

Investigação digital com Autopsy

António Pinto
apinto@estg.ipp.pt

Outubro 2025 (v5)

Sumário

Início rápido

Análise de conteúdos

Processamento de dados

Cronologias

Relatórios

Extração de evidências

Aquisição de imagens

Guymager, FTK Imager

Aquisição de imagem

Descarregue o novamente o ficheiro `pen_usb.zip`, descomprima-o e instale a pen virtual no seu Kali com os comandos:

```
mkdir /media/pen  
mount -t auto -o loop pen_usb.img /media/pen
```

Usando o **guymager** (Kali, pelo terminal e com *sudo*) ou **FTK Imager** (Windows), obtenha uma imagem do *pen*.
Garanta que o programa regista o *hash* SHA-256 da aquisição.

Submeta o relatório da aquisição no moodle.

Conceitos introdutórios

url: <http://www.sleuthkit.org/autopsy/>



- ▶ *Autopsy* é uma ferramenta gráfica vocacionada para a investigação digital de imagens de suportes de armazenamento.
- ▶ Suporta a análise de imagens de sistemas *Android*, *drones*, ...
- ▶ É expansível (suporta módulos desenvolvidos em *Python*)
- ▶ É desenvolvida em Java, tendo Windows como plataforma preferencial

Conteúdos

Início rápido

Análise de conteúdos

Processamento de dados

Cronologias

Relatórios

Extração de evidências

Autopsy 4.19.3

Instalação

Preparação (15 minutos)

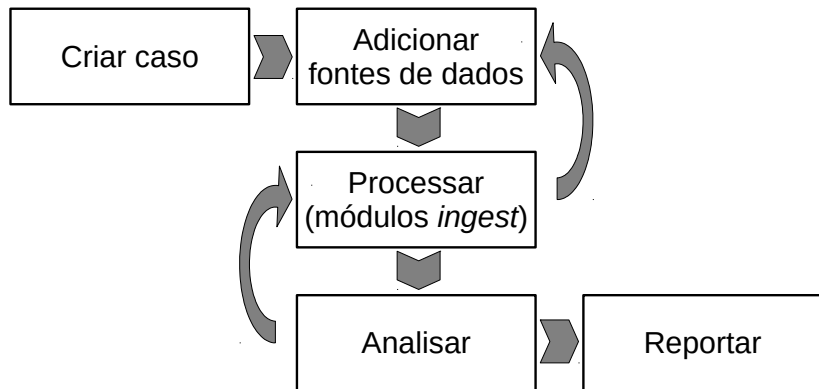
Descarregue e instale o **Autopsy** no seu computador. Use a versão mais recente.

Se durante o processo de instalação, for questionado quando ao uso de um repositório central, diga que não.

(<https://www.autopsy.com/download/>)

Fluxo de trabalho

Autopsy



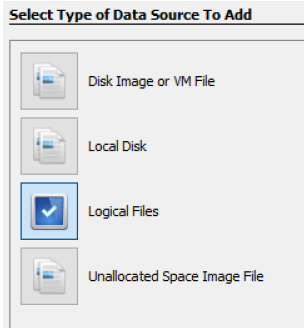
Criação de um caso

1. Criar um caso

- ▶ Informação do caso
- ▶ N.º caso, Investigador

2. Adicionar fonte de dados

- ▶ Imagem *raw* (dd) ou EnCase (E01)
- ▶ Discos, ficheiros ou pastas locais
- ▶ Disco de máquina virtual (vmdk, vhd)



Exercício

Criação de caso (15 minutos)

Crie um novo caso no seu Autopsy de acordo com as seguintes informações:

- ▶ Nome do caso: Exemplo
- ▶ Número do caso: 001
- ▶ Investigador: o seu nome
- ▶ Email: o seu email
- ▶ Fonte de dados: hd.img (disponível no moodle)

No final, mande executar todos os módulos *ingest*

Conteúdos

Início rápido

Análise de conteúdos

Processamento de dados

Cronologias

Relatórios

Extração de evidências

Análise manual de conteúdos

Interface gráfica do Autopsy

The screenshot displays the Autopsy 4.2.0 interface with several components highlighted by colored boxes and labels:

- Tree Viewer (Green box):** Located on the left, it shows a hierarchical view of the data sources. The 'Data Sources' section is expanded, showing a list of files including 'Demo_HD.E01', 'LogicalFileSet1 (1)', 'small2.img', 'small2.jpg', 'small2.png', 'thunderbird_small_image.dd', 'outlook.dd', 'BG01_Memory_card.E01', 'mtd1_userdata.bin', 'mtd1_system.bin', 'mtd1_cache.bin', 'outlo', and 'Demo'. The 'Views' section is also expanded, showing 'File T' and 'By Extension' (Images (15510), Videos (263), Audio (753), Archives (827)).
- Keyword Search (Yellow box):** Located at the top right, it features a search bar and a 'Keyword Search' button.
- Result Viewer (Blue box):** Located in the center, it displays a table of search results. The table has columns for 'Source File', 'Date Created', 'Device Model', and 'Device Make'. The results are filtered to show only 'KODAK 2650 ZOOM DIGITAL CAMERA' devices.
- Content Viewer (Red box):** Located at the bottom right, it displays a preview of the selected file, which is a photograph of a person on a horse in a city street.
- Status Area (Purple box):** Located at the bottom right, it displays the status of the current operation.

Source File	Date Created	Device Model	Device Make
100_6228.JPG	2011-10-25 06:27:23 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
100_6184.JPG	2011-10-25 05:09:12 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
100_6290.JPG	2011-10-25 10:58:19 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
100_6223.JPG	2011-10-25 06:24:43 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
12-198241 LG Vx8350 5.jpg	2011-09-06 23:35:39 EDT	Canon PowerShot SX110 IS	Canon
100_6594.jpg			Canon
100_6418.JPG			Canon
100_6342.JPG			Canon
100_6290.JPG	2011-10-25 10:58:19 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
100_6599.JPG	2011-10-25 10:03:16 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
100_6228.JPG	2011-10-25 06:27:23 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
100_6223.JPG	2011-10-25 06:24:43 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP
100_6192.JPG	2011-10-25 05:19:00 EDT	KODAK 2650 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMP

Análise manual de conteúdos

Tree viewer

O *Tree viewer* indexa informação resultante do processamento automático e dá acesso a quatro grandes áreas

- ▶ **Data sources:** Indica os ficheiros utilizados como fonte de dados, permitindo a navegação dentro dos respetivos sistemas de ficheiros.
- ▶ **Views:** Mostra os ficheiros encontrados sob múltiplas vistas (tipo, tamanho, estado). Um mesmo ficheiro pode surgir aqui várias vezes (em vistas diferentes).
- ▶ **Results:** Mostra os resultados encontrados pelos vários módulos.
- ▶ **Reports:** Indica os vários relatórios produzidos, quer manual, quer automaticamente pelos módulos.

Tree viewer

Views

Em particular, a área **Views** tem disponível

- ▶ **File type:** Ordena ficheiros por extensão ou tipo MIME.
- ▶ **Recent files:** Ficheiros acedidos nos últimos 7 dias.
- ▶ **Deleted files:** Ficheiros eliminados, tentando recuperar o seu nome original.
- ▶ **File size:** Ordena ficheiros por tamanho.

Galeria de imagens

Útil quando a análise de imagens é relevante para o caso em consideração. Está disponível no menu *Tools*

- ▶ Agrupa imagens por pasta, arquivo comprimido
- ▶ Permite a visualização de imagens aquando da deteção
- ▶ Funcionalidade pode ser ativada/desativada nas opções
- ▶ Permite catalogação de imagens (focado em pornografia infantil e similares)

Pesquisa de ficheiros

Útil quando se procura por um ficheiro com características específicas. Está disponível no menu *Tools*

- ▶ Nome
- ▶ Tamanho
- ▶ Tipo MIME
- ▶ Datas
- ▶ Bom/Mau

File Search by Attributes

Search for files that match the following criteria:

☒ Name:

*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported.

☒ Size:

☒ MIME Type:

*Note: Multiple MIME types can be selected

☒ Date:

*Empty fields mean "No Limit" *The date format is mm/dd/yyyy

Timezone:

☒ Modified ☒ Accessed ☒ Created ☒ Changed

☒ Known Status:

☒ Unknown ☒ Known (NSRL or other) ☒ Known bad

Conteúdos

Início rápido

Análise de conteúdos

Processamento de dados

Cronologias

Relatórios

Extração de evidências

Processamento automatizado

Com recurso a módulos

Configure Ingest Modules

☒ Recent Activity

☐ Hash Lookup

☒ File Type Identification

☒ Embedded File Extractor

☒ Exif Parser

☒ **Keyword Search**

☒ Email Parser

☒ Extension Mismatch Detector

☒ E01 Verifier

☒ Android Analyzer

☒ Interesting Files Identifier

☒ PhotoRec Carver

☒ Virtual Machine Extractor

Select All

Deselect All

View Ingest History

☒ Process Unallocated Space

Select keyword lists to enable during ingest:

☒ Phone Numbers

☒ IP Addresses

☒ Email Addresses

☒ URLs

☒ Credit Card Numbers

☐ Lista1

☒ Exercício

Scripts enabled for string extraction from unknown file types:

Latin - Basic

Encodings: UTF8, UTF16

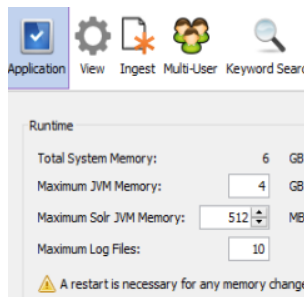
Performs file indexing and periodic search using keywords and ...

Global Settings

Processamento automatizado

Execução eficiente

- ▶ *Autopsy* é uma aplicação intensiva
- ▶ Baseada em Java (JVM)
- ▶ Execução eficiente da JVM requer uso adequado de memória
- ▶ Validar configurações em Ferramentas → *Opções* → Aplicação
- ▶ Requer *restart* ao Autopsy

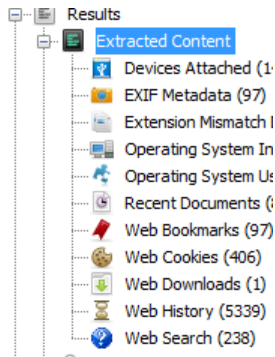


Módulo: Recent Activity

Extrai informação dos últimos 7 dias

- ▶ Utilização da Internet (incluindo pesquisas)
- ▶ Programas instalados
- ▶ Equipamentos ligados (USB)
- ▶ Processa o *Registry hive*

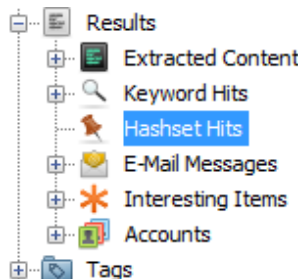
Informação é colocada em **Extracted Content**, dentro de **Results**



Módulo: Hash Lookup

Calcula valores de resumo (MD5) de todos os ficheiros encontrados e compara-os com bases de dados deste tipo de valores (*hashs* MD5)

- ▶ Known hash sets
 - ▶ Ficheiros que podem ser ignorados
- ▶ Notable hash sets
 - ▶ Ficheiros que devem ser validados



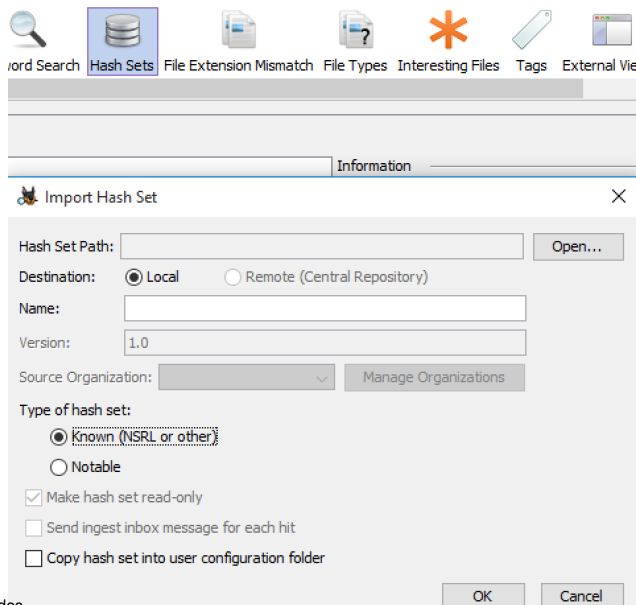
Módulo: Hash Lookup

Hash sets

- ▶ Muitos só são disponibilizadas para forças policiais (ex.: *hash sets* de imagens de pornografia infantil)
- ▶ Lista pode ser de *conhecidos (known)* ou de *merecedores de nota (notable)*, dependendo do caso
- ▶ National Software Reference Library (NSRL) do NIST
 - URL:** <http://www.nsrl.nist.gov/>
 - URL:** <http://sourceforge.net/projects/autopsy/files/NSRL/>
- ▶ VirusShare
 - URL:** <https://virusshare.com/hashes.4n6>

Módulo: Hash Lookup

Importação de *Hash sets*



The screenshot shows a software interface with a top toolbar containing icons for Word Search, Hash Sets (highlighted with a blue box), File Extension Mismatch, File Types, Interesting Files, Tags, and External View. Below the toolbar is a main content area with an 'Information' tab. A dialog box titled 'Import Hash Set' is open, featuring a close button (X) in the top right corner. The dialog contains the following fields and options:

- Hash Set Path:** A text input field with an 'Open...' button to its right.
- Destination:** Two radio buttons: 'Local' (selected) and 'Remote (Central Repository)'.
- Name:** A text input field.
- Version:** A text input field containing '1.0'.
- Source Organization:** A dropdown menu with a 'Manage Organizations' button to its right.
- Type of hash set:** Two radio buttons: 'Known (NSRL or other)' (selected) and 'Notable'.
- Checkboxes:**
 - ☒ Make hash set read-only
 - ☐ Send ingest inbox message for each hit
 - ☐ Copy hash set into user configuration folder
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Exercício

Importação de *hash set* (30 minutos)

Importe o *hash set* **badfiles** para a sua instalação do Autopsy. Este *hash set* está disponível no moodle.

No final, mande executar o módulo *hash lookup* novamente no caso criado no exercício anterior.

Foram identificados alguns resultados desta nova execução do módulo? Quais? Porquê?

Submeta sua análise crítica (ficheiro PDF).

Módulo: File Type Identification

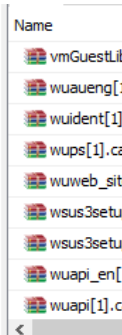
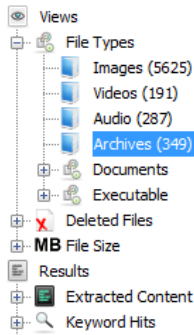
Verifica o tipo de cada ficheiro em função das suas características e recolhe meta dados

- ▶ Utiliza o *Tika* (<http://tika.apache.org/>)
- ▶ Módulo de indexação sem *output* próprio
- ▶ Gera informação para outros módulos
 - ▶ Extension Mismatch Detector
 - ▶ Keyword Search

Módulo: Embedded File Extraction

Descomprime ficheiros comprimidos (ZIP, RAR) ou embarcados (DOC, DOCX, PPT, PPTX, XLS e XLSX), processando-os de novo.

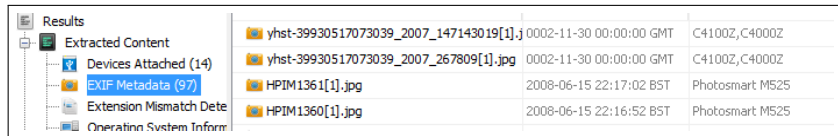
- ▶ Possibilita a análise de ficheiros incluídos nestes arquivos
- ▶ Resultados aparecem na vista **Archives**, em **File types**



Módulo: EXIF Parser

Extraí informação em formato EXIF (*Exchangeable Image File Format*) armazenada em imagens

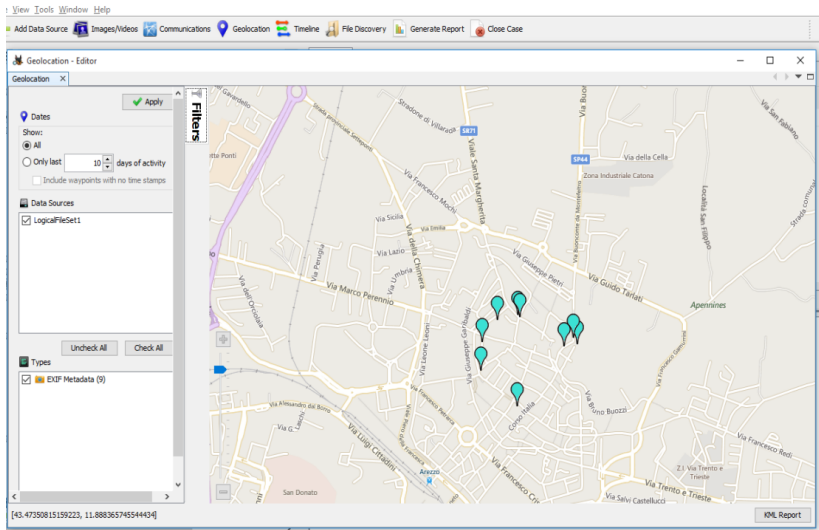
- ▶ Geolocalização, data, hora
- ▶ Modelo da câmara, definições (exposição, resolução)
- ▶ Resultados aparecem em **EXIF Metadata**, em **Extracted content**



yhst-39930517073039_2007_147143019[1].jpg	0002-11-30 00:00:00 GMT	C4100Z,C4000Z
yhst-39930517073039_2007_267809[1].jpg	0002-11-30 00:00:00 GMT	C4100Z,C4000Z
HPIM1361[1].jpg	2008-06-15 22:17:02 BST	Photosmart M525
HPIM1360[1].jpg	2008-06-15 22:16:52 BST	Photosmart M525

Geolocalização

Exemplo



Exercício

EXIF e geolocalização (30 minutos)

Recupere os ficheiros eliminados com o Autopsy. Se não surgir nenhum ficheiro ZIP, corra o **foremost** sobre **hd.img**. Adicione todos os ficheiros ZIP como novas fontes de dados ao seu caso.

No final, execute novamente os módulos relacionados com imagens e geolocalização.

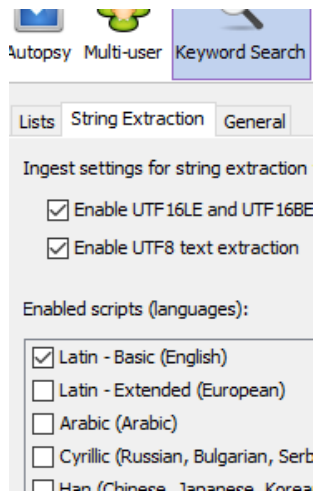
Que ficheiros referenciam coordenadas GPS? As coordenadas dizem respeito a que cidade?

Submeta sua análise crítica (ficheiro PDF).

Módulo: Keyword Search

Pesquisa por palavras chave durante o processamento inicial ou a pedido

- ▶ Extrai texto dos ficheiros em processamento e adiciona-as a um índice (Solr)
- ▶ Suporta vários formatos (Texto, MS Office, PDF, E-mails)
- ▶ Em formatos não suportados
 - ▶ Algoritmo de *String Extraction*
 - ▶ Possibilita identificação de codificações e línguas



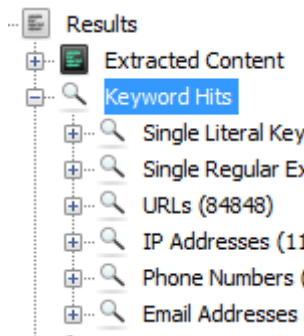
Módulo: Keyword Search

Listas predefinidas

Autopsy inclui listas predefinidas para palavras chave frequentes

- ▶ Endereços *web* (URLs)
- ▶ Endereços IP
- ▶ Números de telefone
- ▶ Endereços de e-mail

Geram um número significativo de falsos positivos



Exercício

Pesquisa de *keywords* (15 minutos)

Crie uma lista de palavras chave, com nome **MinhaLista1**, que lhe permita procurar por ocorrências da palavra “**forensics**”.

Mande executar o módulo *keyword search* novamente no seu caso.

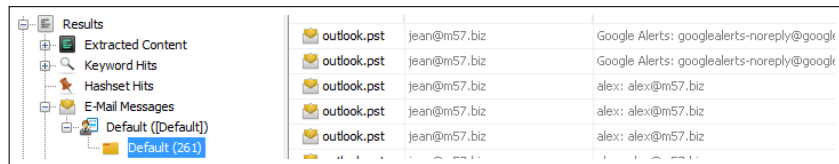
Foram identificados alguns resultados? Descreva-os.

Submeta sua análise crítica (ficheiro PDF)

Módulo: Email Parser

Identifica e processa ficheiros de programas de correio eletrónico (MBOX, PST)

- ▶ Extrai e-mails lá contidos
- ▶ Processa os respetivos anexos



The screenshot displays a software interface for email processing. On the left, a file tree shows the hierarchy: Results > Extracted Content > Keyword Hits > Hashset Hits > E-Mail Messages > Default ([Default]) > Default (261). The 'Default (261)' folder is selected. On the right, a table lists the extracted email data.

outlook.pst	jean@m57.biz	Google Alerts: googlealerts-noreply@google
outlook.pst	jean@m57.biz	Google Alerts: googlealerts-noreply@google
outlook.pst	jean@m57.biz	alex: alex@m57.biz
outlook.pst	jean@m57.biz	alex: alex@m57.biz
outlook.pst	jean@m57.biz	alex: alex@m57.biz

Módulo: Extension Mismatch Detector

Identifica ficheiros que tenham uma extensão diferente da esperada

- ▶ Visa identificar tentativas de camuflagem de ficheiros



File Name	Extension	MIME Type
Envelope Wizard.wiz	wiz	application/msword
WEBPAGE.WIZ	wiz	application/msword
A0003824.rbf	rbf	application/pdf
GR8GALRY.GRA	gra	application/vnd.ms-excel

Módulo: E01 Verifier

Verifica o valor de *checksum* de ficheiros fonte em formato E01

- ▶ Calcula e compara com os valores contidos nos próprios ficheiros E01
- ▶ Visa evitar o processamento de ficheiros E01 corrompidos

Módulo: Interesting Files Identifier

Gerar alertas quando detetar ficheiros e pastas com determinadas características

- ▶ Tipo (ficheiro/pasta)
- ▶ Tamanho, Extensão
- ▶ Nome, Caminho
- ▶ Tipo MIME

Interesting Files Set

Enter information about files that you want to find.

Type: ☐ Files ☒ Directories ☐ Files and Directories

☒ Name Pattern: Backup
☒ Full Name ☐ Extension Only ☐ Regex

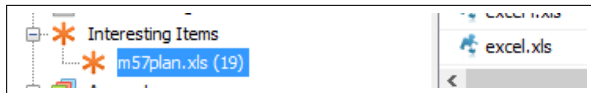
☒ Path Pattern: Apple Computer/MobileSync
☐ Regex [i](#) Use / as path separator

☐ MIME Type:

☐ File Size:

Rule Name (Optional):

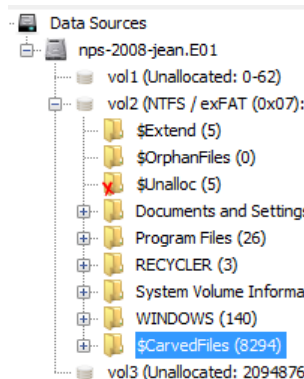
OK Cancel



Módulo: PhotoRec Carver

Extraí ficheiros de espaços não alocados

- ▶ Suporta vários tipos de ficheiros
- ▶ Possibilita a descoberta de ficheiros eliminados recentemente
- ▶ Permite a adição personalizada de assinaturas de ficheiros
- ▶ Opção “Process Unallocated Space” têm de estar ativa



Módulo: Virtual Machine Extractor

Identifica discos de máquinas virtuais e adiciona-os como novas fontes de dados

- ▶ Suporta ficheiros VMWare (vmdk) e Microsoft Virtual Hard Drives (vhd)

Conteúdos

Início rápido

Análise de conteúdos

Processamento de dados

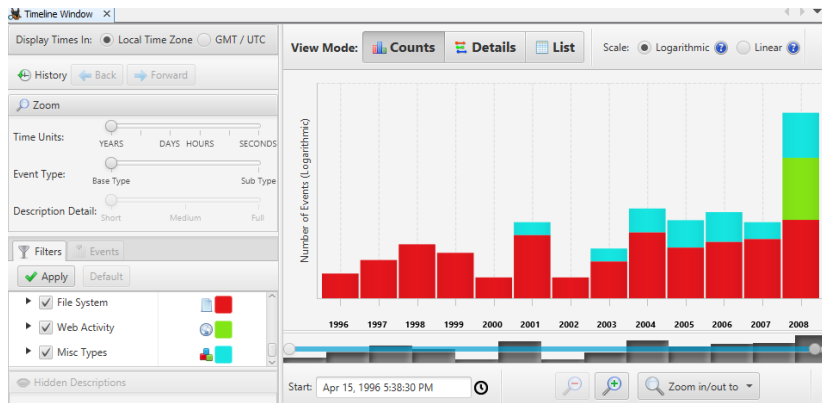
Cronologias

Relatórios

Extração de evidências

Cronologias

Após a indexação de eventos, o Autopsy permite a criação de cronologias com base nas datas em que tais eventos ocorreram



Cronologias

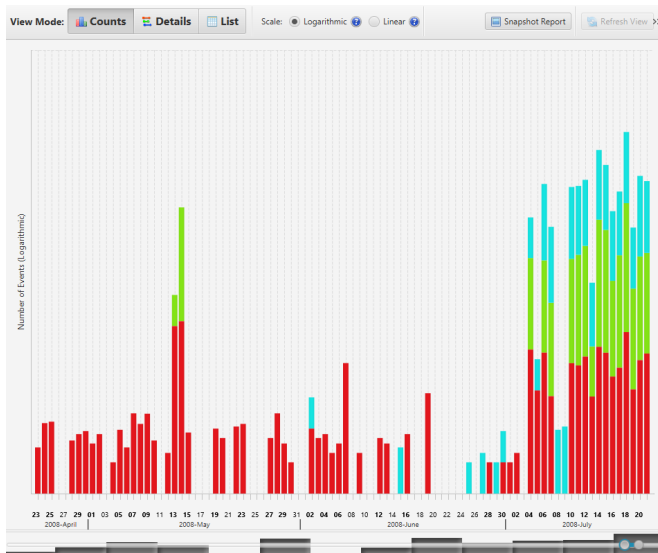
Eventos

Autopsy reconhece eventos como

- ▶ Ficheiros (modificação, acesso, criação, alteração)
- ▶ Acesso à Internet (*downloads*, *cookies*, criação de *bookmarks*, pesquisas, histórico de navegação)
- ▶ Outros (mensagens, chamadas telefónicas, e-mails, rotas GPS, ...)

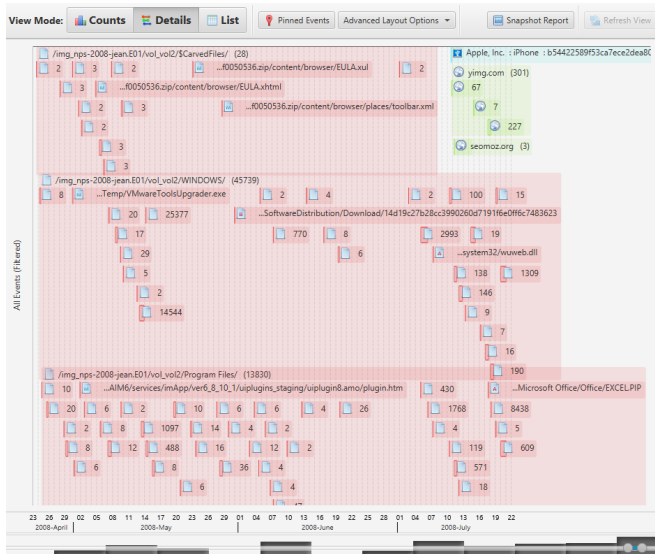
Visualização de cronologias

Histograma



Visualização de cronologias

Vista detalhada

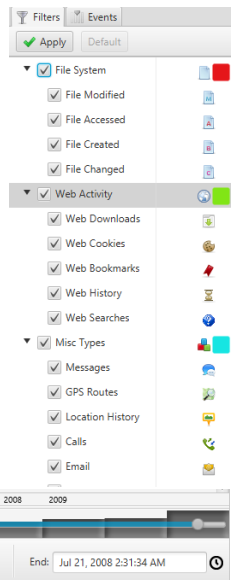


Visualização de cronologias

Filtros

Autopsy possibilita a redução da quantidade de elementos de uma cronologia usando filtros

- ▶ Filtrar ficheiros conhecidos
- ▶ Filtrar por texto
- ▶ Tipos de eventos
- ▶ Janelas temporais



Exercício

Cronologias (15 minutos)

Usando a ferramenta de *timeline* do Autopsy, identifique, no contexto do caso atual, que **ficheiros** foram **criados** em **maio de 2020**.

Submeta sua análise crítica (ficheiro PDF).

Conteúdos

Início rápido

Análise de conteúdos

Processamento de dados

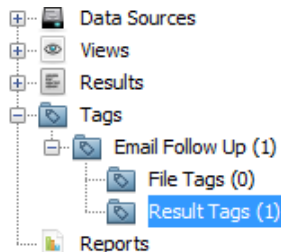
Cronologias

Relatórios

Extração de evidências

Etiquetagem

- ▶ Marcação de resultados com etiquetas
- ▶ Itens para referência futura
- ▶ Possibilita a marcação de ficheiros ou resultados
- ▶ Nome das etiquetas definido pelo investigador
- ▶ Marcações surgem como subárea de **Results**



Geração de relatórios

Estão disponíveis vários tipos de relatórios

- ▶ **Results:** Incide sobre os itens da vista resultados, podendo ser filtrados
- ▶ **Tagged:** Incide sobre itens marcados
- ▶ **Files:** Lista de todos os ficheiros em análise
- ▶ **KML:** Lista de coordenadas GPS em formato *Google Earth*
- ▶ **TSK:** Lista de tempos MAC de todos os ficheiros

Select and Configure Report

Report Modules:

- ☐ Results - HTML
- ☐ Results - Excel
- ☐ Add Tagged Hashes
- ☐ Files - Text
- ☐ Google Earth/KML
- ☐ STIX
- ☒ TSK Body File

☐ Permissions

☐ Full Paths

Select All Deselect All

☒ Web Search

Conteúdos

Início rápido

Análise de conteúdos

Processamento de dados

Cronologias

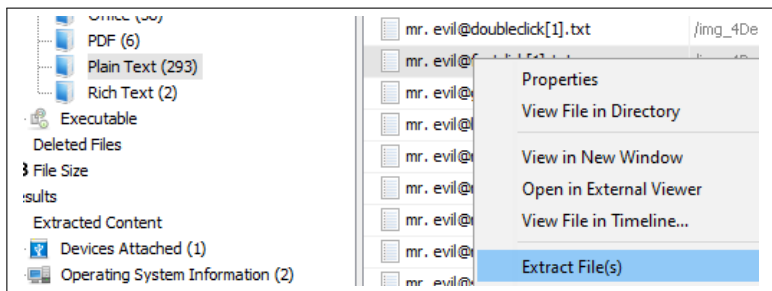
Relatórios

Extração de evidências

Extração de evidências

Autopsy permite a extração de ficheiros

- ▶ Tratamento com outras ferramentas
- ▶ Comparação
- ▶ Arquivo



Extração manual de evidências

Autopsy não consegue extrair todos os ficheiros

- ▶ Ficheiros baseados em texto são problemáticos
- ▶ Emails, código fonte, txt . . .
- ▶ Solução passa por análise e extração manual

Exercício

Extração manual (15 minutos)

Usando uma ferramenta à sua escolha (ex: HxD, wxHexEditor), extraia **133.525** bytes consecutivos a partir da posição **4.571.136** do ficheiro **hd.img**.

Analise o ficheiro resultante.

Submeta sua análise crítica (ficheiro PDF).

Desafio continuado...

Ferramentas anti-forense

Existem ferramentas que permitem esconder informação dentro de outros ficheiros. Esta técnica chama-se de estenografia digital (**steganography**)

Existem dois casos de informações escondidas nas evidências já utilizadas ao longa da aula.

Consegues descobri-las?

Bibliografia

- ▶ Autopsy User's Guide, Autopsy User Documentation
<https://github.com/sleuthkit/autopsy/tree/develop/docs/doxygen-userr>
- ▶ Autopsy Forensic Browser User Guide
Julia Keffer, 2013
https://juliakeffer.files.wordpress.com/2013/06/autopsy_user_guide.pdf