44 45 4E 00	00 00 15 00	o6mp41.TDEN.....
0x00000070:	00 03 32 30	31 35 2D 30	33 2D 33 30	20 32 33 3A	..2015-03-30 23:
0x00000080:	33 38 3A 33	38 00 54 53	53 45 00 00	00 0D 00 00	38:38.TSSE.....

VII. Análise de Criptografia

A criptografia pode ser definida como o conjunto de técnicas utilizadas para se cifrar a escrita, tornando-a ininteligível para os que não possuem conhecimento de tais técnicas.

Existem diversos métodos de criptografia, desde os mais rudimentares (como Cifra de César) até aqueles que precisariam de um computador quântico para serem quebrados (como algumas implementações de RSA). Recomendo se familiarizar com eles (e com os abordados no próximo capítulo) através da playlist sobre o assunto gravada no canal, disponível em <https://www.youtube.com/playlist?list=PLIevgZoV2cAi6wQj2J4HGfEqSilHK8s0M>.

Uma forma relativamente popular (e facilmente violável) de criptografia são os algoritmos de base numérica, como o binário, hexadecimal e octal. Eles funcionam substituindo os caracteres do texto por valores correspondentes na tabela ASCII.

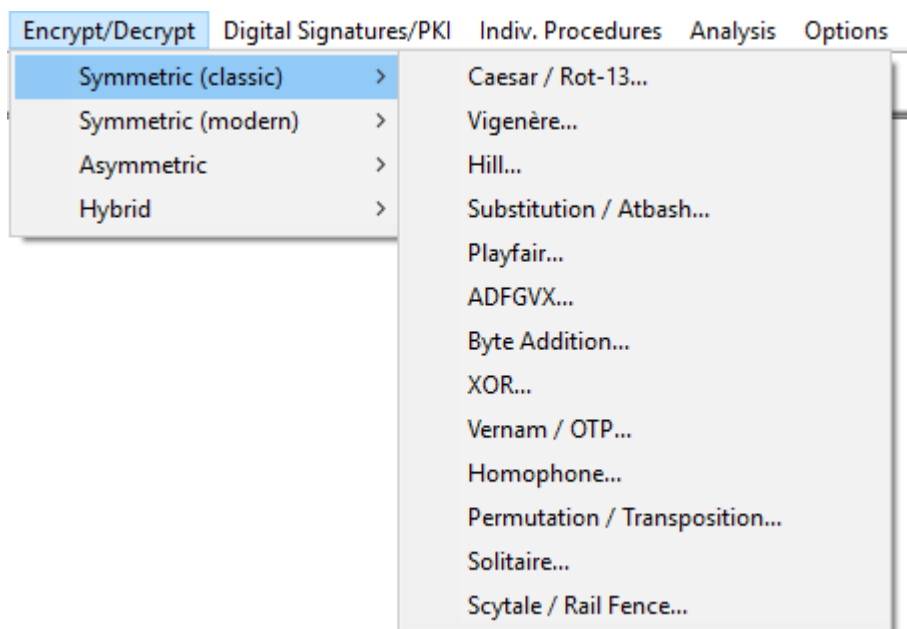
ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	\$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(72	48	110	H	104	68	150	h
9	9	11		41	29	51)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	
29	1D	35		61	3D	75	=	93	5D	135]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

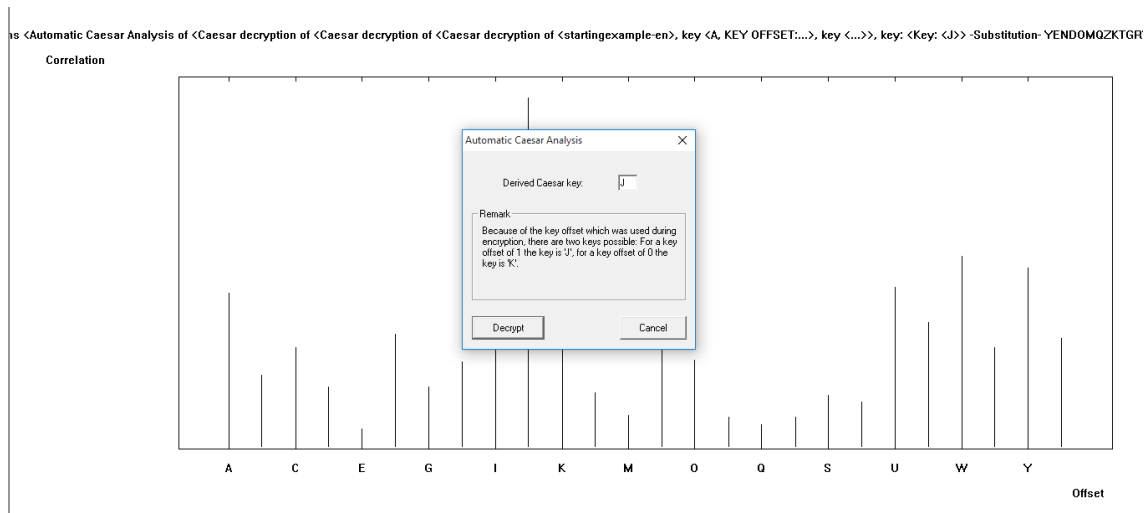
A análise de tais cifras depende apenas de identificar a cifra utilizada (~~ou de tentar todas, se você for absurdamente ruim~~). Para isso, consulte a tabela abaixo e as decifre utilizando o [Unit-Conversion.info](http://www.unit-conversion.info/texttools/) em <http://www.unit-conversion.info/texttools/>.

Criptografia	Texto cifrado	Características
Binário	01101000 01100101 01101100 01101100 01101111	Presença apenas de caracteres 1 e 0.
Hexadecimal	68 65 6c 6c 6f	Presença das letras a,b,c,d,e,f e separação a cada 2 caracteres.
Octal	150 145 154 154 157	Geralmente separado a cada 3 caracteres, começando por 1.
ASCII	104 101 108 108 111	Mesmas do Octal, porém sem valores maiores que 127.

Para demais criptografias, utilizaremos o **CrypTool 1**, disponível em <https://www.cryptool.org/en/cryptool1>. O programa permite realizar uma série de ataques contra diversos tipos de criptografia, e funciona melhor se forem adicionados arquivos em txt contendo textos em seu idioma nativo na pasta **CrypTool\reference** para servir de referência em algumas análises.



Uma mensagem em Cifra de César pode ser facilmente quebrada através do método de análise por frequência de caracteres.

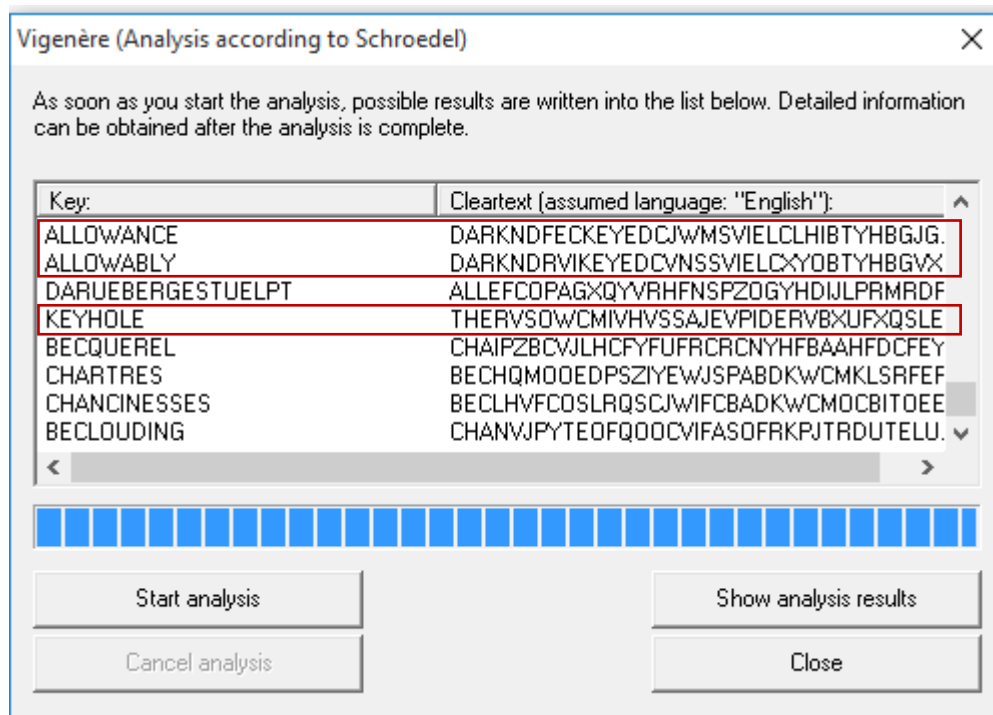


Outra forma é testar as 26 chaves possíveis e procurar por uma sequência que faça sentido, o que pode ser feito em <http://www.dcode.fr/caesar-cipher>.

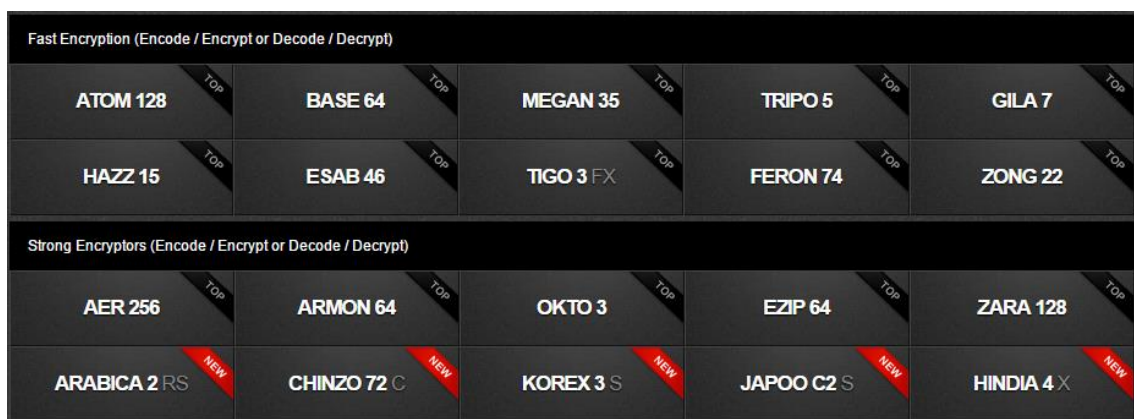


Caso nenhuma das sequências corresponda a uma mensagem compreensível, é provável que ela esteja cifrada em Vigenère. Tal criptografia também pode ser quebrada de forma semelhante, mas possui menos chance de sucesso. Nesse ataque, o programa irá retornar possíveis chaves, e cabe ao investigador procurar quais fazem mais sentido.

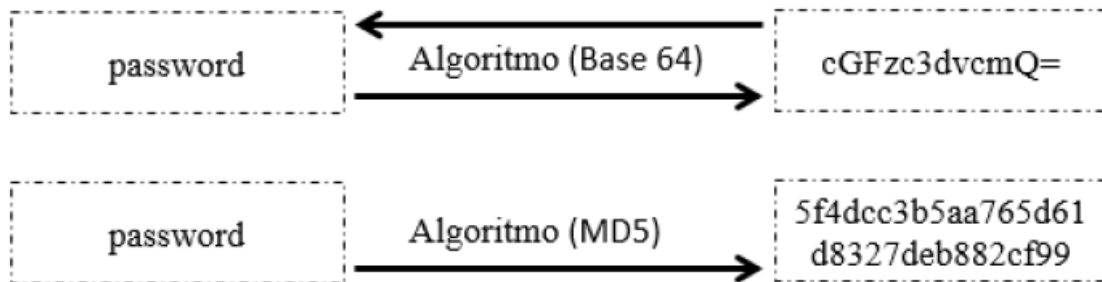
Note que caso apenas parte do texto descriptografado faça sentido, é provável que a chave real corresponda a parte da chave indicada pelo programa.



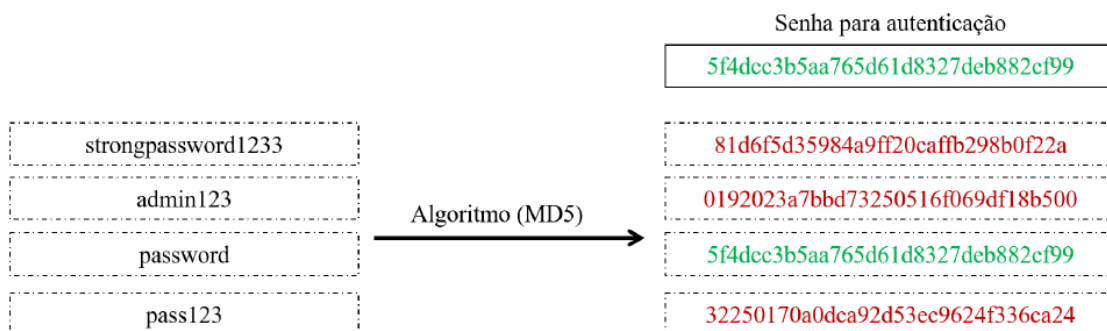
Existem também os métodos de critpografia moderna como Base64, Megan35, Feron74, entre outros. Nesse caso, o melhor a se fazer é testar possibilidades utilizando algum serviço como o Crypto (<http://crypto.pw/encryptors>), pois é provável que a cifra foi codificada nesse site.



Já as sequências de hash podem ser quebradas em sites como o HashKiller (<https://hashkiller.co.uk/>) ou o Crackstation (<https://crackstation.net>), mas não podem ser decodificadas. Isso acontece porque, ao contrário dos métodos de criptografia estudados até agora, essas funções são unidirecionais. Isso significa que é possível criptografar utilizando um algoritmo, mas não é possível fazer o processo contrário. Esses recursos são utilizados, por exemplo, para realizar autenticações de login ou armazenar senhas em bancos de dados.



A única forma de se quebrar uma função de hash, como MD5 é a partir de um ataque de força bruta, onde uma lista com possíveis senhas e suas respectivas codificações é comparada com a hash até uma correspondência ser encontrada. Logo, uma hash gerada de uma senha forte é resistente a ataques de força bruta.



Caso não saibamos qual o algoritmo utilizado em uma hash, podemos encontrar pistas dele utilizando o [hashID](https://github.com/davidaurelio/hashids-python) (<https://github.com/davidaurelio/hashids-python>) , script feito em Python que retorna possíveis algoritmos através da quantidade de bits presentes na função.

```
4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877
Analyzing '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877'
[+] Snefru-256
[+] SHA-256
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94
[+] GOST CryptoPro S-Box
[+] SHA3-256
[+] Skein-256
[+] Skein-512(256)
```

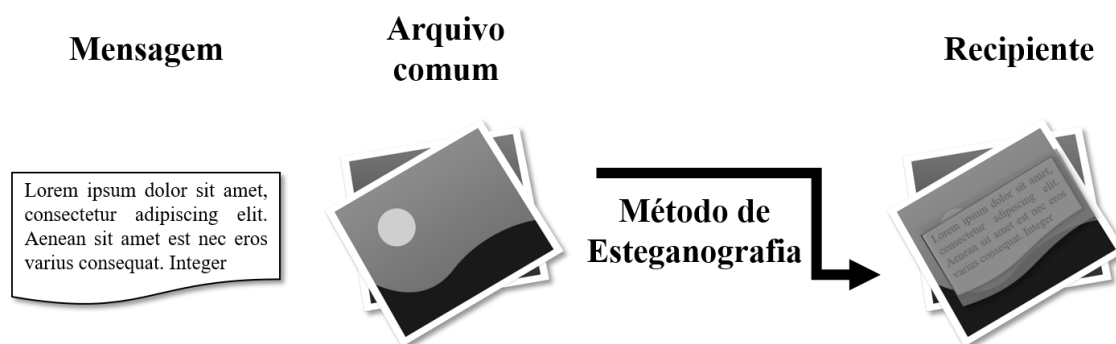
VIII. Análise de Esteganografia

A esteganografia é a técnica usada para esconder a própria dentro de um recipiente, normalmente um arquivo que não levante suspeitas.

Tem como objetivo impedir que tais dados ocultos sejam descobertos por terceiro, e funciona através da substituição dos bytes menos relevantes do arquivo recipiente pelos bytes da mensagem real, sem grandes mudanças na primeira.

Existem diversas ferramentas que possibilitam a esteganografia, desde as mais simples e identificáveis até as mais complexas, feitas com programas próprios para o assunto.

Por se tratar de um curso sobre computação forense, a abordagem estará voltada para a identificação e quebra de métodos de esteganografia, e é interessante que você conheça o funcionamento dos mesmos para melhor compreensão dos procedimentos apresentados.

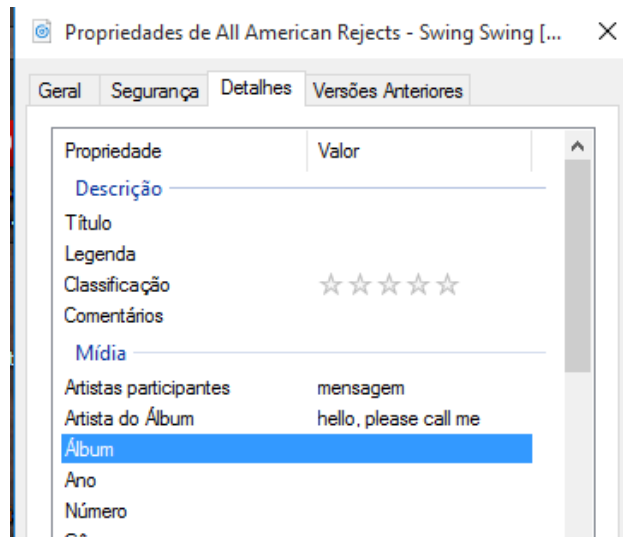


A análise de esteganografia pode ser facilitada se um ou mais dos seguintes fatores forem conhecidos:

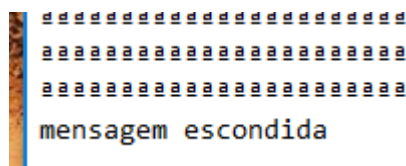
- Método de esteganografia
- Recipiente
- Mensagem escondida

As formas mais simples de esteganografia consistem em esconder mensagens importantes nos detalhes sutis de um arquivo, como por exemplos nos campos “artista” e “álbum” de uma música.

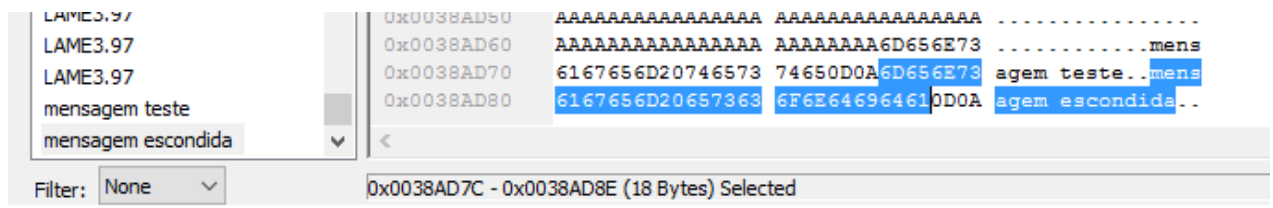
Tais mensagens podem ser facilmente detectadas analisando-se a aba **Detalhes** no menu **Propriedades do arquivo**. Daí, eis a importância de se realizar uma análise atenta em cada detalhe de uma evidência suspeita.



Outra técnica simples consiste em inserir uma mensagem em texto dentro de outro arquivo, que pode ser recuperada abrindo o recipiente pelo Bloco de Notas.



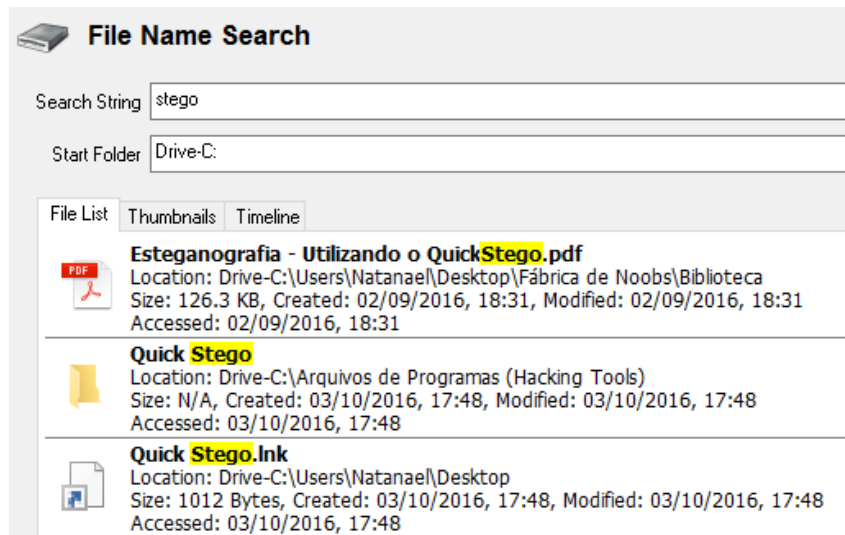
Mensagens desse tipo podem ser facilmente encontradas efetuando-se uma busca por strings. No exemplo abaixo, usamos o **OSForensics**.



Já a esteganografia feita utilizando um editor hexadecimal também pode ser facilmente recuperada através da busca de possíveis headers no código hexadecimal do arquivo.

Outros tipos de esteganografia (principalmente as feitas a partir de programas próprios) são mais complexos de se detectar. Porém, tais programas quase sempre deixam rastros de sua existência na máquina alvo. Buscar por eles pode ser uma boa forma de identificar o método de esteganografia, facilitando o resto da investigação.

Isso pode ser feito através de uma busca por palavras-chave relacionadas a esteganografia. No exemplo abaixo, buscamos por “stego” na ferramenta de busca do **OSForensics**. Recomendo orientar a busca conforme os nomes dessa lista https://en.wikipedia.org/wiki/Steganography_tools.



Uma vez identificado o programa, podemos pesquisar pelos seus formatos de saída e procurar arquivos que correspondem a esse formato.

Também é interessante observar as seguintes ocorrências:

- **Arquivos grandes demais para seu formato:** uma imagem com 10MB certamente possui algo dentro dela.
- **Imagens em BMP:** alguns programas de ocultação de dados em imagens costumam retorná-las nesse formato.
- **Ruídos de áudio “estranhos”:** é possível fazer esteganografia através de espectogramas, e os resultados retornam áudios um tanto incomuns.
- **Pixelização incomum:** imagens podem apresentar contornos diferentes quando são utilizadas como recipiente para esteganografia.



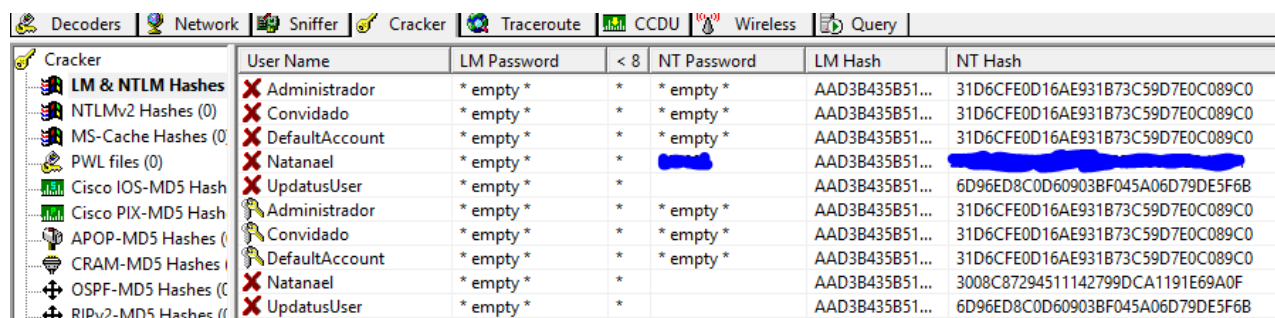
IX. Quebra de Senhas

Durante o processo de investigação forense frequentemente nos deparamos com arquivos, partições, discos ou máquinas inteiras protegidas por senha. Nessas situações, é comum utilizarmos programas para quebrar tais senhas.

Existem três tipos de ataques:

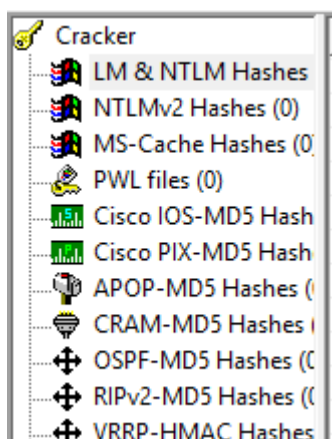
- **Retorno da própria senha:** alguns programas conseguem ser vulneráveis o bastante para exibir a senha procurada (criptografada ou não) sem maiores problemas. Pouco comum.
- **Retorno da hash da senha:** a senha em si não é armazenada, mas sim a sua hash corresponde. Comum para hacking de contas de usuário do Windows, por exemplo.
- **Ataque de força bruta:** não temos acesso tanto à senha quanto à sua hash. É necessário tentar possíveis senhas até se obter sucesso.

O Windows costuma armazenar a hash da senha de suas contas de usuário. Tais hashes podem ser obtidas com programas como o **OSForensics** ou o **Cain & Abel** (<http://www.oxid.it/cain.html>).

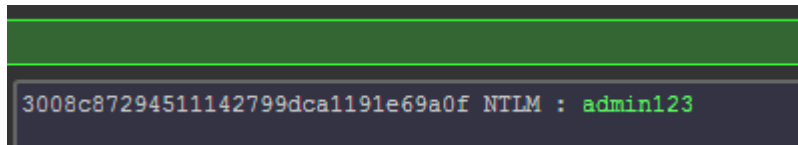


	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash
✗	Administrador	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
✗	Convidado	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
✗	DefaultAccount	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
✗	Natanael	* empty *	*	[REDACTED]	AAD3B435B51...	[REDACTED]
✗	UpdatusUser	* empty *	*		AAD3B435B51...	6D96ED8C0D60903BF045A06D79DE5F6B
✗	Administrador	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
✗	Convidado	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
✗	DefaultAccount	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
✗	Natanael	* empty *	*		AAD3B435B51...	3008C87294511142799DCA1191E69A0F
✗	UpdatusUser	* empty *	*		AAD3B435B51...	6D96ED8C0D60903BF045A06D79DE5F6B

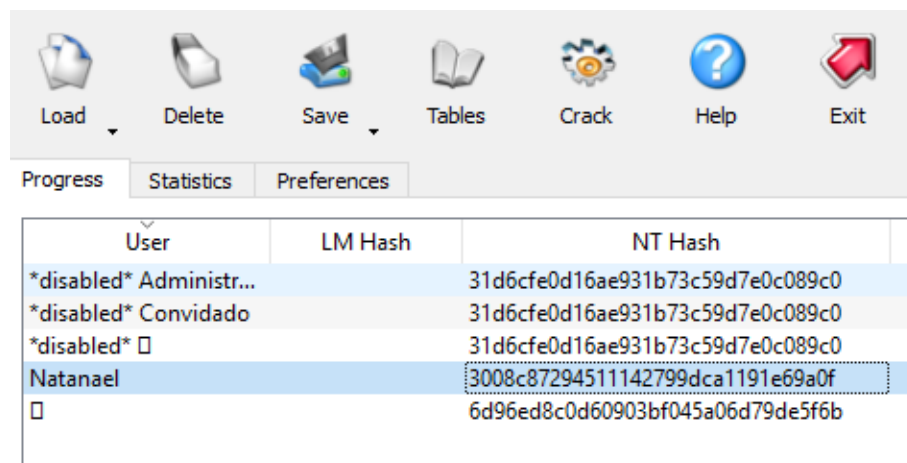
Note que o programa também oferece a possibilidade de crackear diversos outros serviços:



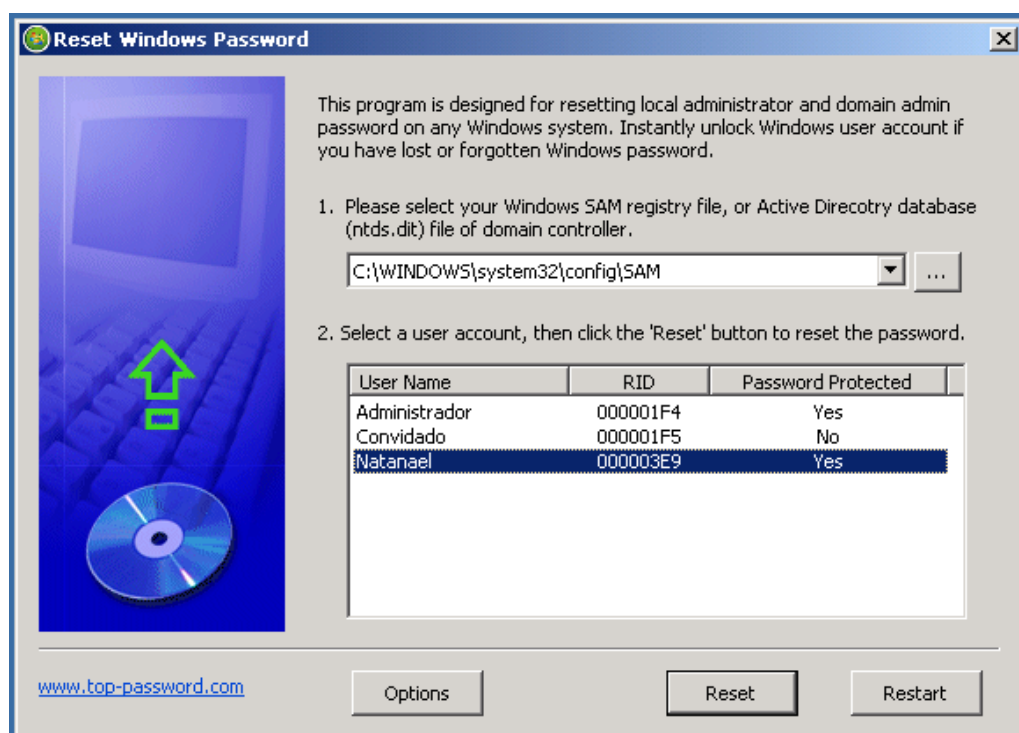
Uma vez obtida a hash, basta quebrá-la para se retornar a senha original. Senhas comuns tem mais chance de serem quebradas com sucesso.



Outra ferramenta semelhante é o [ophcrack](https://sourceforge.net/projects/ophcrack/?source=typ_redirect) (https://sourceforge.net/projects/ophcrack/?source=typ_redirect), que permite realizar a mesma função a partir da opção Local SAM.



Caso disponhamos de uma máquina cujo acesso ao desktop não está disponível, podemos redefinir as senhas de usuário através de programas graváveis em imagens ISO, como o [Windows Password Genius](http://www.isunshare.com/windows-password-genius.html) (<http://www.isunshare.com/windows-password-genius.html>).



Também podemos obter as senhas de usuário de uma máquina recuperando os arquivos presentes nos seguintes diretórios através de um live CD ou um cabo USB.

- C:\Windows\system32\config\SAM
- C:\Windows\system32\config\SYSTEM



Com os arquivos em mãos, basta utilizar a opção **Encrypted SAM** do **ophcrack** na partição em que os mesmos se encontram.

Progress	Statistics	Preferences
User	NT Hash	
disabled Administrador	31d6cfe0d16ae931b73c59d7e0c089c0	
disabled Convidado	31d6cfe0d16ae931b73c59d7e0c089c0	
Natanael	209c6174da490caeb422f3fa5a7ae634	

Existem também situações em que é necessário quebrar a senha de um arquivo, normalmente zipados ou documentos do Office. Esse tipo de ataque é feito através da força bruta, o qual consiste em tentar todas as senhas de uma lista na expectativa de que uma delas corresponda a senha procurada.

**Arquivo
com senha**



Wordlist

- ✗ apppl
- ✗ apppe
- ✗ appla
- ✗ applp
- ✗ appll
- ✓ apple

**Senha
descoberta**



Porém, bastam alguns conhecimentos de análise combinatória para se perceber que esse método se torna inviável para senhas mais complexas. Porém, para senhas simples (poucos caracteres ou palavras de dicionário) pode se tornar eficaz.

O primeiro passo lançarmos um ataque é criarmos a lista de senhas, conhecida no vocabulário técnico por wordlist. A grosso modo, existem dois tipos de wordlists: as feitas por combinação pura, e as feitas com base em um dicionário. As primeiras são eficazes para senhas curtas, principalmente

numéricas. Já as segundas podem servir em casos onde a senha em questão corresponde a uma palavra.

Wordlists do primeiro tipo podem ser facilmente criadas utilizando o **crunch** (<https://sourceforge.net/projects/crunch-wordlist/>), ferramenta nativa de diversas distribuições Linux e que também conta com versão em Windows.

A sintaxe fundamental do crunch é:

```
crunch mínimo máximo set de caracteres -o arquivo de saída.txt
```

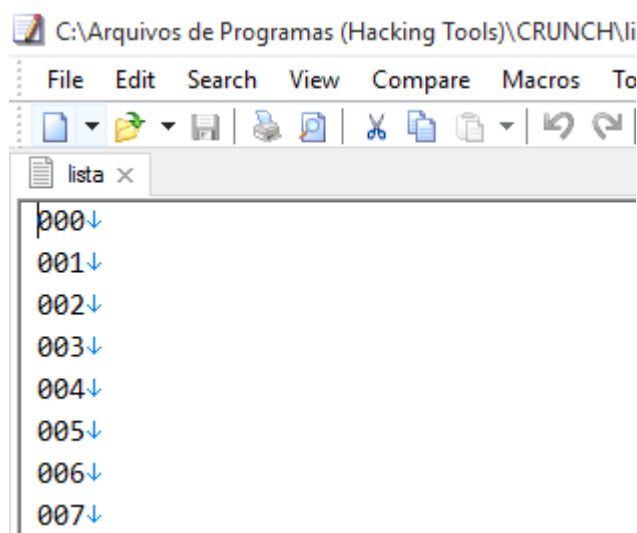
Em que:

- Mínimo e máximo correspondem, respectivamente, a quantidade mínima e máxima de caracteres nas senhas.
- Set de caracteres correspondem aos caracteres que podem ser utilizados na criação das senhas.
- Arquivo de saída corresponde ao arquivo onde a wordlist será salva.

Assim, se quisermos criar uma lista com todas as senhas numéricas (0 a 9) de 3 a 6 caracteres, usamos:

```
\CRUNCH>crunch 3 6 0123456789 -o lista.txt
```

O arquivo será salvo no diretório onde o programa está instalado. Para lidar com a leitura de listas grandes, recomendo o **Em Editor** (<http://appnee.com/emeditor-pro-universal-registration-keys-collection/>).



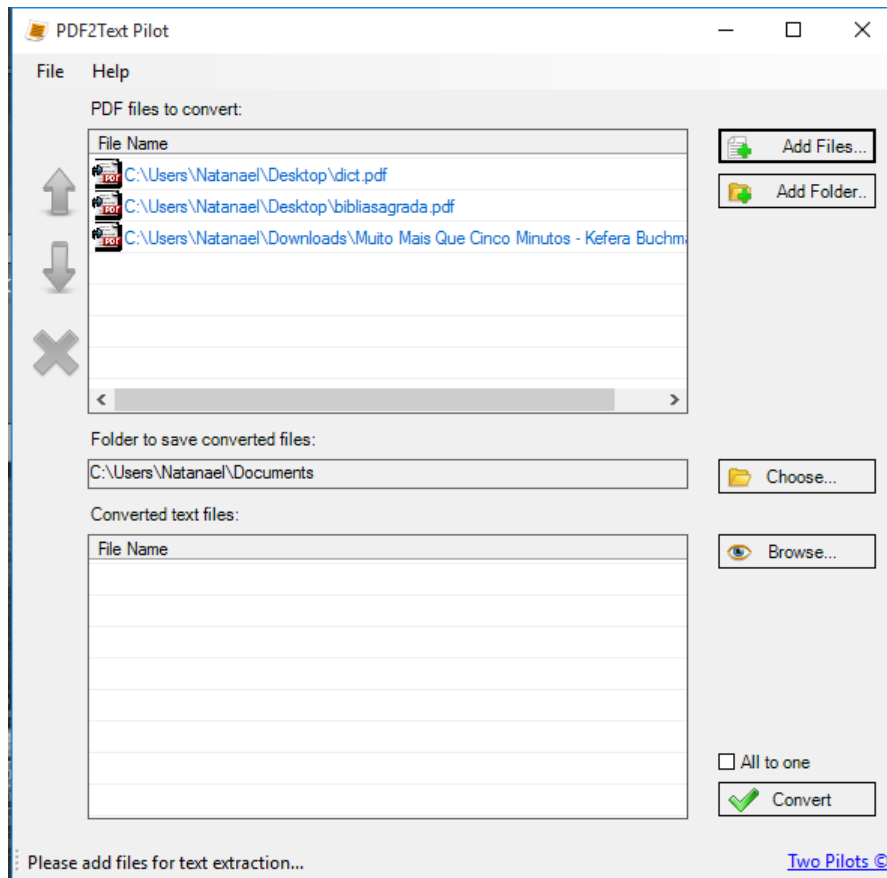
Já as worldlists de dicionário podem ser criadas através do [WordListCompiler](http://word-list-compiler.software.informer.com/download/), ferramenta gratuita e eficaz disponível em <http://word-list-compiler.software.informer.com/download/>.

Seu funcionamento é simples: adicionamos um arquivo de texto qualquer e ele procura extrair o máximo possível de palavras desse texto. Ele trabalha apenas com arquivos em txt, então é interessante procurar por livros nesse formato ou convertê-los para txt antes de montar a wordlist.

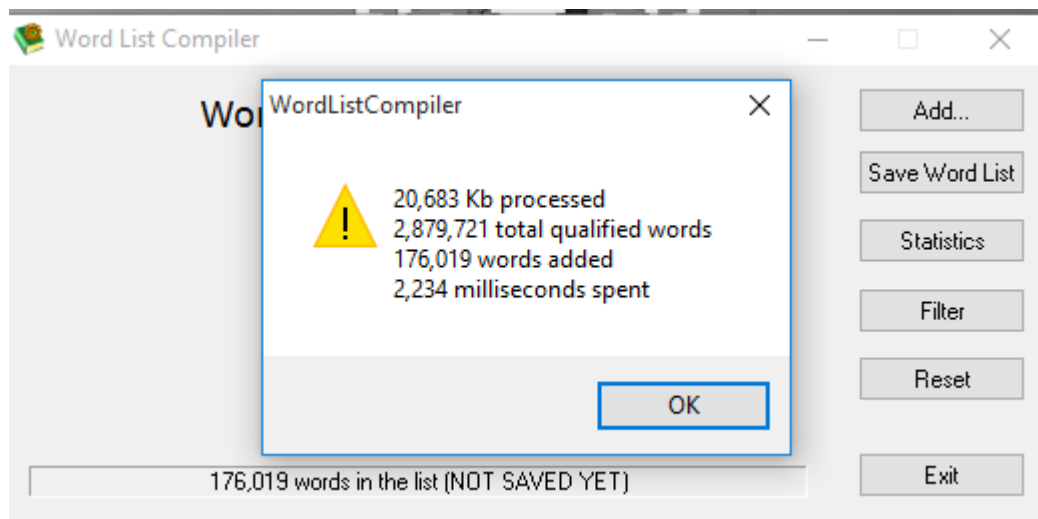
Boas opções de arquivo base são:

- Dicionário;
- Bíblia;
- Best-sellers;
- Listas de senhas mais comuns;
- Listas de palavrões;
- Relações com nomes de pessoas, cidades, times de futebol, números de telefone.

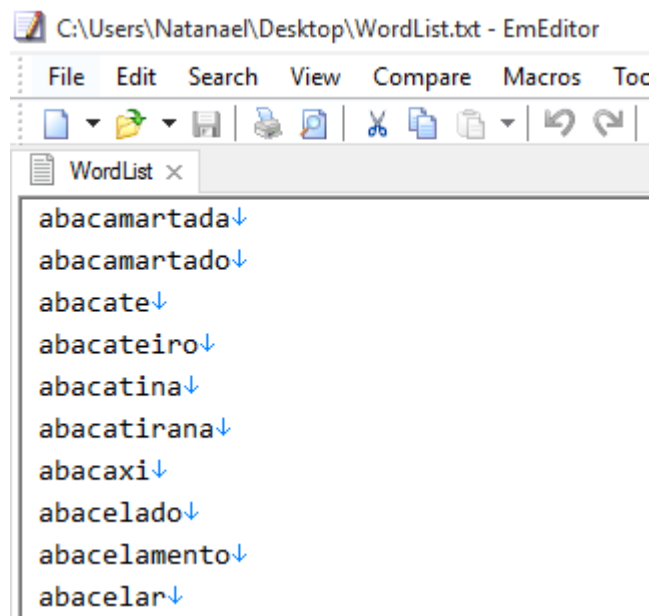
PDF's, por exemplo, podem ser facilmente convertidos para texto com o uso do PDF2Text Pilot (<http://www.colorpilot.com/extract-pdf-text.html>). Basta adicioná-los e iniciar a conversão.



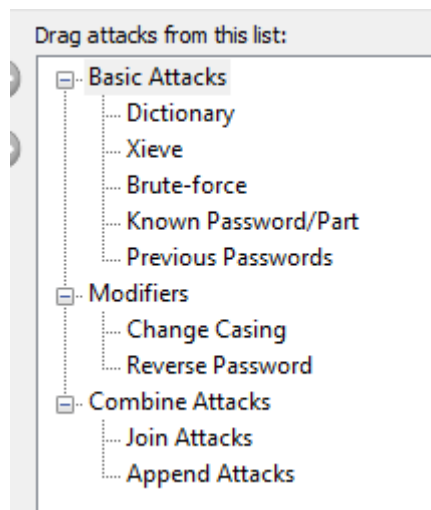
Todos os livros são convertidos em arquivos txt, prontos para serem usados na criação da wordlist. Basta adicioná-los no programa e iniciar a criação.



Uma vez criada, a wordlist já está pronta para ser usada. Lembre-se que um ataque tem mais chances de ser bem-sucedido se uma boa wordlist for utilizada.

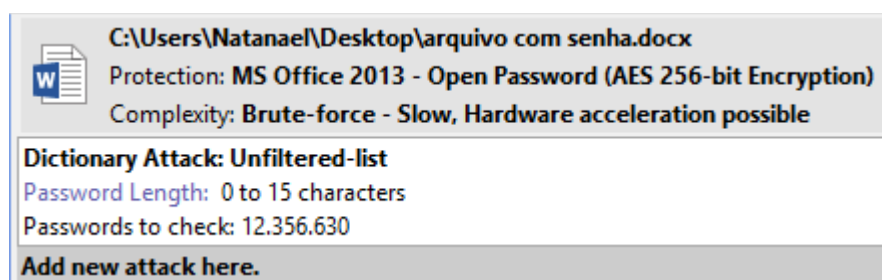


Voltando ao tema do capítulo, podemos realizar ataques de força bruta em arquivos com senha utilizando o Passware Kit Professional (<https://www.passware.com/kit-standard-plus/>). Uma vez selecionado o alvo, o programa permite configurar e combinar uma série de ataques possíveis. Vale lembrar que tais ataques levam tempo, e um ataque bem configurado pode economizar

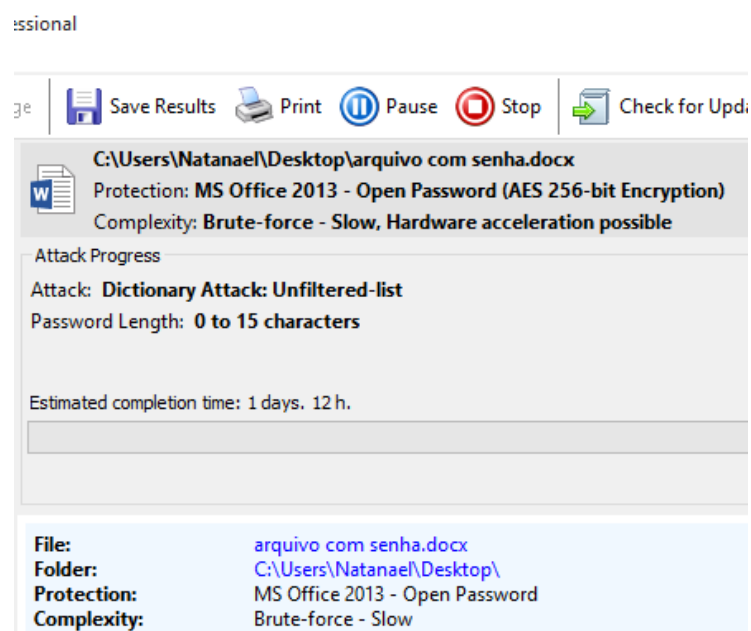


Vale lembrar que tais ataques levam tempo, e um ataque bem configurado pode economizar várias horas de alto consumo de RAM.

Uma vez configurado, basta rodá-lo e aguardar seu resultado.



Dependendo da configuração escolhida, ataques podem levar horas ou dias para serem concluídos, e a única forma de otimizar tal processo é através da aquisição de mais memória RAM. Meu Intel Core i3 com 4GB de RAM apresentou uma taxa de aproximadamente 105 senhas por segundo.



X. Auditoria no Android

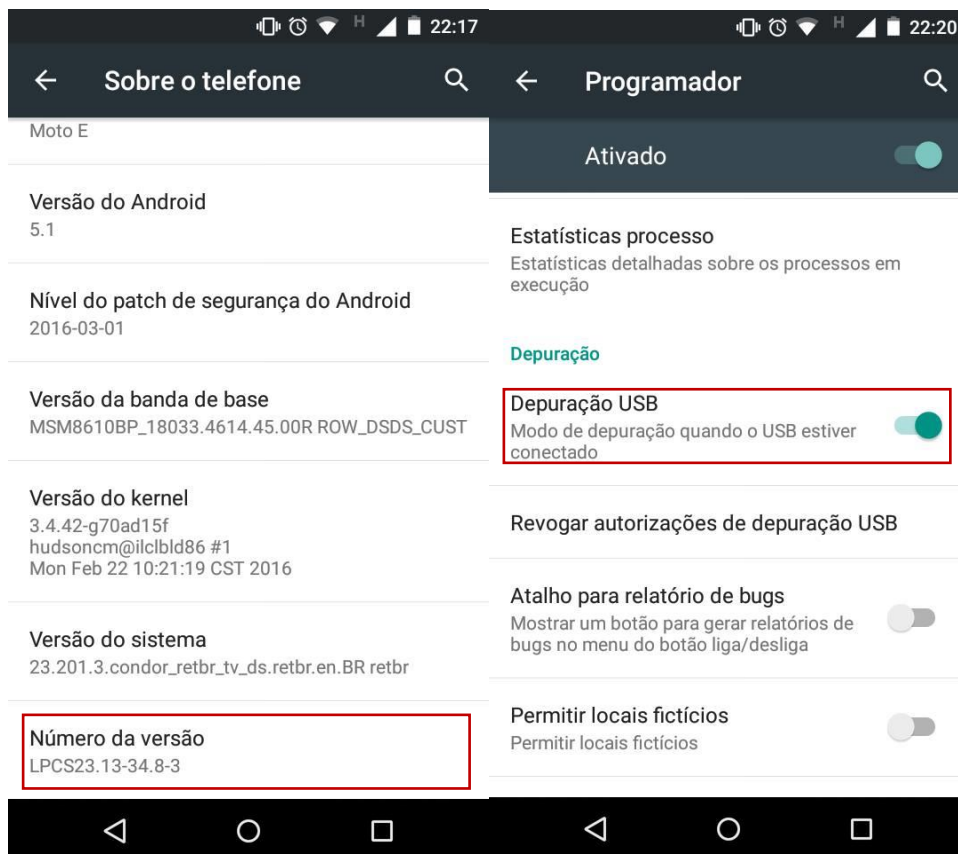
Os smartphones são cada vez mais populares em todo mundo, realizando não apenas as funções clássicas de um telefone, mas também armazenamento de fotos, envio de e-mails, SMS, agenda e aplicativos. Por essa razão, celulares também são estudados como evidências forenses.

O trabalho de auditoria em um smartphone pode se tornar árduo caso o dispositivo não possua root ou a senha de desbloqueio seja desconhecida. Por essa razão, abordarei nessa apostila os procedimentos forenses para um dispositivo Android que possua:

- Acesso ao root
- Senha de desbloqueio conhecida

Primeiramente, será necessário instalar os drivers correspondentes à marca do celular no computador. Isso pode ser feito com uma simples busca no Google.

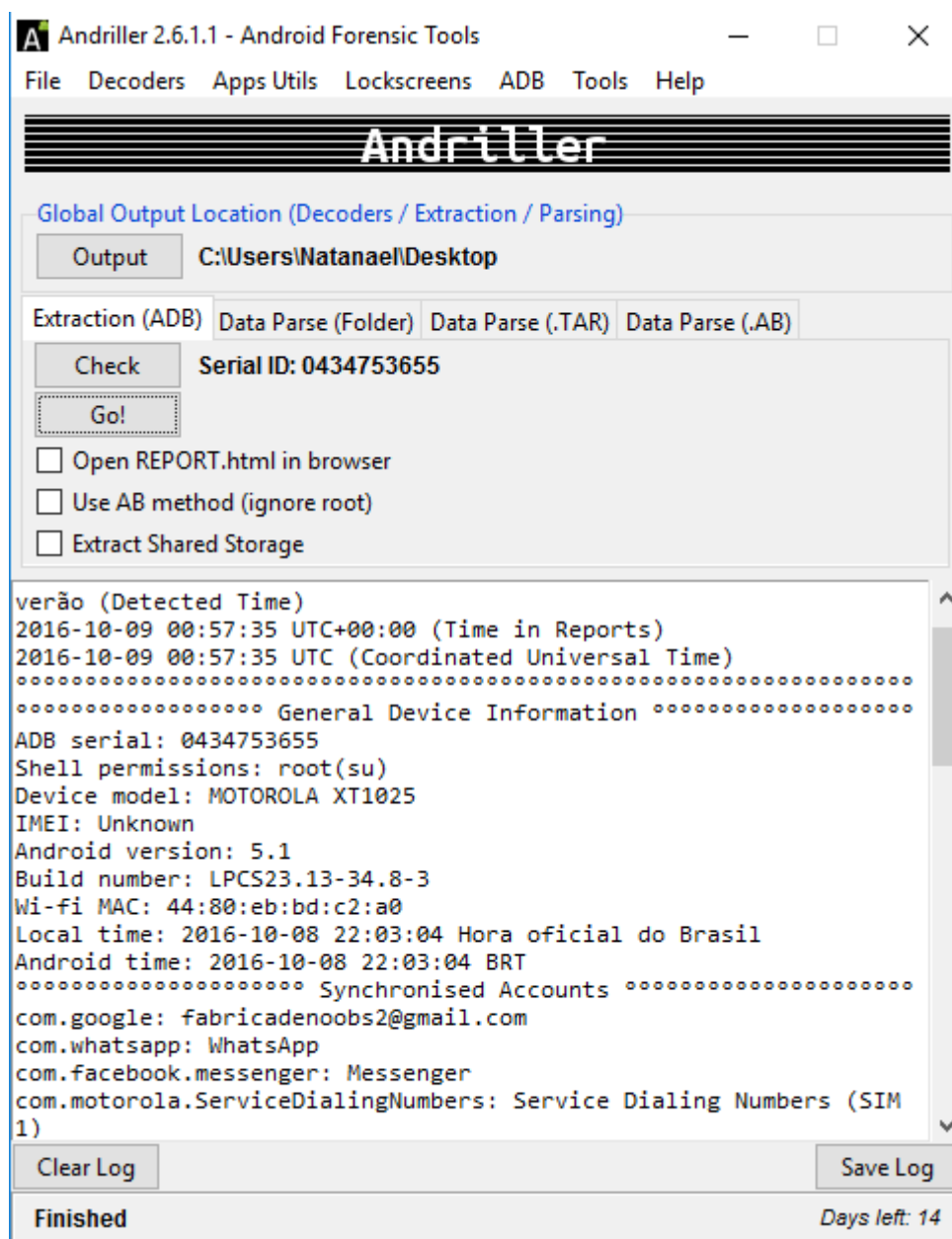
Em seguida, deveremos ativar as Opções de Desenvolvedor no aparelho em questão. Para tanto, vá em [Configurações > Sobre o telefone](#) e clique repetidas vezes no campo [Número da versão](#).



Uma vez ativadas, vá em Programador e marque Depuração USB. Seu dispositivo estará pronto para ser auditado.

Em seguida, usaremos o **Andriller** (<http://andriller.com>) para extrair as informações úteis. O programa é pago, ~~mas por incrível que pareça basta usar a opção Migrate License para conseguir outra trial.~~

Uma vez no programa, devemos ligar o dispositivo ao computador via cabo USB, definir um diretório, clicar em **Check** e em seguida clicar em **Go!**. Ele começará a realizar a auditoria do aparelho. Caso queira que seja feito o mesmo no cartão de memória, marque **Extract Shared Storage**.



Assim que o processo for terminado, os resultados serão salvos para uma pasta previamente identificada.

	MOTOROLA_XT1025_2016-10-08_22.03.04			
	Nome	Data de modificaç...	Tipo	Tamanho
Trabalhc	db	08/10/2016 22:04	Pasta de arquivos	
ids	wa_media	08/10/2016 22:04	Pasta de arquivos	
ntos	accounts	08/10/2016 22:04	Vivaldi HTML Doc...	2 KB
	andriller	08/10/2016 22:05	Documento de Te...	5 KB
	call_logs	08/10/2016 22:04	Vivaldi HTML Doc...	2 KB
de Proj	chrome_history	08/10/2016 22:04	Vivaldi HTML Doc...	14 KB
astboot	contacts	08/10/2016 22:04	Vivaldi HTML Doc...	49 KB

O relatório completo da auditoria está presente em [REPORT.html](#). Lá, podemos encontrar todas as informações sobre o dispositivo, como registro de chamadas, histórico de navegação, contas, logs de aplicativos (Whatsapp e Facebook) etc.

This report was generated using Andriller # (This field is editable in Preferences)

This report was generated using Andriller version 2.6.1.1 on 2016-10-08 22:03:04 Hora oficial do Brasil

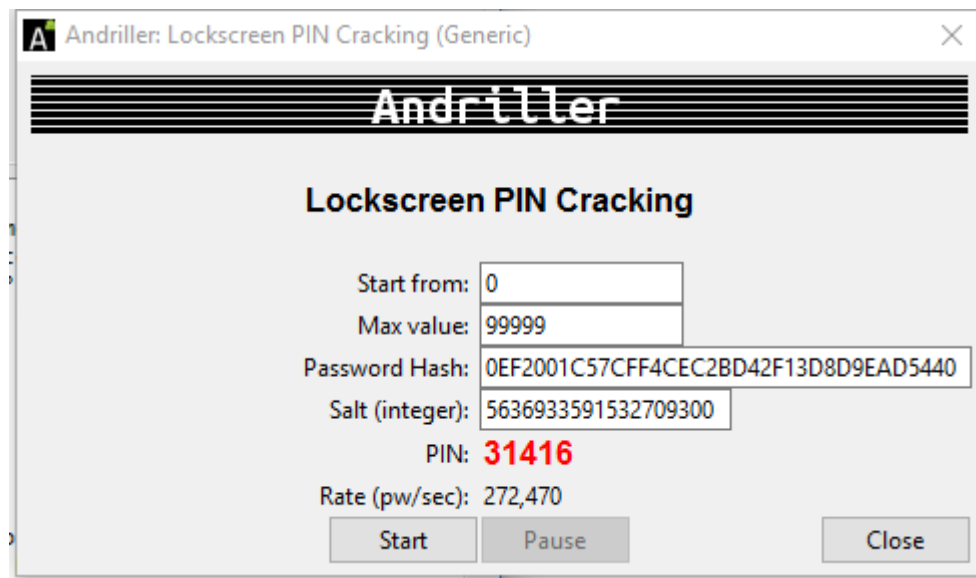
[Andriller Report] MOTOROLA XT1025 | IMEI:Unknown

Type	Data
ADB serial:	0434753655
Android ID:	e3c3faf74c6e889c
Shell permissions:	root(su)
Manufacturer:	MOTOROLA
Model:	XT1025
IMEI:	Unknown
Android version:	5.1
Build name:	LPSC23.13-34.8-3
Wifi MAC:	44:80:eb:bd:c2:a0
Bluetooth MAC:	44:80:eb:bd:c2:9f
Bluetooth name:	XT1025
Local time:	2016-10-08 22:03:04 Hora oficial do Brasil
Android time:	2016-10-08 22:03:04 BRT
Accounts:	com.google: fabricadenoobs2@gmail.com com.whatsapp: WhatsApp com.facebook.messenger: Messenger com.motorola.ServiceDialingNumbers: Service Dialing Numbers (SIM 1)
Security (Gesture Hash):	da39a3ee5e6b4b0d3255bfef95601890afd80709
Security (Lockscreen Pattern):	None
Security (Lockscreen Hash):	5FCF9F698913E652C4156FCE3E50987307A50EF2001C57CFF4CEC2BD42F13D8D9EAD5440
Security (Lockscreen Salt):	5636933591532709300
System:	Synchronised Accounts (4)
System:	Wi-Fi Passwords (9)
System:	Android Download History (1)
Web browser:	Google Chrome History (30)
Communications data:	Contacts (281)
Communications data:	Call logs (8)
Communications data:	SMS Messages (4)
Applications data:	Facebook Messages (1,311)
Applications data:	WhatsApp Contacts (133)
Applications data:	WhatsApp Calls (3)
Applications data:	WhatsApp Messages (36,496)

andriller.com # (This field is editable in Preferences)

Podemos ainda descobrir a senha do dispositivo inserindo os valores presentes nos campos [Lockscreen Hash](#) e [Lockscreen Salt](#) na opção Crack

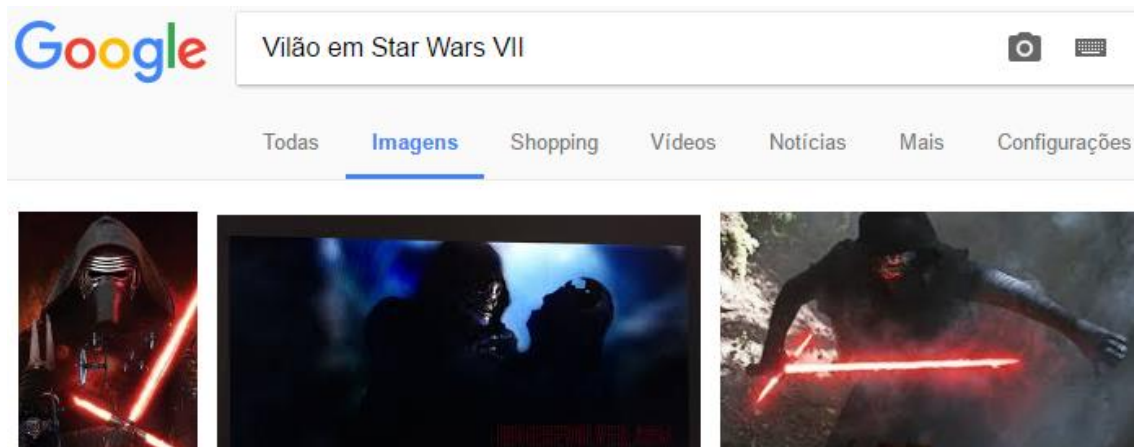
PIN (para senhas numéricas) ou Crack Password (para senhas de qualquer tipo). A quebra é feita através de um ataque de força bruta.



XI. Busca Reversa

Todos sabemos que a Internet é uma verdadeira teia de informações. Praticamente qualquer ação que realizamos online deixa rastros, e encontrar tais rastros pode ser fundamental em uma investigação ou busca forense.

Em uma busca padrão, procuramos por alguma palavra-chave, que nos leva à determinado conteúdo. Por exemplo, se pesquisamos por “Vilão em Star Wars VII”, somos imediatamente direcionados para resultados sobre Kylo Ren.



Já em uma busca reversa, realizamos o processo contrário, normalmente em algum material gráfico como vídeo ou imagem. Assim, ao realizarmos o procedimento com a fotografia de Kylo Ren, somos direcionados para páginas que nos dão maiores informações sobre o personagem.



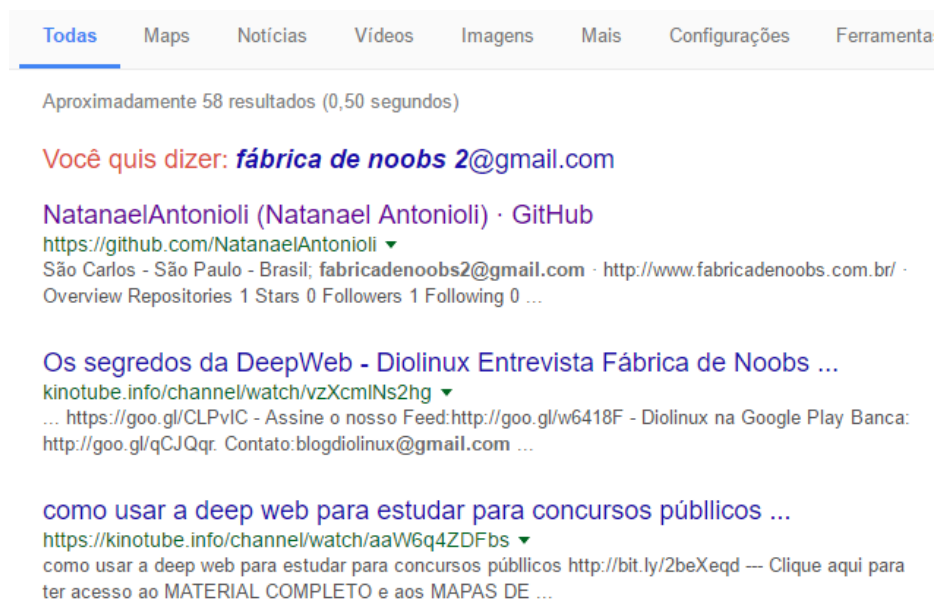
Tal ferramenta, apesar de parecer banal, tem inúmeras utilidades. Por exemplo, se temos uma situação na qual uma pessoa ameaça outra através de alguma rede social exibindo a foto de uma arma, podemos pesquisar a mesma imagem e verificar que, talvez, ela tenha sido apenas retirada da internet.

Outra finalidade da busca reversa é procurar por atividades realizadas por determinada pessoa na Internet. Se descobrimos que determinado endereço de e-mail foi utilizado para hospedar um site, podemos realizar buscas reversas nesse endereço para talvez encontrar outros serviços que estejam vinculados a ele, tais como contas em redes sociais – as quais podem revelar o paradeiro do indivíduo que estamos procurando.

Além disso, realizar uma busca reversa em materiais de mídia (músicas, imagens ou vídeos) pode nos ajudar a descobrir a veracidade dos mesmos, além de detectar possíveis violações de direitos autorais e fotomontagens, desmascarando farsas da Internet.

Antes de realizarmos buscas propriamente reversas, é importante enfatizarmos algumas opções adicionais de buscas simples que o próprio Google nos fornece, mas muitas vezes são ignoradas.

Uma delas é a função de **busca ao pé da letra**. Ela nos permite que procuremos por algum termo em específico, descartando todos os outros que diferem dele. Por exemplo, uma busca comum por “fabricadenoobs2@gmail.com” nos retorna uma imensa gama de resultados, sendo que muitos deles sequer possuem o termo que procuramos.



The screenshot shows the Google search interface with the 'Todas' (All) tab selected. Below the navigation bar, it indicates 'Aproximadamente 58 resultados (0,50 segundos)'. The search query is 'Você quis dizer: **fábrica de noobs 2@gmail.com**'. The first result is for 'NatanaelAntonioli (Natanael Antonioli) · GitHub', with a link to 'https://github.com/NatanaelAntonioli'. The second result is 'Os segredos da DeepWeb - Diolinux Entrevista Fábrica de Noobs ...' with a link to 'kinotube.info/channel/watch/vzXcmIJs2hg'. The third result is 'como usar a deep web para estudar para concursos públicos ...' with a link to 'https://kinotube.info/channel/watch/aaW6q4ZDFbs'. Each result includes a brief description and a link to the full content.

Todas Maps Notícias Vídeos Imagens Mais Configurações Ferramenta

Aproximadamente 58 resultados (0,50 segundos)

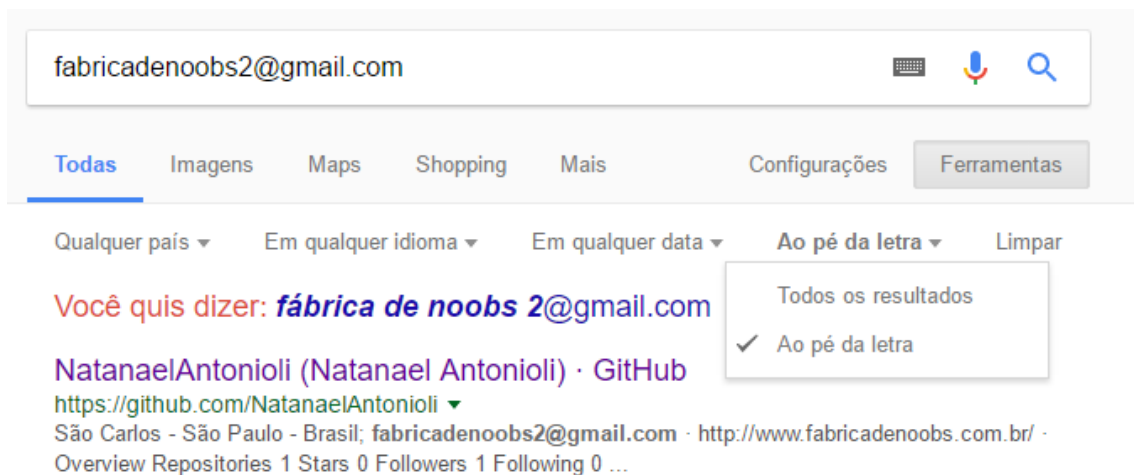
Você quis dizer: **fábrica de noobs 2@gmail.com**

NatanaelAntonioli (Natanael Antonioli) · GitHub
<https://github.com/NatanaelAntonioli> ▼
São Carlos - São Paulo - Brasil; fabricadenoobs2@gmail.com · <http://www.fabricadenoobs.com.br/> ·
Overview Repositories 1 Stars 0 Followers 1 Following 0 ...

Os segredos da DeepWeb - Diolinux Entrevista Fábrica de Noobs ...
<kinotube.info/channel/watch/vzXcmIJs2hg> ▼
... <https://goo.gl/CLPvIC> - Assine o nosso Feed: <http://goo.gl/w6418F> - Diolinux na Google Play Banca:
<http://goo.gl/qCJQqr>. Contato: blogdiolinux@gmail.com ...

como usar a deep web para estudar para concursos públicos ...
<https://kinotube.info/channel/watch/aaW6q4ZDFbs> ▼
como usar a deep web para estudar para concursos públicos <http://bit.ly/2beXeqd> — Clique aqui para
ter acesso ao MATERIAL COMPLETO e aos MAPAS DE ...

Já uma busca ao pé da letra irá retornar apenas os resultados que contenham exatamente o que procuramos. Na situação mostrada, este endereço de e-mail está relacionado apenas à uma página do Git-Hub.



A screenshot of a Google search interface. The search bar contains the text 'fabricadenoobs2@gmail.com'. Below the search bar are tabs for 'Todas', 'Imagens', 'Maps', 'Shopping', 'Mais', 'Configurações', and 'Ferramentas'. Below the tabs are filters for 'Qualquer país', 'Em qualquer idioma', 'Em qualquer data', 'Ao pé da letra', and 'Limpar'. The 'Ao pé da letra' filter is selected, and a dropdown menu shows 'Todos os resultados' and 'Ao pé da letra' (checked). The search results show a link to 'NatanaelAntonioli (Natanael Antonioli) · GitHub' with the URL 'https://github.com/NatanaelAntonioli'. Below the link is the text 'São Carlos - São Paulo - Brasil; fabricadenoobs2@gmail.com · http://www.fabricadenoobs.com.br/ · Overview Repositories 1 Stars 0 Followers 1 Following 0 ...'.

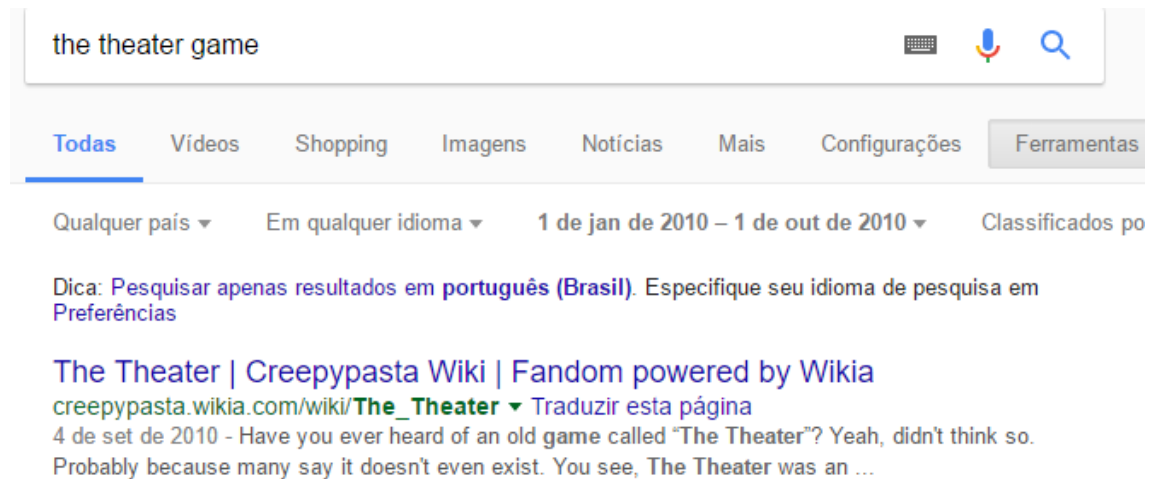
Há também a ferramenta de Pesquisa Avançada do Google, que pode ser acessada em https://www.google.com.br/advanced_search e permite que nossas buscas sejam refinadas por país, idioma, tipo de arquivo e data.

Em seguida, limite seus resultados por...

idioma:	<input type="text" value="qualquer idioma"/>
região:	<input type="text" value="qualquer país"/>
última atualização:	<input type="text" value="em qualquer data"/>
site ou domínio:	<input type="text"/>
termos que aparecem:	<input type="text" value="qualquer lugar da página"/>
SafeSearch:	<input type="text" value="Mostrar resultados mais relevantes"/>
tipo de arquivo:	<input type="text" value="qualquer formato"/>
direitos de uso:	<input type="text" value="não filtrados por licença"/>

A pesquisa por data pode ser extremamente útil caso queiramos saber, por exemplo, qual foi o primeiro uso de determinado termo na Internet, ou quando e onde se deu a primeira postagem de determinada notícia.

Por exemplo, realizando uma busca reversa pelo termo “The Theater Game”, é possível encontrar a primeira menção sobre tal jogo. Isso nos permite deduzir que a história foi originalmente postada num portal de Creepypastas.



Uma busca por data deve ser conduzida dentro de intervalos cada vez menores, a fim de encontrar exatamente onde está o resultado que procuramos. A tabela abaixo exemplifica o procedimento realizado no exemplo acima.

Função da Busca	Intervalo	Resultado
Determinar em qual "grande intervalo" o alvo se encontra	2000 → 2007	✗
Verificar em qual período de 5 anos aconteceu	2007 → 2010	✓
Verificar ano por ano.	2007 → 2008	✗
	2008 → 2009	✗
	2009 → 2010	✓
Aconteceu em 2010. Determinar o mês.	jan/10 → fev/10	✗
	fev/10 → mar/10	✗
	...	
	set/10 → out/10	

		✓
--	--	---

Entrando finalmente no quesito de buscas reversas, o [Google Imagens](https://images.google.com) (<https://images.google.com>) pode ser uma ferramenta extremamente útil para se procurar pela origem de uma imagem.

Por exemplo, se quisermos saber qual a origem da foto abaixo (quem é o homem, e porque ele anda com o tamanduá no meio de uma grande cidade), basta realizar a pesquisa com a ferramenta do Google.



10897...0256_n.jpg x salvador dali oso hormiguero

Todas **Imagens** Maps Shopping Mais Configurações Ferramentas

Aproximadamente 25.270.000.000 resultados (1,05 segundos)

Tamanho da imagem: 468 × 700

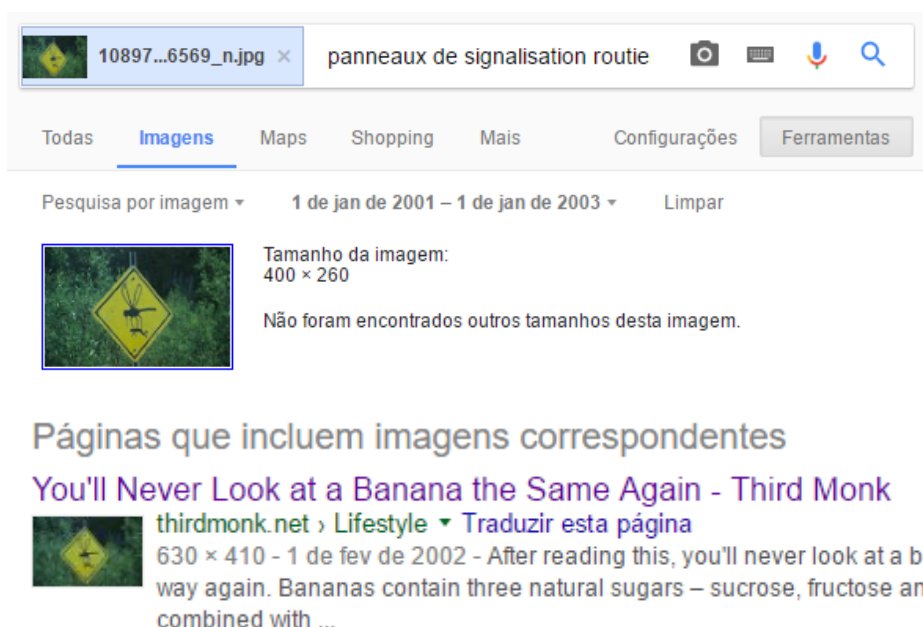
Encontrar esta imagem em outros tamanhos: Todos os tamanhos - Médio - Grande

Melhor sugestão para esta imagem: **salvador dali oso hormiguero**

Cuando Dalí puso de moda entre la alta sociedad parisina tener un ...
blogs.20minutos.es/.../cuando-dali-puso-de-moda-entre-la-alta-so... ▼ Traduzir esta página
 19 de jun de 2014 - Esta costumbre la puso de moda Salvador Dalí, famoso por sus ... de una estación de metro de París paseando a un oso hormiguero dio la ...

Imediatamente, o mecanismo de busca já dá a resposta procurada. Trata-se do famoso pintor Salvador Dalí, posando em uma foto para a revista Paris Match, da edição de número 1055, de 26 de julho de 1969.

Podemos ainda utilizar a busca reversa por imagem em conjunto com a filtragem por datas. Porém, é necessário ter cautela, pois o resultado pode corresponder ao momento em que o site foi indexado pelo mecanismo de buscas, e não ao momento da postagem de determinada imagem. Por exemplo, ao realizarmos a busca por essa outra curiosa imagem, constatamos um resultado de 2002.

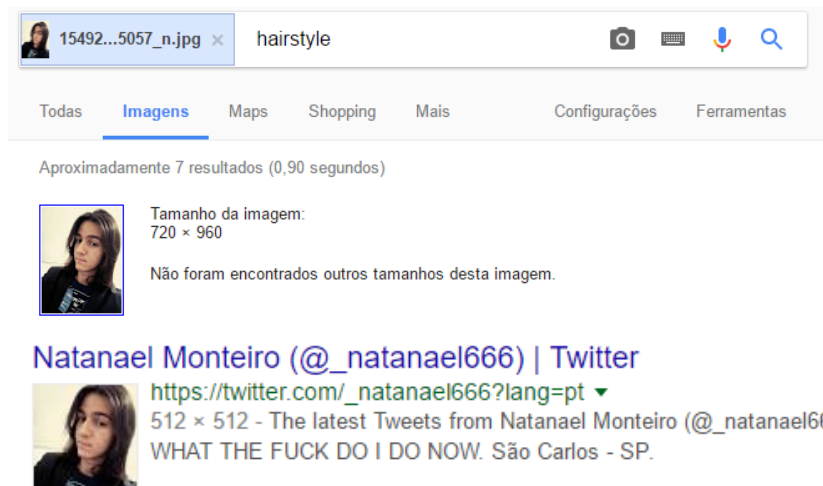


O endereço em questão nos retorna leva a um site sobre os benefícios do consumo de banana (<http://thirdmonk.net/nutrition/never-look-at-banana-same.html>), e a imagem foi utilizada para ilustrar que a banana pode agir como repelente de insetos. No entanto, ao analisarmos o código fonte da página em questão, notamos que se trata, na verdade, de uma postagem de 2013. Sendo assim, devemos ignorar este resultado.

```
29 <meta property="article:tag" content="Public Health" />
30 <meta property="article:section" content="Lifestyle" />
31 <meta property="article:published_time" content="2013-12-31T11:55:42-07:00" />
32 <meta property="article:modified_time" content="2016-06-17T00:32:04-07:00" />
33 <meta property="og:updated_time" content="2016-06-17T00:32:04-07:00" />
34 <meta property="og:image" content="http://thirdmonk.net/postcont/2013/11/Bananas-cover.jpg" />
35 <meta property="og:image:width" content="3008" />
```

Essa verificação é fundamental, e deve ser realizada antes de qualquer constatação, especialmente quando chegamos a um resultado duvidoso. Procure manualmente pela data no código fonte, ou busque termos como “date” e “time”.

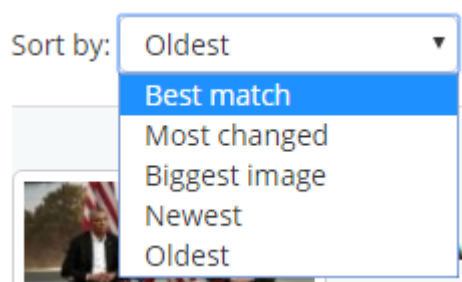
Além disso, a mesma técnica pode ser utilizada para descobrir a identidade de alguém partindo de uma fotografia (tal como fizemos na investigação sobre o 432 Mystery). Basta pesquisar a imagem em qualquer mecanismo e busca e analisar os resultados apontados. Você provavelmente será apontado para as redes sociais da pessoa procurada, que fornecerão outras informações.



Caso queiramos procurar por manipulações de imagem, o [TinEye](https://www.tineye.com) (<https://www.tineye.com>) pode ser uma excelente ferramenta. Para demonstração, iremos encontrar a fonte utilizada para a seguinte montagem.

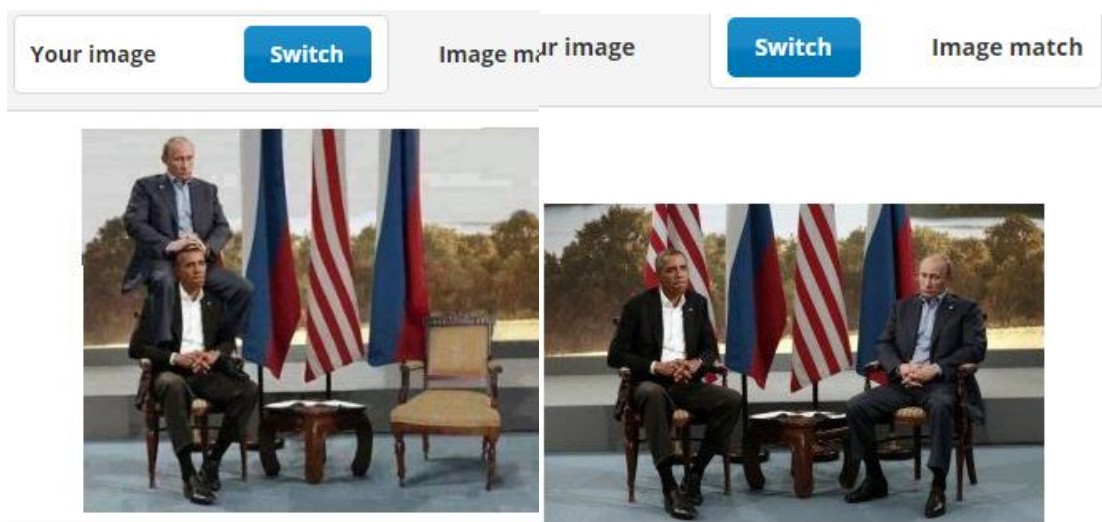


Utilizado o mecanismo, podemos elencar os resultados conforme o objetivo de nossa busca. São elas:



- Best match: permite encontrar a imagem que mais se assemelha àquela que possuímos.
- Most changed: permite encontrar a imagem que menos se assemelha àquela que possuímos. Pode ser útil para encontrar a origem de uma montagem, ou montagens feitas a partir de uma original.
- Biggest Image: útil para designers que procuram fotos em alta resolução. Encontra a maior imagem que possua os mesmos traços da imagem buscada.
- Newest e Oldest: retornam a imagem mais nova e mais velha, respectivamente.

Assim, através desta análise forense, conseguimos encontrar a imagem original, que foi utilizada para produzir a montagem. A ferramenta ainda nos permite comparar as duas.



Através desta comparação, podemos entender mais sobre como a montagem foi feita e encontrar outros elementos estranhos à fotografia original, como a cadeira que deveria estar sendo utilizada por Vladimir Putin – note que ela foi inserida de uma fonte externa.

No entanto, esse processo costuma requerer alguns passos a mais. A simples busca pela seção da fotografia, na maioria dos casos, simplesmente retorna resultados correspondentes à mesma montagem que procurarmos e, portanto, são inúteis.

Para evitar que isso ocorra, é necessário separar totalmente a parte procurada (no caso, a cadeira) do resto da imagem, o que pode ser facilmente feito em um programa de edição de imagem como o Photoshop.



Após os cortes – os quais não precisam ser dignos de um anúncio publicitário – podemos realizar a busca reversa através dos mecanismos vistos anteriormente. Na situação específica, o próprio Google nos trouxe as respostas que procurávamos.

Páginas que incluem imagens correspondentes

Antiques, Furniture and America on Pinterest



<https://www.pinterest.com/pin/318700111100869994/>

236 × 317 - Invest in a look you'll always love with always-in-style bedroom furniture at irresistible prices from Joss & Main. Then, craft the bedroom oasis of your dreams ...

1000+ images about Eastlake furniture on Pinterest | Furniture ...



<https://br.pinterest.com/ishadodi/eastlake-furniture/> ▼

324 × 436 - Victorian pieces | See more about Furniture, Victorian bookcases and First girl.

Ou seja, a imagem da cadeira utilizada foi retirada de alguma página sobre móveis antigos. Lembre-se que, dependendo da situação, poderia ser necessário realizar mais uma busca, a fim de filtrar os resultados por data.

Apesar de ser um procedimento mais complexo, também podemos realizar a busca reversa por vídeos. Ela se baseia no pressuposto de que um vídeo é, na verdade, uma sucessão de imagens.

Dessa forma, separamos, arbitrariamente, algumas imagens deste vídeo e realizamos a busca por elas. Felizmente, existem algumas ferramentas que automatizam a maior parte do processo, como as ferramentas da [Intel Techniques](#).

Em <https://inteltechniques.com/osint/reverse.video.html>, podemos inserir o link de um vídeo das mais diversas redes sociais: Youtube, Vimeo, Facebook, Vine, Instagram ou LiveLeak. Há ainda a possibilidade de pesquisarmos por um frame específico do vídeo, que deve ser upado em alguma ferramenta do gênero.

Custom Reverse Video Search

This tool allows you to conduct a reverse image search from the stored thumbnail images associated with videos. It will often locate ad target video. The results for each search include Google, TinEye, Yandex, Bing, and Baidu. If using Chrome, you will need to allow popu found in the address of each video page, as indicated in red below.

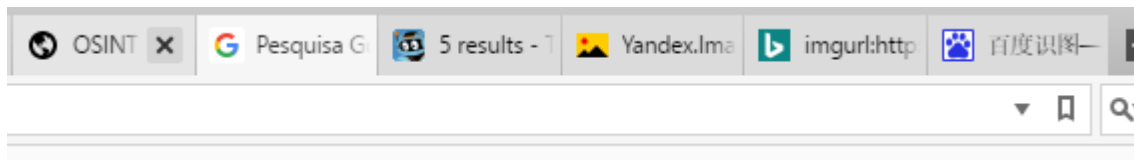
Reverse YouTube Video Search - ex: <http://www.youtube.com/watch?v=VRFCMM3bra8>

Por exemplo, vamos realizar uma pesquisa rápida por uma das cenas mostradas neste vídeo de terror psicológico (<https://www.youtube.com/watch?v=BhqRZJQb3qU&t=1s>). Mais especificamente, procuraremos pela cena mostrada aos 0:55, que mostraria um cadáver tendo seus membros cortados – seria uma cena de tortura real?



Vídeo Retirado da Deep Web #1

Para tanto, copiamos o frame em questão (realizando um print da tela) e o enviamos para um serviço de upload de imagens. Em seguida, colamos o endereço de imagem obtida no último campo da ferramenta. Imediatamente, o site irá abrir algumas guias (ou se for um vídeo inteiro, uma quantidade considerável delas) de buscadores diferentes.



Logo temos nossa resposta. A cena foi retirada, na verdade, de um filme chamado Men Behind The Sun, como mostram vários resultados. Lembre-se também de utilizar a busca por data, caso necessário.

