FICHA TRABALHO 2

MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico de Cibersegurança		
UC:	Instalar e configurar ferramentas de análise e recolha de logs e evidências	CÓDIGO UC:	UC01485
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Saber como instalar e configurar o programa de auditoria e análise forense
- Utilização do software Autopsy

A Computação Forense é descrita como a ciência responsável pela recolha, salvaguarda e análise de pegadas digitais, presentes nos diversos dispositivos de processamento (computador, telemóveis, tablets, entre outros), armazenamento (discos rígidos HDD, SSD, backups de rede, entre outros) e comunicação. Para além disso, as ferramentas de computação forense pegam nesses dados para recolha, analisar e interpretar evidências em investigações criminais e civis. Para a realização deste trabalho há várias ferramentas.

Uma das ferramentas de analise forense para obter evidencias digitais em investigações é o Autopsy.

O Autopsy é um software de análise forense digital gratuito utilizado para investigar dispositivos eletrónicos. Permite examinar, recuperar e analisar dados para identificar evidências em investigações criminais, auditorias ou recuperação de informações. Para além disso, é possível integrar mais funcionalidades, com a instalação de plugins (suplementos adicionais) para ajudar a ter uma ferramenta mais completa e verificar casos mais específicos.

O que é possível fazer com o Autopsy?

- Investigação forense
  - Recuperação de ficheiros apagados
  - Análise de metadados dos ficheiros
  - Identificação de atividades suspeitas (ex. acesso a sites ou alterações de ficheiros)

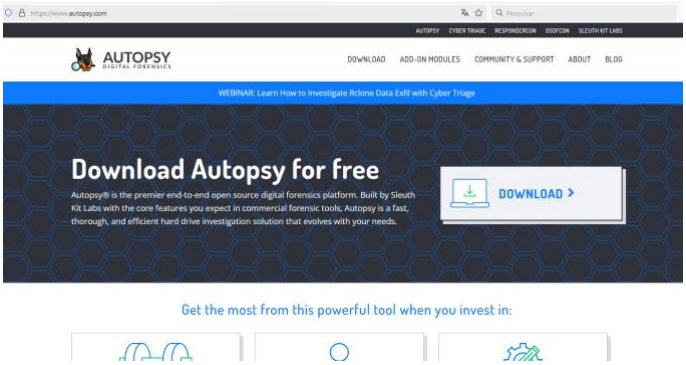
- Análise de sistemas
  - Detetar malware ou atividades maliciosas no sistema
  - Examinar logs de sistemas para verificar eventuais comportamentos

- Recuperação de dados
  - Recuperação de dados perdidos ou danificados devido a falhas no sistema ou exclusões acidentais.

Depois de toda a investigação estar concluída, podemos gerar um relatório acedendo ao separador Tools e clicando em Generate Report.

Parte 1 – Processo de instalação

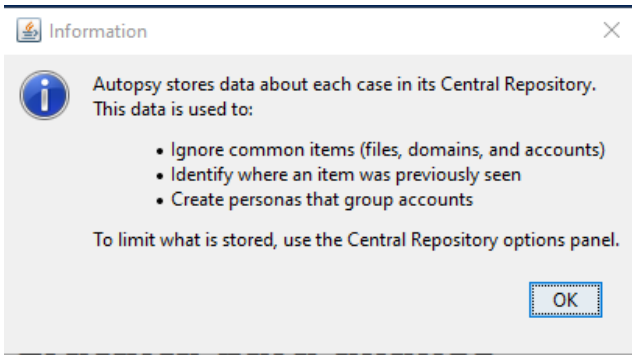
Passo 1 – Aceder a página oficial do Autopsy: https://www.autopsy.com e clicar no botão Download



Passo 2 – Retirar a versão para Windows clicando no botão **Download 64-bit**

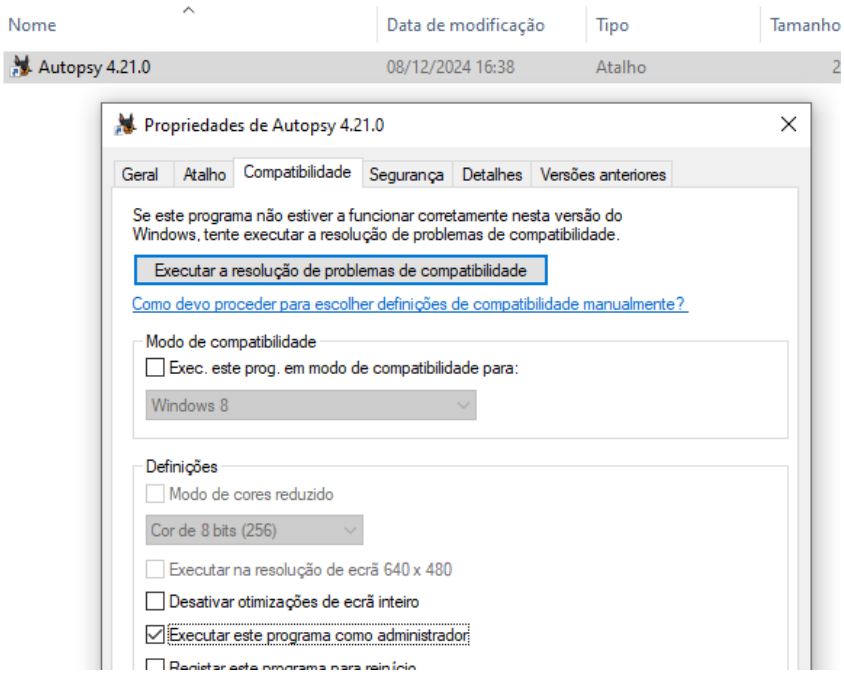


Passo 3 – No processo da instalação será exibida a mensagem a informar sobre alguns aspetos da utilização do programa. De resto, basta seguir os passos da instalação:



Passo 4 – Após a instalação do programa se este arrancar o mesmo automaticamente, deve fechar a aplicação. De seguida, deve clicar com o lado direito do rato em cima do ícone do programa e escolher a opção propriedades.

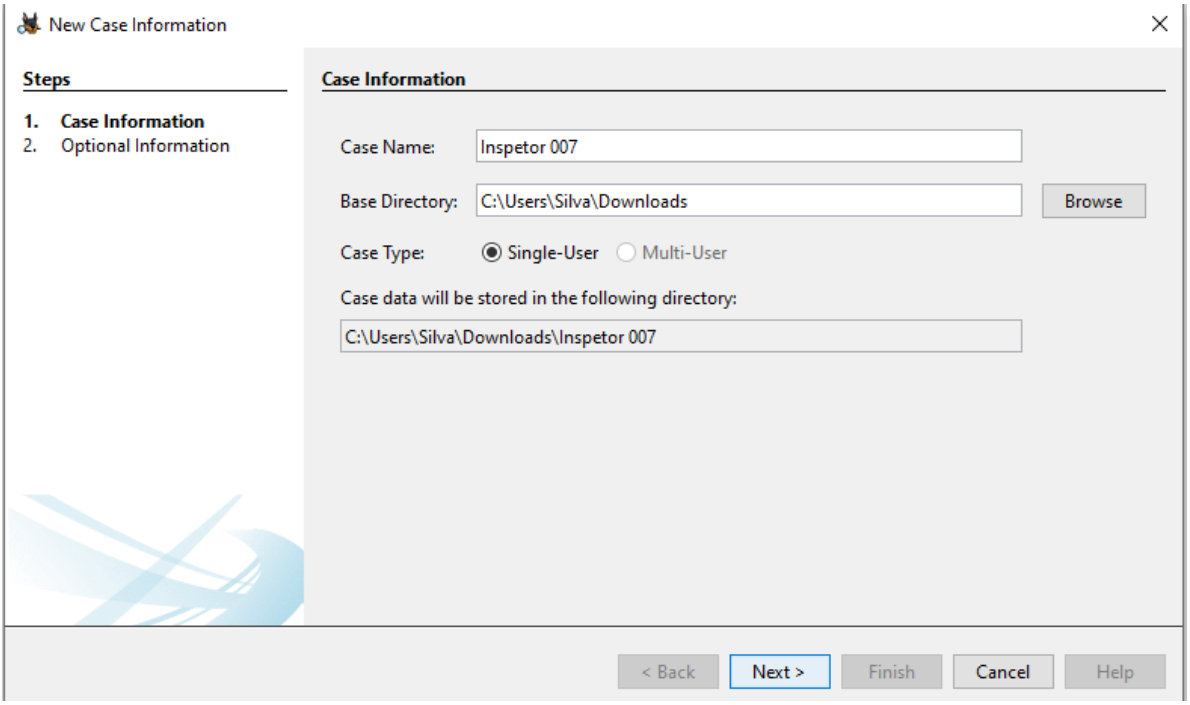
Selecione o separador Compatibilidade e mais abaixo selecione a opção "**Executar este programa como administrador"**.



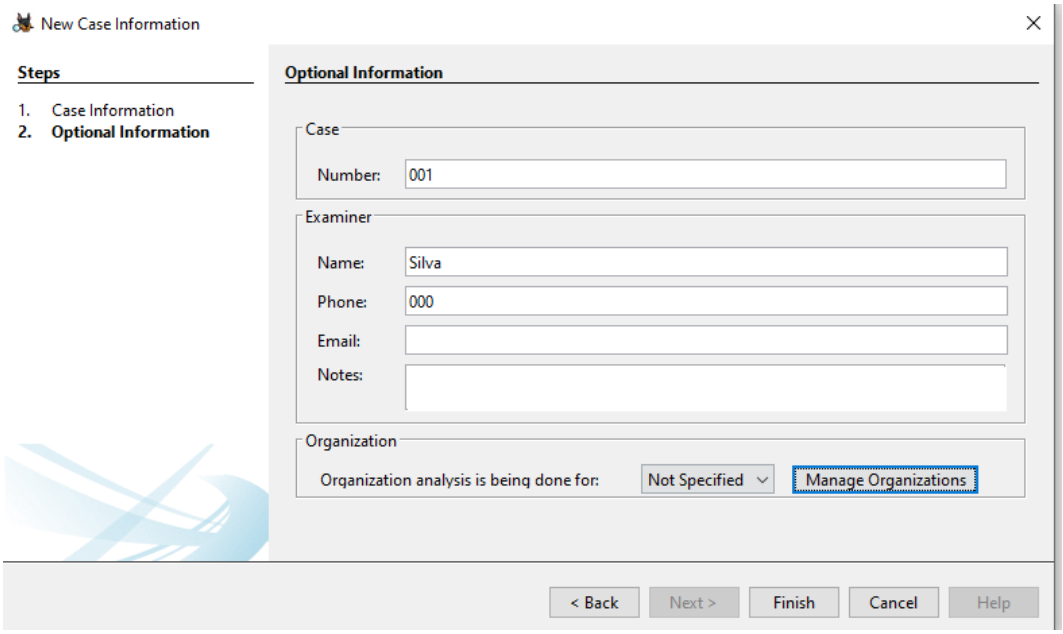
Passo 5 – Na abertura do programa, deve criar um novo caso (embora que possa abrir casos já existentes se já trabalhou anteriormente nalgum procedimento):



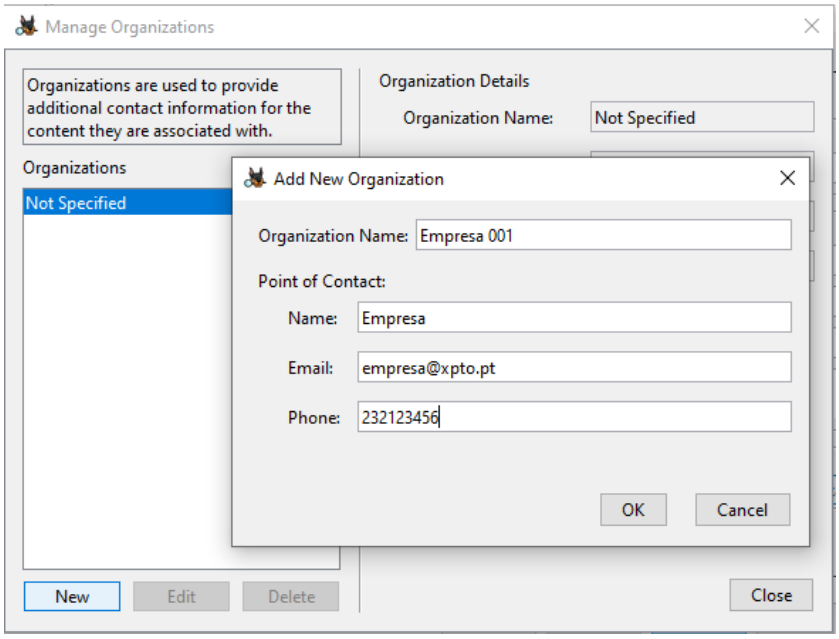
Passo 6 – Colocar as informações sobre o caso, mais especificamente, o nome de identificação, qual o sítio onde vamos guardar os dados da análise:



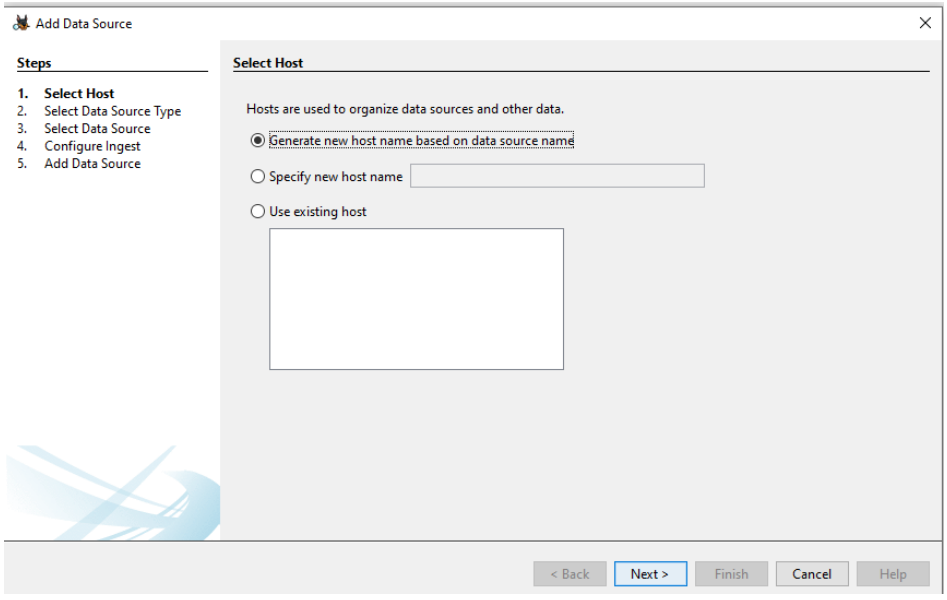
Passo 7 – Colocar as informações opcionais sobre o caso, mais especificamente, o número do caso (ideal para questões de organização e auditorias), dados do examinador/agente e se achar necessário:



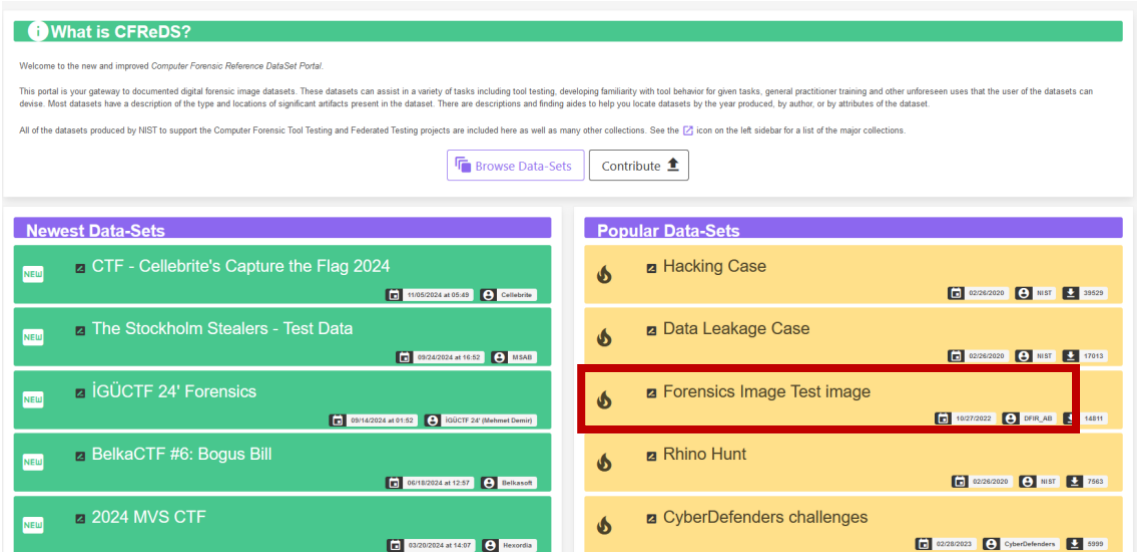
Também pode clicar na opção "Manage Organizations" para colocar dados de organizações a analisar (informações que são usadas para providenciar informações com contatos adicionais para o contexto do quais estão associadas):



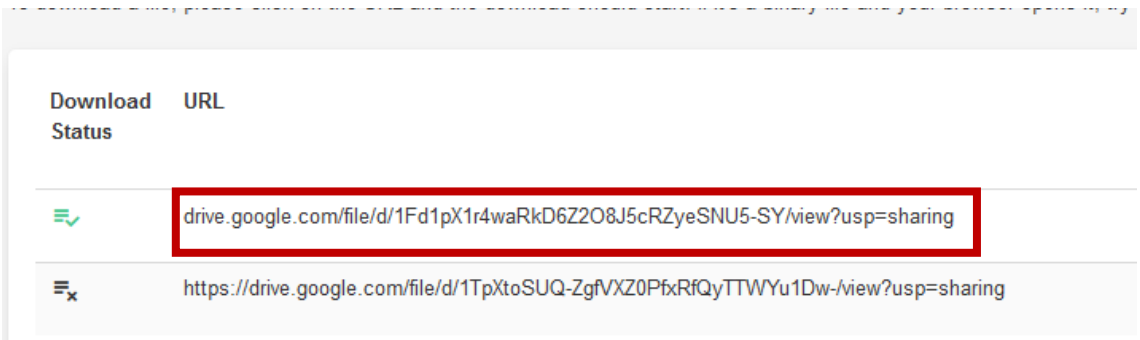
Passo 8 – Normalmente, após adicionar os dados anteriores, será aberto automaticamente a opção para inserir a fonte de dados a analisar. Na primeira parte, vamos indicar a opção "Generate new host name based on data source name":



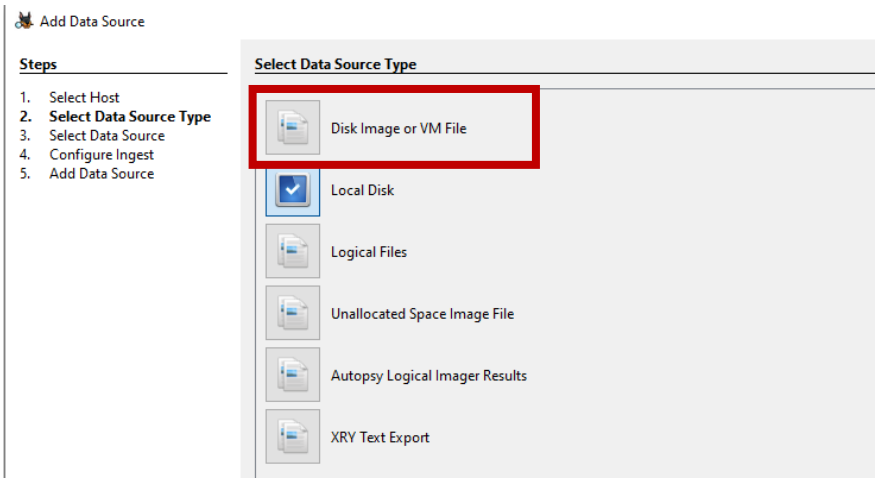
Passo 9 – Podemos selecionar várias fontes de dados a analisar. Neste caso, vamos analisar um Dataset específico (uma imagem de dados de um disco rígido existente) do endereço https://cfreds.nist.gov/, mais especificamente, será a imagem do grupo "Forensics Image Disk Image":



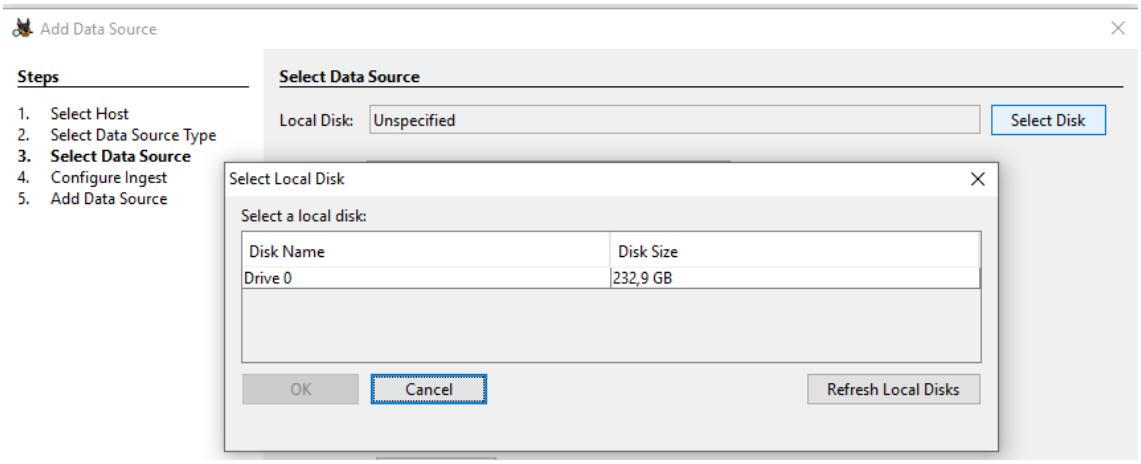
Dentro deste grupo, temos uma imagem pré-preparada com alguns ficheiros suspeitos com o nome "2020JimmyWilson.E01" com cerca de 295MB (bastando clicar no primeiro link):



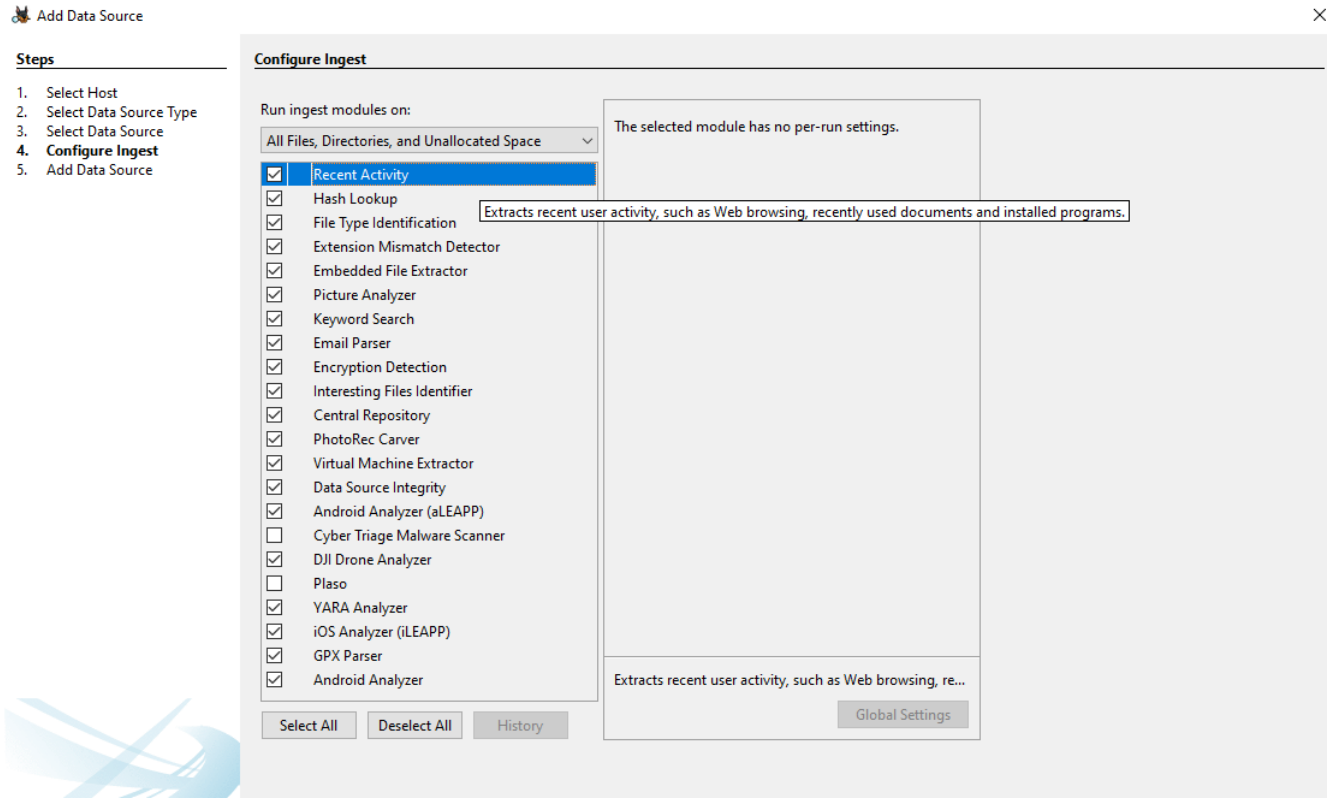
Na continuação da instalação, podemos selecionar várias opções, mas para este caso, vamos selecionar uma imagem existente e como tal, deve selecionar a opção "Disk Image or VM File"



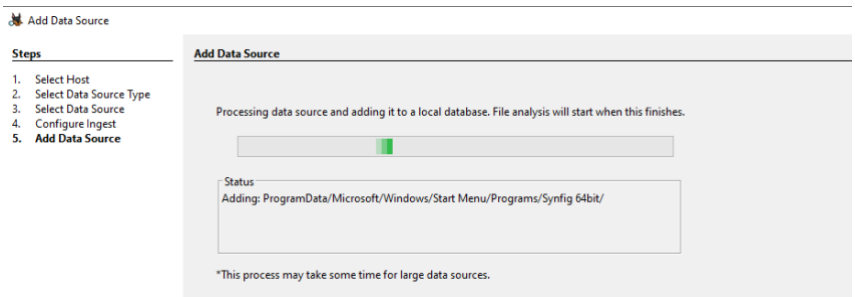
Passo 10 – Depois de analisar a imagem, o programa vai perguntar onde vamos colocar a informação da imagem a analisar:



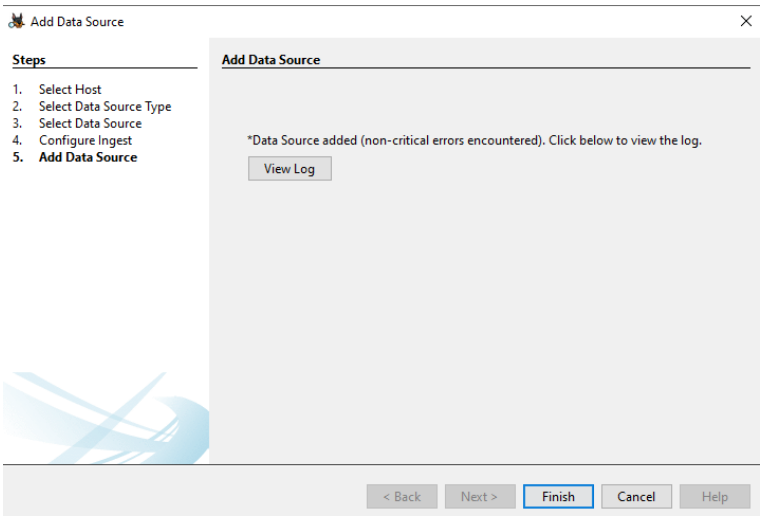
Passo 11 – Vamos deixar todas as opções selecionadas para uma análise mais pormenorizada:

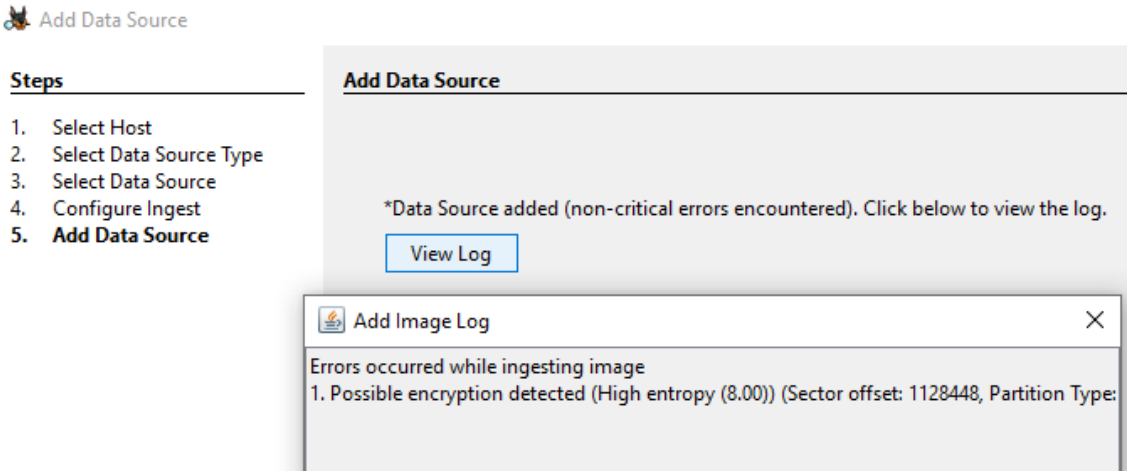


Passo 12 – Após a seleção das opções personalizadas, este irá montar a imagem, analisar, verificar e classificar os conteúdos em causa (este processo pode demorar algum tempo, dependendo da quantidade de informação do disco rígido ou imagem):

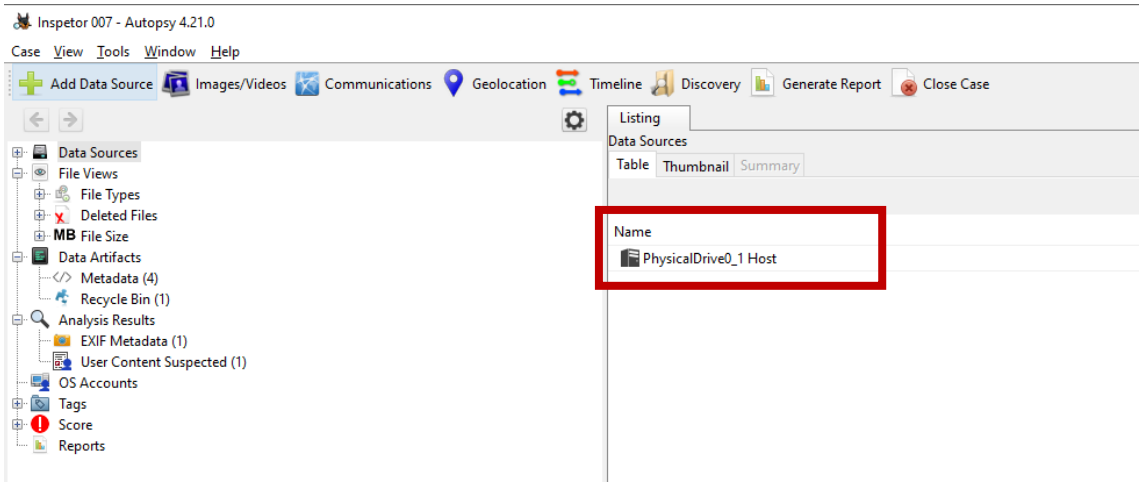


Passo 13 – Após a importação da informação, será exibido os resultados e vamos clicar no botão de finalização:

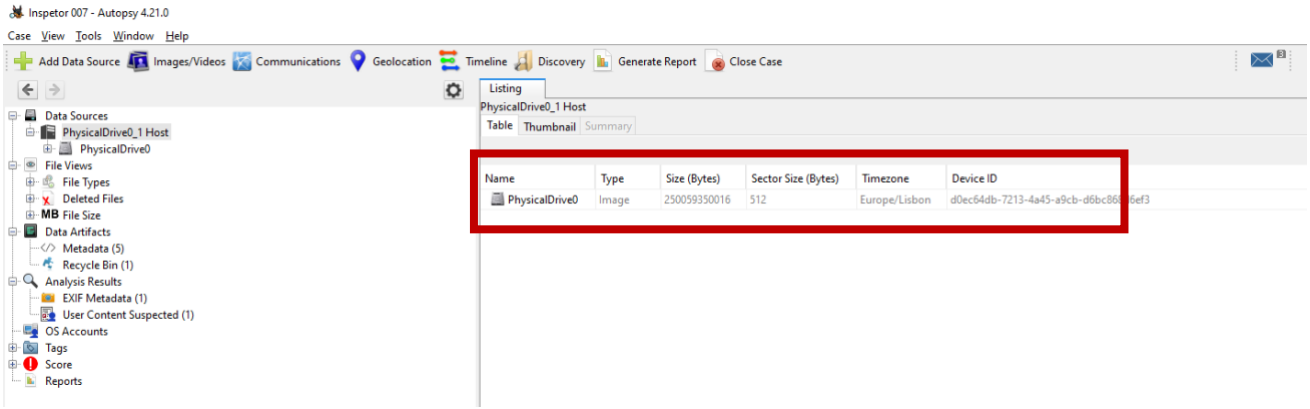




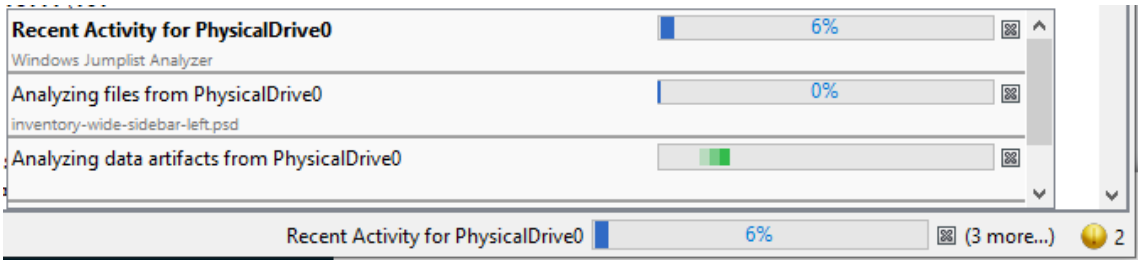
Passo 13 – No ecrã principal, vamos clicar na opção do disco rígido:



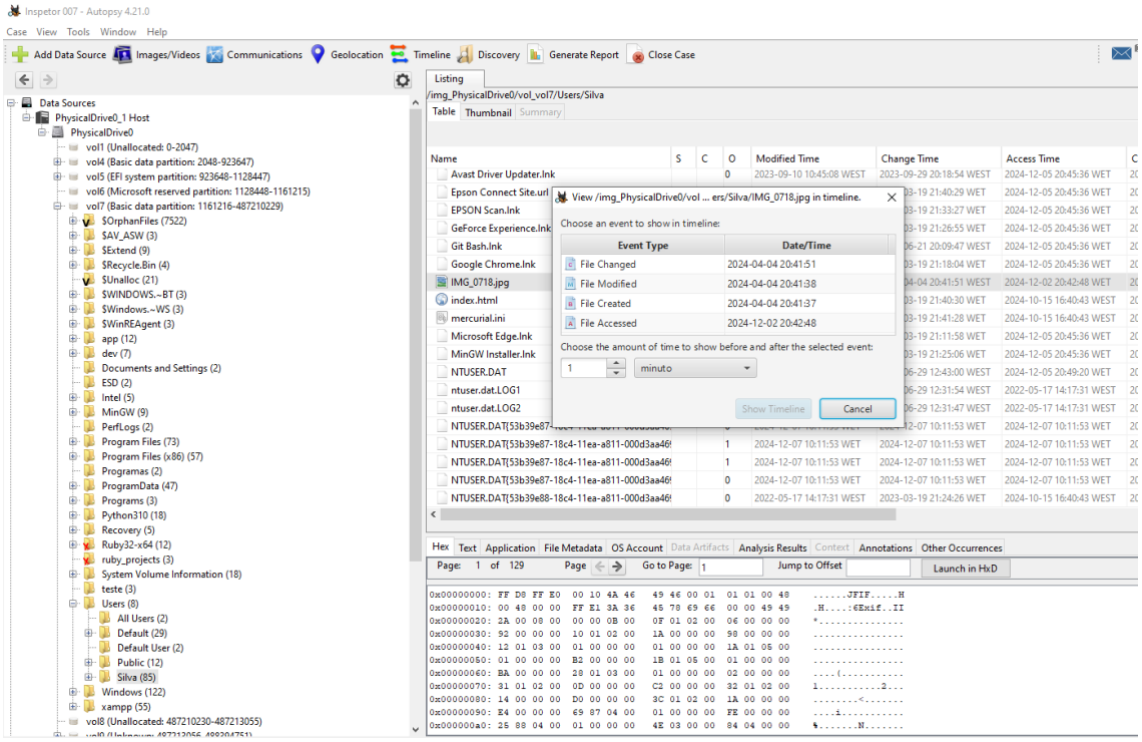
Repare na informação geral que foi identificada na análise do disco principal (ID do dispositivo, Tipo, Tamanho em bytes, Tamanho de Setor e o Fuso Horário):

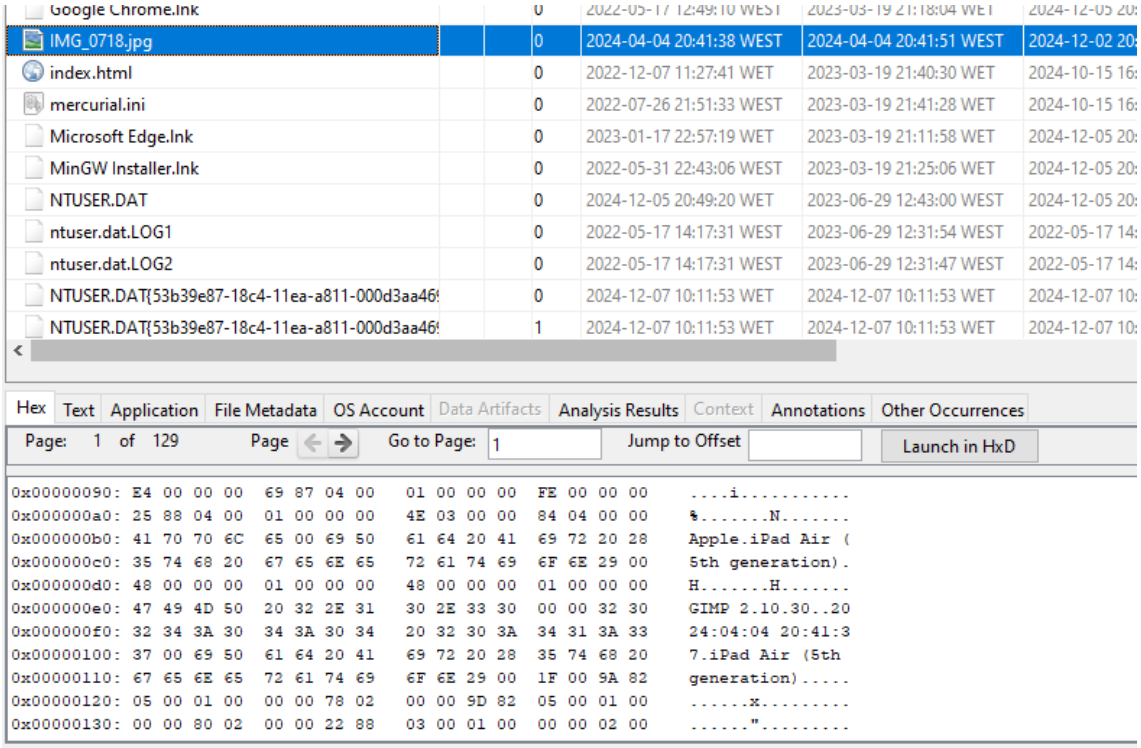


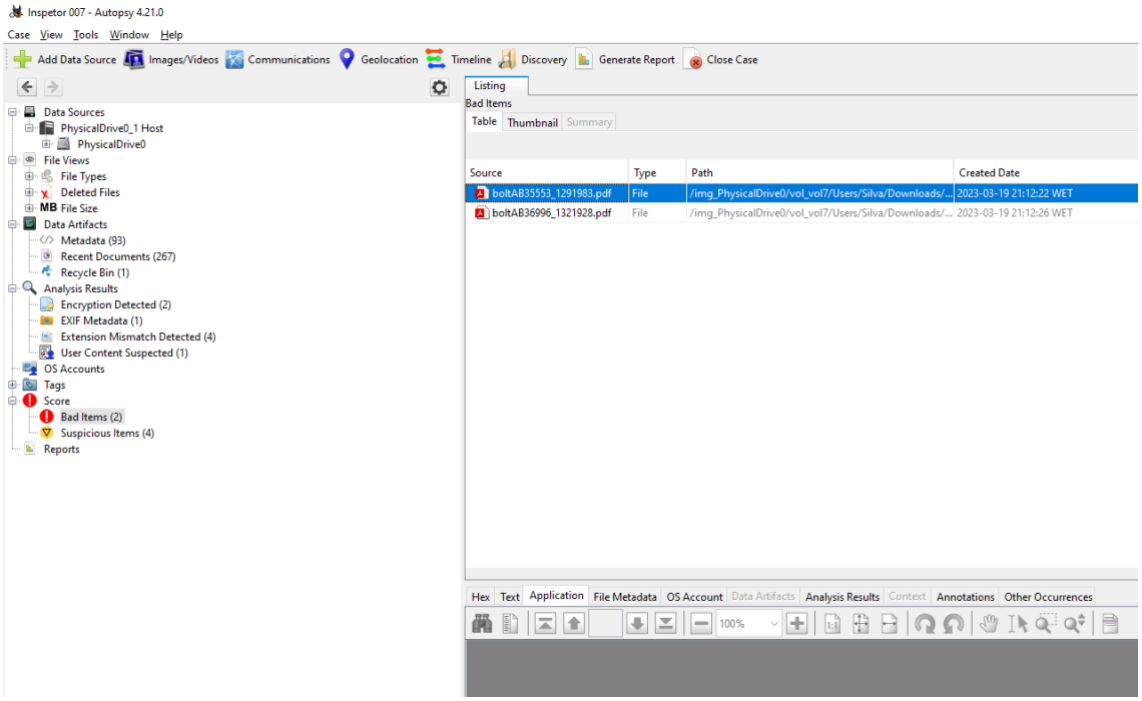
Passo 14 – Se reparar no canto inferior direito da aplicação a operação de atividade e classificação de informação ainda está a ser processada. Este processo é vital, para depois retirar relatórios e ajudar a compilar informação vital na análise forense:

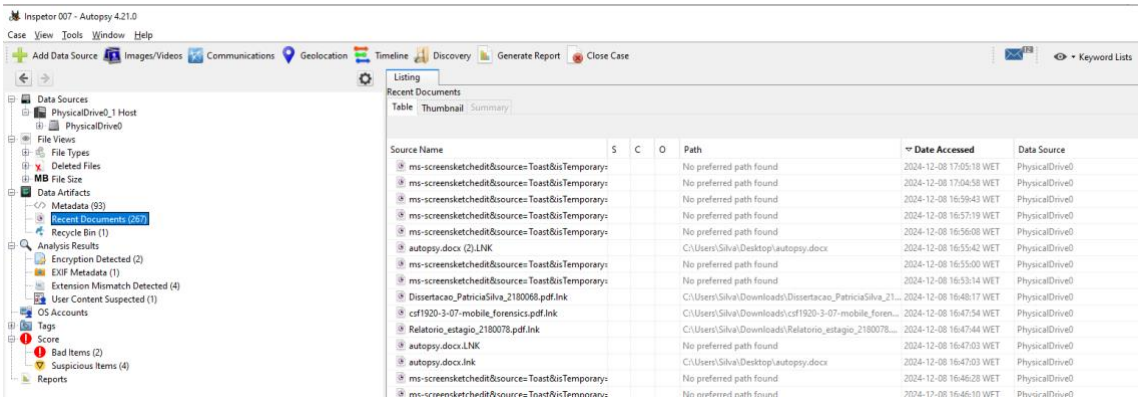


Passo 14 – Se reparar no canto inferior direito da aplicação a operação de atividade e classificação de informação ainda está a ser processada. Este processo é vital, para depois retirar relatórios e ajudar a compilar informação vital na análise forense:

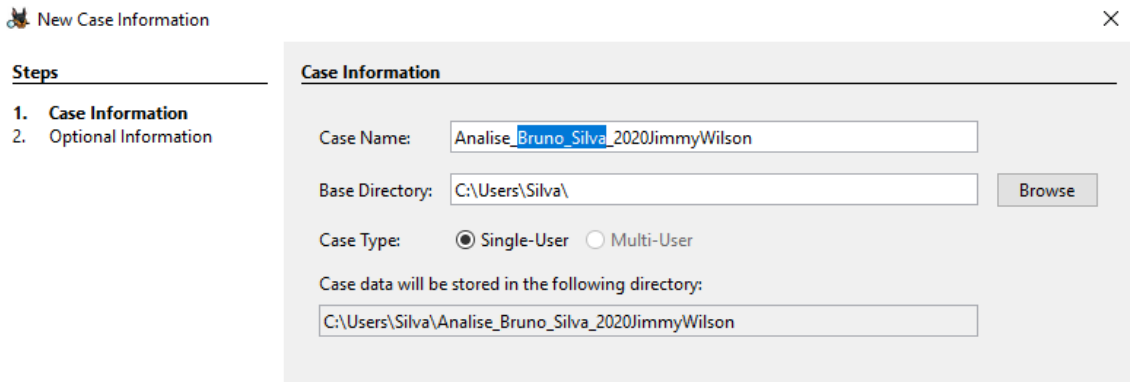

Inspetor 007 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Data Sources
PhysicalDrive0_1 Host
PhysicalDrive0
vol1 (Unallocated: 0-2047)
vol4 (Basic data partition: 2048-923647)
vol5 (EFI system partition: 923648-1128447)
vol6 (Microsoft reserved partition: 1128448-1161215)
vol7 (Basic data partition: 1161216-487210229)
$OrphanFiles (7522)
$AV_ASW (3)
$Extend (9)
$Recycle.Bin (4)
$Unalloc (21)
$WINDOWS.~BT (3)
$Windows.~WS (3)
$WinREAgent (3)
app (12)
dev (7)
Documents and Settings (2)
ESD (2)
Intel (5)
MinGW (9)
PerfLogs (2)
Program Files (73)
Program Files (x86) (57)
Programas (2)
ProgramData (47)
Programs (3)
Python310 (18)
Recovery (5)
Ruby32-x64 (12)
ruby_projects (3)
System Volume Information (18)
teste (3)
Users (8)
All Users (2)
Default (29)
Default User (2)
Public (12)
Silva (85)
Windows (122)
xampp (55)
vol8 (Unallocated: 487210230-487213055)
Listing
/img_PhysicalDrive0/vol_vol7/Users/Silva
Table Thumbnail Summary
Name S C O Modified Time Change Time Access Time
Avast Driver Updater.lnk 0 2023-09-10 10:45:08 WEST 2023-09-29 20:18:54 WEST 2024-12-05 20:45:36 WET
Epson Connect Site.url 2023-03-19 21:40:29 WET 2024-12-05 20:45:36 WET
EPSON Scan.lnk 2023-03-19 21:33:27 WET 2024-12-05 20:45:36 WET
GeForce Experience.lnk 2023-03-19 21:26:55 WET 2024-12-05 20:45:36 WET
Git Bash.lnk 2023-06-21 20:09:47 WEST 2024-12-05 20:45:36 WET
Google Chrome.lnk 2023-03-19 21:18:04 WET 2024-12-05 20:45:36 WET
IMG_0718.jpg 2024-04-04 20:41:51 WEST 2024-12-02 20:42:48 WET
index.html 2023-03-19 21:40:30 WET 2024-10-15 16:40:43 WEST
mercurial.ini 2023-03-19 21:41:28 WET 2024-10-15 16:40:43 WEST
Microsoft Edge.lnk 2023-03-19 21:11:58 WET 2024-12-05 20:45:36 WET
MinGW Installer.lnk 2023-03-19 21:25:06 WET 2024-12-05 20:45:36 WET
NTUSER.DAT 2023-06-29 12:43:00 WEST 2024-12-05 20:49:20 WET
ntuser.dat.LOG1 2022-05-17 14:17:31 WEST 2023-06-29 12:31:54 WEST 2022-05-17 14:17:31 WEST
ntuser.dat.LOG2 2022-05-17 14:17:31 WEST 2023-06-29 12:31:47 WEST 2022-05-17 14:17:31 WEST
NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa46 0 2024-12-07 10:11:53 WET 2024-12-07 10:11:53 WET 2024-12-07 10:11:53 WET
NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa46 1 2024-12-07 10:11:53 WET 2024-12-07 10:11:53 WET 2024-12-07 10:11:53 WET
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa46 0 2022-05-17 14:17:31 WEST 2023-03-19 21:24:26 WET 2024-10-15 16:40:43 WEST
View /img_PhysicalDrive0/vol ... ers/Silva/IMG_0718.jpg in timeline.
Choose an event to show in timeline:
Event Type Date/Time
File Changed 2024-04-04 20:41:51
File Modified 2024-04-04 20:41:38
File Created 2024-04-04 20:41:37
File Accessed 2024-12-02 20:42:48
Choose the amount of time to show before and after the selected event:
1 minuto
Show Timeline Cancel
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Page: 1 of 129 Page Go to Page: 1 Jump to Offset Launch in HxD

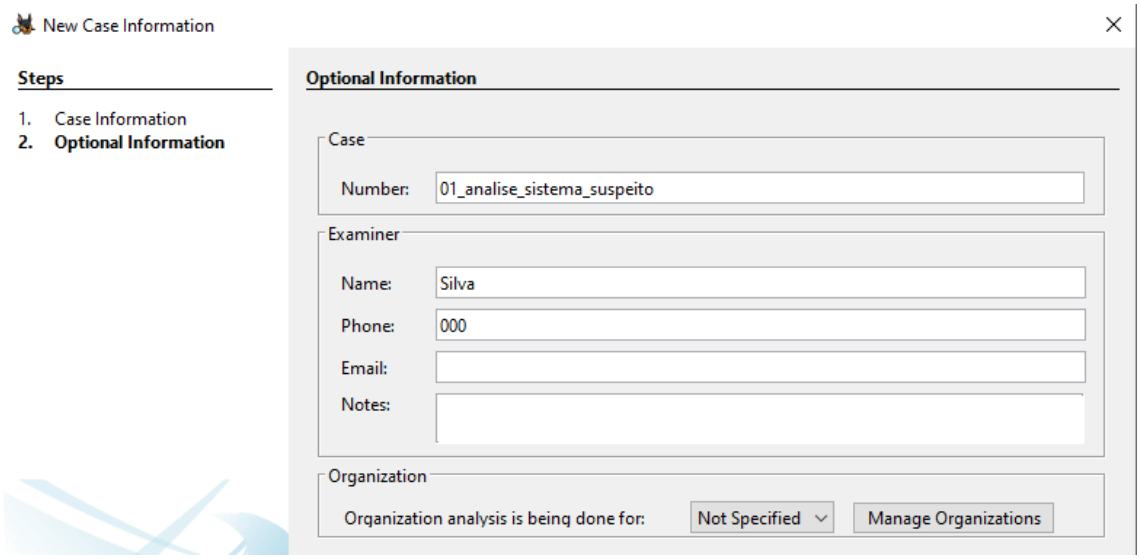

Google Chrome.lnk 0 2022-05-17 12:49:10 WEST 2023-03-19 21:18:04 WET 2024-12-05 20:
IMG_0718.jpg 0 2024-04-04 20:41:38 WEST 2024-04-04 20:41:51 WEST 2024-12-02 20:
index.html 0 2022-12-07 11:27:41 WET 2023-03-19 21:40:30 WET 2024-10-15 16:
mercurial.ini 0 2022-07-26 21:51:33 WEST 2023-03-19 21:41:28 WET 2024-10-15 16:
Microsoft Edge.lnk 0 2023-01-17 22:57:19 WET 2023-03-19 21:11:58 WET 2024-12-05 20:
MinGW Installer.lnk 0 2022-05-31 22:43:06 WEST 2023-03-19 21:25:06 WET 2024-12-05 20:
NTUSER.DAT 0 2024-12-05 20:49:20 WET 2023-06-29 12:43:00 WEST 2024-12-05 20:
ntuser.dat.LOG1 0 2022-05-17 14:17:31 WEST 2023-06-29 12:31:54 WEST 2022-05-17 14:
ntuser.dat.LOG2 0 2022-05-17 14:17:31 WEST 2023-06-29 12:31:47 WEST 2022-05-17 14:
NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa46 0 2024-12-07 10:11:53 WET 2024-12-07 10:11:53 WET 2024-12-07 10:
NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa46 1 2024-12-07 10:11:53 WET 2024-12-07 10:11:53 WET 2024-12-07 10:
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Page: 1 of 129 Page Go to Page: 1 Jump to Offset Launch in HxD
0x00000090: E4 00 00 00 69 87 04 00 01 00 00 00 FE 00 00 00 ....i...........
0x000000a0: 25 88 04 00 01 00 00 00 4E 03 00 00 84 04 00 00 %.......N.......
0x000000b0: 41 70 70 6C 65 00 69 50 61 64 20 41 69 72 20 28 Apple.iPad Air (
0x000000c0: 35 74 68 20 67 65 6E 65 72 61 74 69 6F 6E 29 00 5th generation).
0x000000d0: 48 00 00 00 01 00 00 00 48 00 00 00 01 00 00 00 H.......H.......
0x000000e0: 47 49 4D 50 20 32 2E 31 30 2E 33 30 00 00 32 30 GIMP 2.10.30..20
0x000000f0: 32 34 3A 30 34 3A 30 34 20 32 30 3A 34 31 3A 33 24:04:04 20:41:3
0x00000100: 37 00 69 50 61 64 20 41 69 72 20 28 35 74 68 20 7.iPad Air (5th
0x00000110: 67 65 6E 65 72 61 74 69 6F 6E 29 00 1F 00 9A 82 generation).....
0x00000120: 05 00 01 00 00 00 78 02 00 00 9D 82 05 00 01 00 ......x.........
0x00000130: 00 00 80 02 00 00 22 88 03 00 01 00 00 00 02 00 ......".........

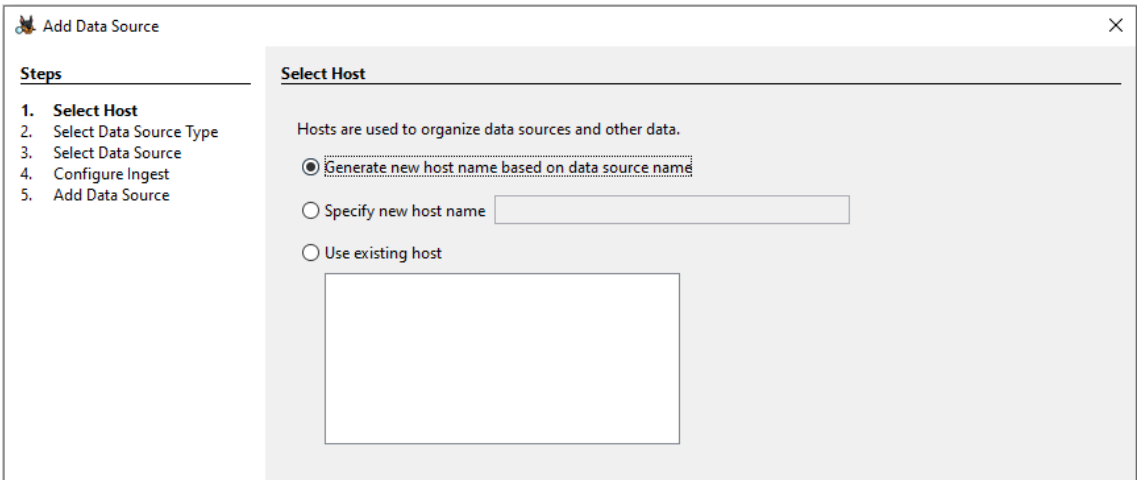


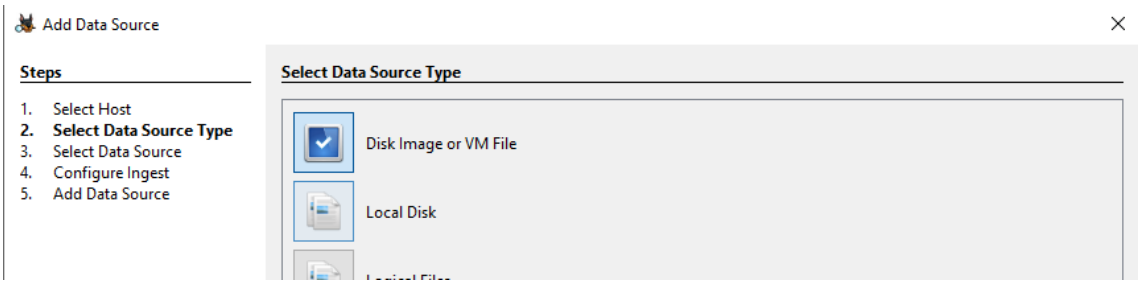


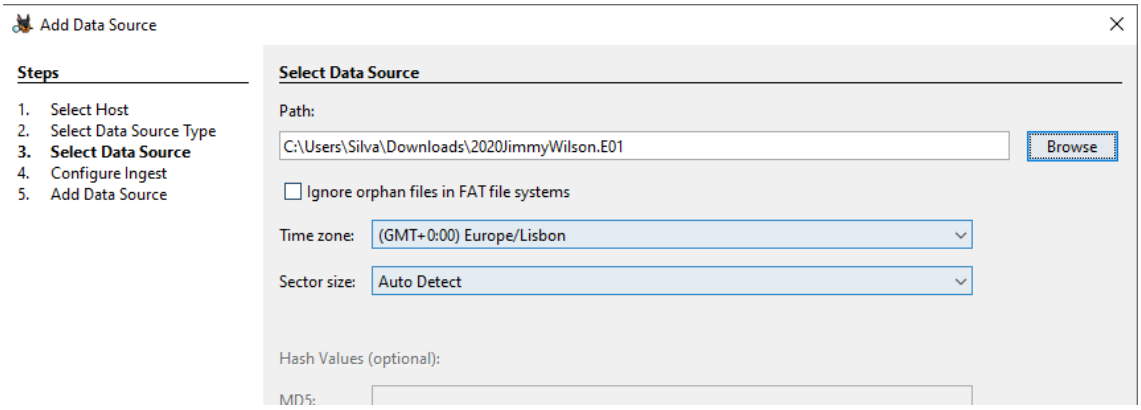
Exercício Prático:

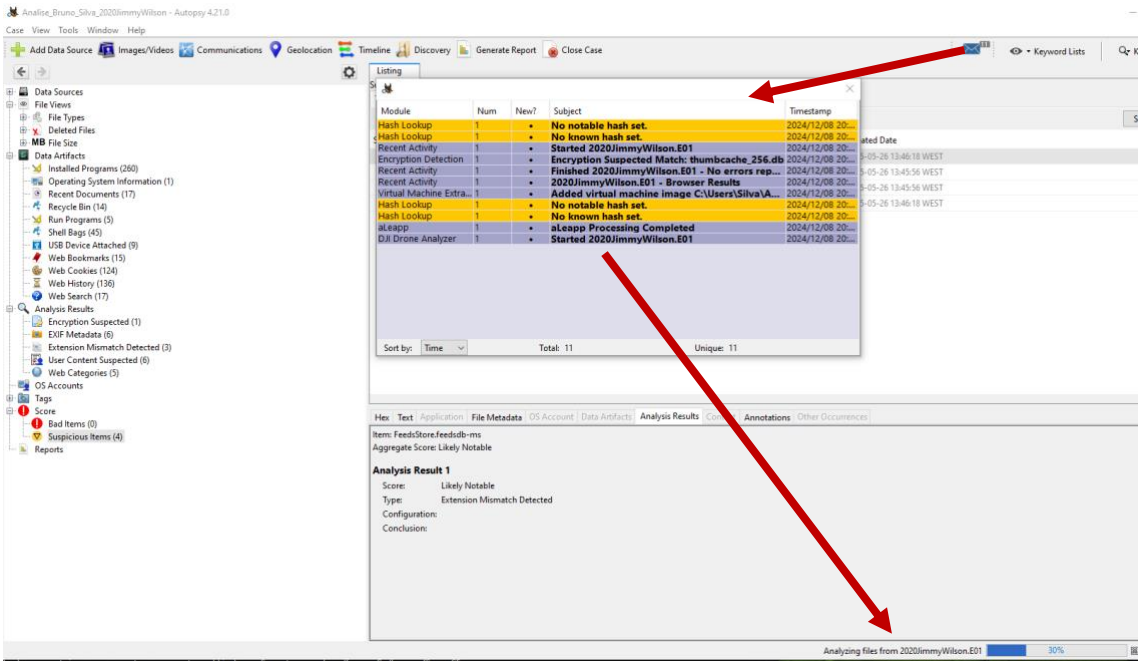

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: Analise_Bruno_Silva_2020JimmyWilson
Base Directory: C:\Users\Silva\
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
C:\Users\Silva\Analise_Bruno_Silva_2020JimmyWilson

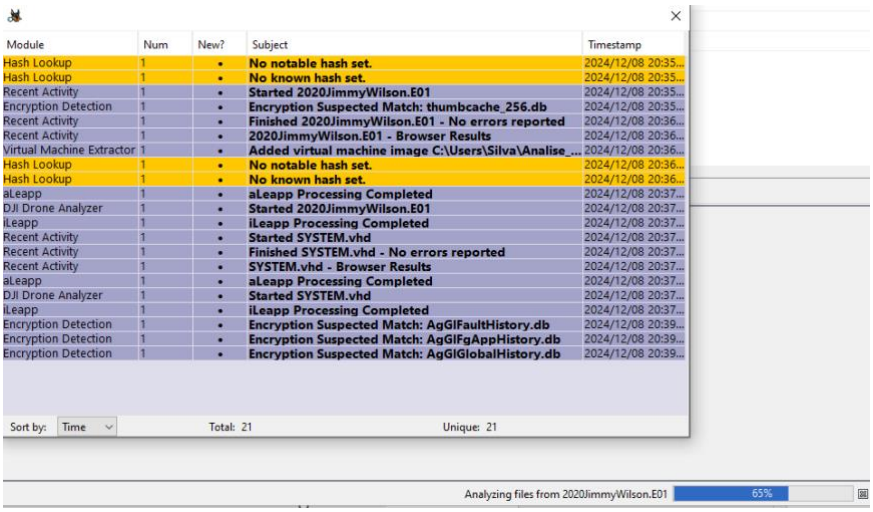

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 01_analise_sistema_suspeito
Examiner
Name: Silva
Phone: 000
Email:
Notes:
Organization
Organization analysis is being done for: Not Specified
Manage Organizations


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk

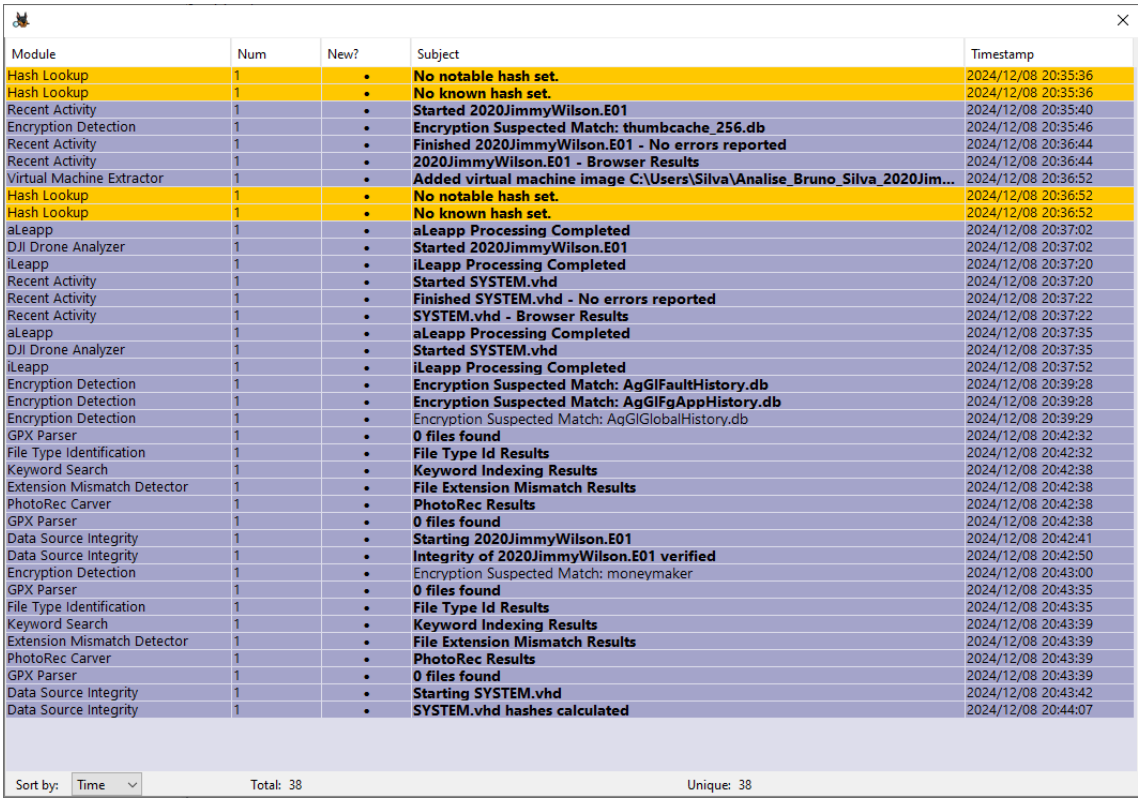

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
C:\Users\Silva\Downloads\2020JimmyWilson.E01
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT+0:00) Europe/Lisbon
Sector size:
Auto Detect
Hash Values (optional):
MD5:


Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Listing
Module
Num
New?
Subject
Timestamp
Hash Lookup
No notable hash set.
No known hash set.
Recent Activity
Started 2020JimmyWilson.E01
Encryption Detection
Encryption Suspected Match: thumbcache_256.db
Finished 2020JimmyWilson.E01 - No errors rep...
2020JimmyWilson.E01 - Browser Results
Virtual Machine Extra...
Added virtual machine image C:\Users\Silva\A...
aLeapp
aLeapp Processing Completed
DJI Drone Analyzer
Started 2020JimmyWilson.E01
Sort by:
Time
Total: 11
Unique: 11
Analysis Result 1
Score:
Likely Notable
Type:
Extension Mismatch Detected
Configuration:
Conclusion:
Analyzing files from 2020JimmyWilson.E01
30%



Módulos suspeitos:

- Ponto 4 → Tumbcache_256.db
- Ponto 19-21 → AgGlFgAppHistory.db
- Ponto 30 → moneymaker

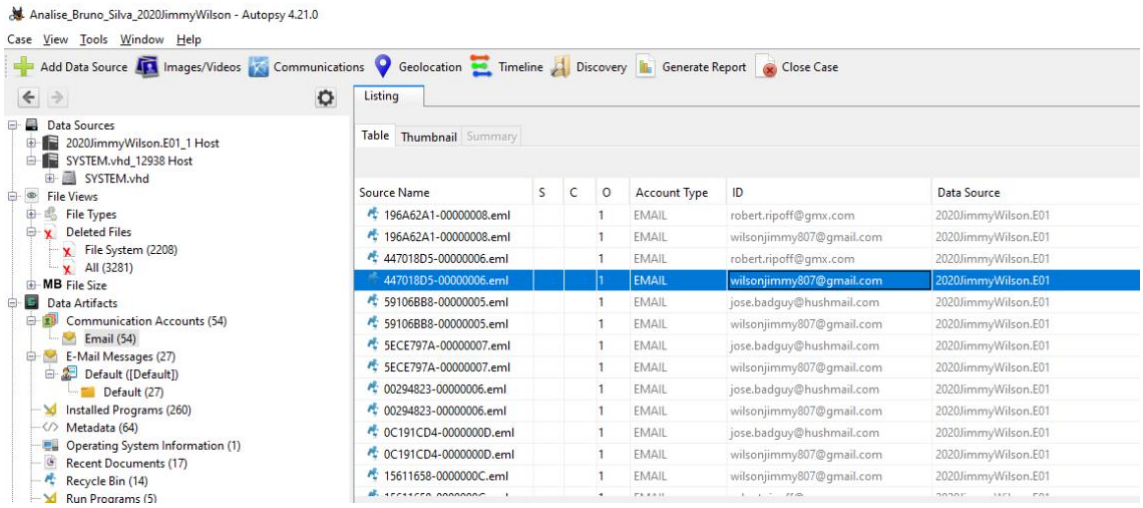


Module	Num	New?	Subject	Timestamp
Hash Lookup	1	•	**No notable hash set.**	2024/12/08 20:35:36
Hash Lookup	1	•	**No known hash set.**	2024/12/08 20:35:36
Recent Activity	1	•	**Started 2020JimmyWilson.E01**	2024/12/08 20:35:40
Encryption Detection	1	•	**Encryption Suspected Match: thumbcache_256.db**	2024/12/08 20:35:46
Recent Activity	1	•	**Finished 2020JimmyWilson.E01 - No errors reported**	2024/12/08 20:36:44
Recent Activity	1	•	**2020JimmyWilson.E01 - Browser Results**	2024/12/08 20:36:44
Virtual Machine Extractor	1	•	**Added virtual machine image C:\Users\Silva\Analise_Bruno_Silva_2020Jim...**	2024/12/08 20:36:52
Hash Lookup	1	•	**No notable hash set.**	2024/12/08 20:36:52
Hash Lookup	1	•	**No known hash set.**	2024/12/08 20:36:52
aLeapp	1	•	**aLeapp Processing Completed**	2024/12/08 20:37:02
DJI Drone Analyzer	1	•	**Started 2020JimmyWilson.E01**	2024/12/08 20:37:02
iLeapp	1	•	**iLeapp Processing Completed**	2024/12/08 20:37:20
Recent Activity	1	•	**Started SYSTEM.vhd**	2024/12/08 20:37:20
Recent Activity	1	•	**Finished SYSTEM.vhd - No errors reported**	2024/12/08 20:37:22
Recent Activity	1	•	**SYSTEM.vhd - Browser Results**	2024/12/08 20:37:22
aLeapp	1	•	**aLeapp Processing Completed**	2024/12/08 20:37:35
DJI Drone Analyzer	1	•	**Started SYSTEM.vhd**	2024/12/08 20:37:35
iLeapp	1	•	**iLeapp Processing Completed**	2024/12/08 20:37:52
Encryption Detection	1	•	**Encryption Suspected Match: AgGlFaultHistory.db**	2024/12/08 20:39:28
Encryption Detection	1	•	**Encryption Suspected Match: AgGlFgAppHistory.db**	2024/12/08 20:39:28
Encryption Detection	1	•	Encryption Suspected Match: AgGlGlobalHistory.db	2024/12/08 20:39:29
GPX Parser	1	•	**0 files found**	2024/12/08 20:42:32
File Type Identification	1	•	**File Type Id Results**	2024/12/08 20:42:32
Keyword Search	1	•	**Keyword Indexing Results**	2024/12/08 20:42:38
Extension Mismatch Detector	1	•	**File Extension Mismatch Results**	2024/12/08 20:42:38
PhotoRec Carver	1	•	**PhotoRec Results**	2024/12/08 20:42:38
GPX Parser	1	•	**0 files found**	2024/12/08 20:42:38
Data Source Integrity	1	•	**Starting 2020JimmyWilson.E01**	2024/12/08 20:42:41
Data Source Integrity	1	•	**Integrity of 2020JimmyWilson.E01 verified**	2024/12/08 20:42:50
Encryption Detection	1	•	Encryption Suspected Match: moneymaker	2024/12/08 20:43:00
GPX Parser	1	•	**0 files found**	2024/12/08 20:43:35
File Type Identification	1	•	**File Type Id Results**	2024/12/08 20:43:35
Keyword Search	1	•	**Keyword Indexing Results**	2024/12/08 20:43:39
Extension Mismatch Detector	1	•	**File Extension Mismatch Results**	2024/12/08 20:43:39
PhotoRec Carver	1	•	**PhotoRec Results**	2024/12/08 20:43:39
GPX Parser	1	•	**0 files found**	2024/12/08 20:43:39
Data Source Integrity	1	•	**Starting SYSTEM.vhd**	2024/12/08 20:43:42
Data Source Integrity	1	•	**SYSTEM.vhd hashes calculated**	2024/12/08 20:44:07

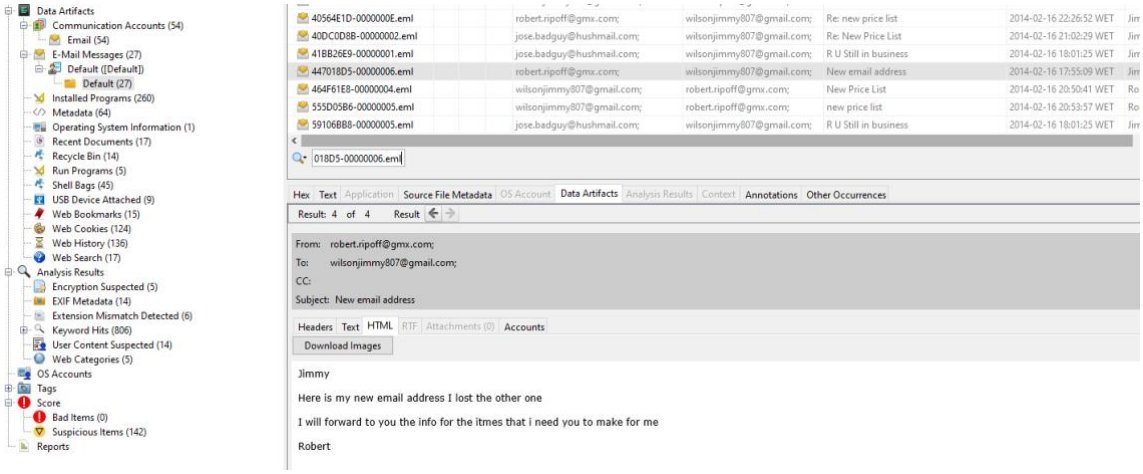
Sort by: Time — Total: 38 — Unique: 38

1. Analise o grupo Data Artifacts, e tente descobrir as seguintes informações:

1.1. No separador "Communication accounts" → "Email", verifique se encontra a conta do email com o nome wilsonjimmy807@gmail.com;

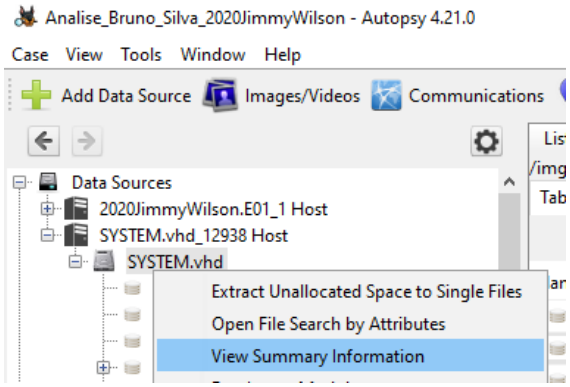


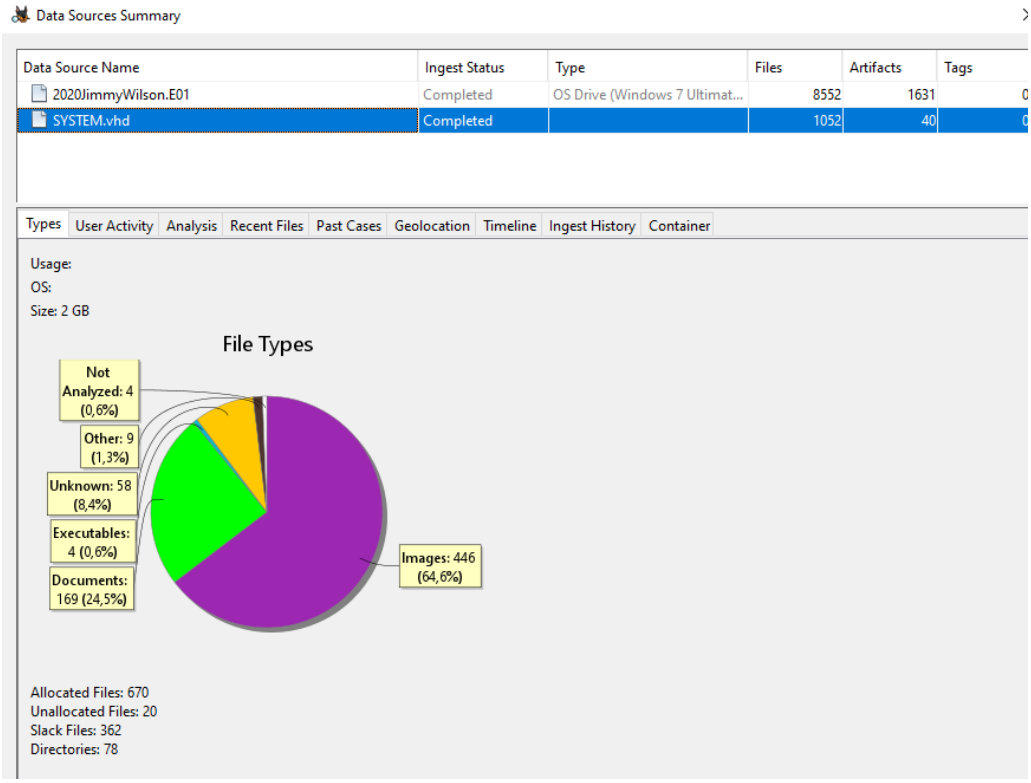
1.2. Dentro do separador "E-mail Messages" veja se encontra o pacote do email com a informação "447018D5-00000006.eml" e indique qual é o fuso horário da data em que recebeu o email;



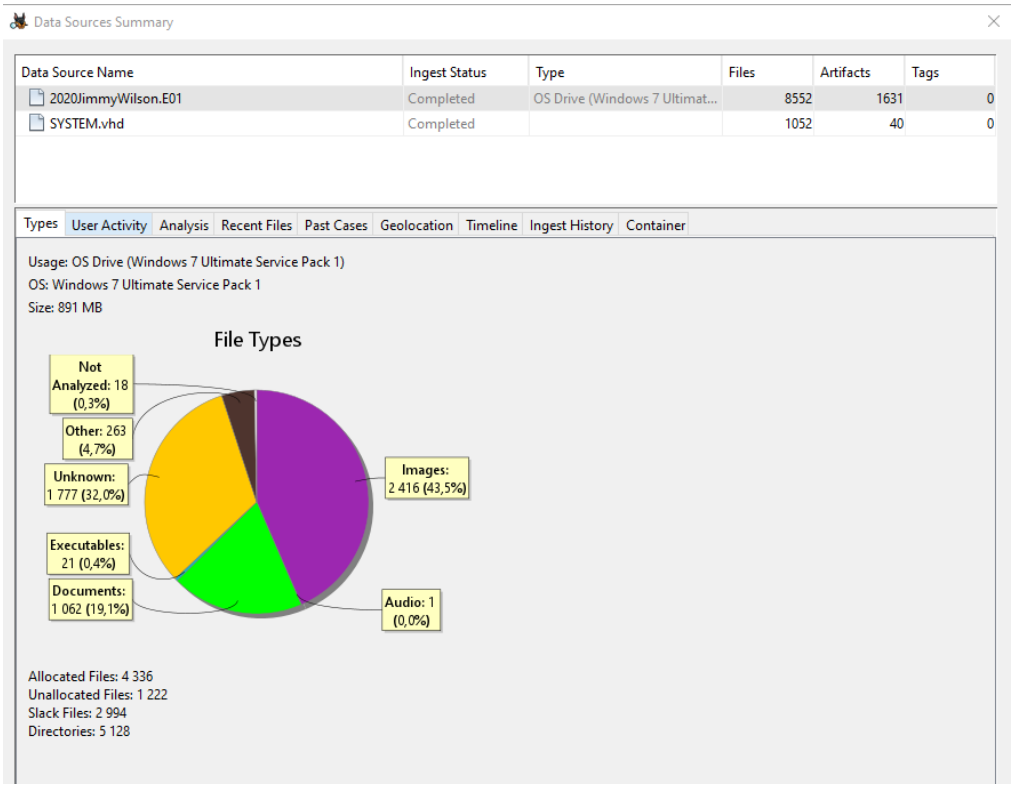
1.3. Coordinated Universal Time (UTC) é o mesmo de Western European Time (WET)?

1.4. No disco "SYSTEM.vhd" é possível verificar o gráfico com informações de ficheiros. Após analisar o gráfico, qual é a informação que representa a maior percentagem de informação?



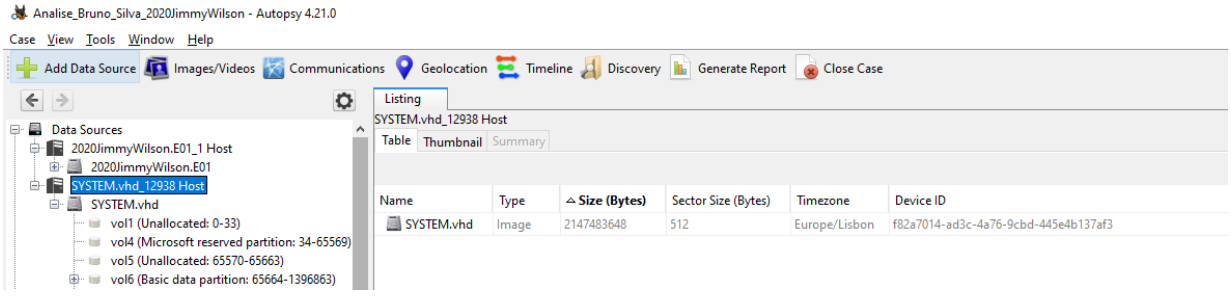


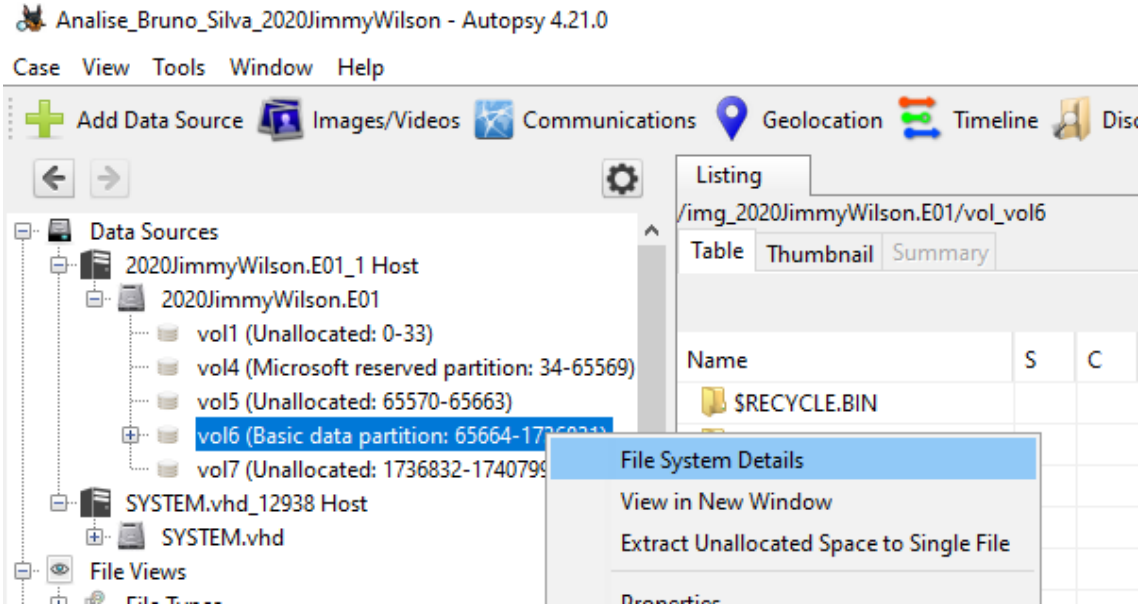
1.5. No disco "/img_2020JimmyWilson.E01_1 Host" é possível verificar o gráfico com informações de ficheiros. Após analisar o gráfico, qual é a informação que representa a maior percentagem de informação?

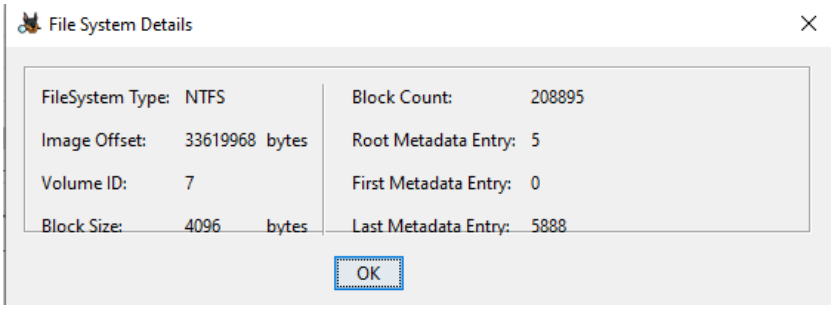


1.6. Ainda na análise do disco "/img_2020JimmyWilson.E01_1 Host, mais especificamente, no separador "User activity", podemos verificar informações sobre a atividade recente do utilizador. Quais são as informações?

1.7. Analise o disco "SYSTEM.vhd" e indique qual é o tamanho da imagem/disco medida em Bytes e o ID do dispositivo?







Ver registos de atividade do computador num determinado dia (neste caso, 20-02-2014 pelas 17:02:35 com o código de inicialização 6015)

Acquiring the required file from the evidence

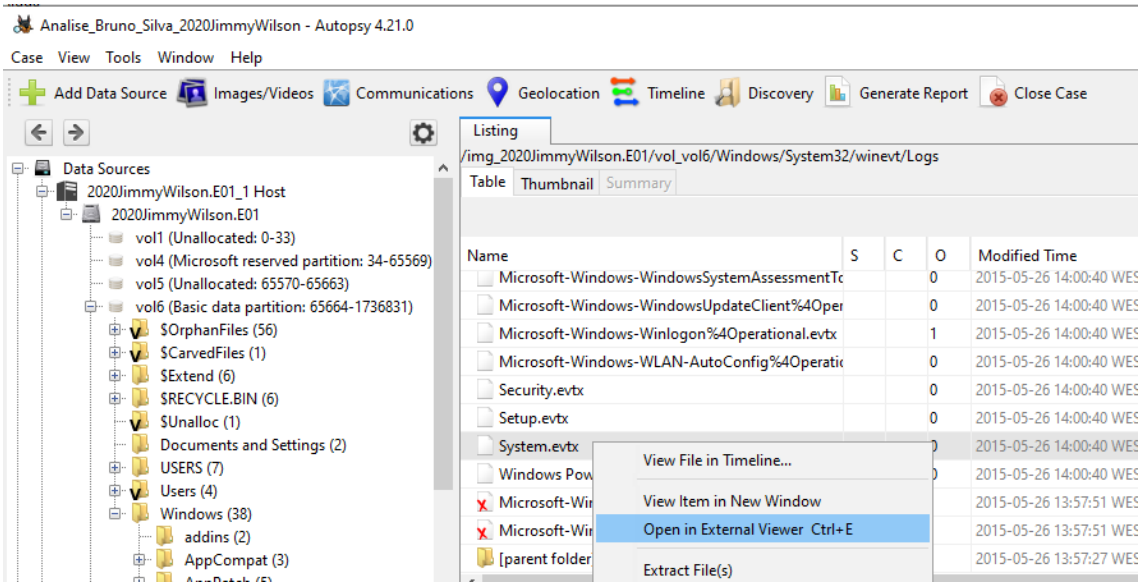
First, we need to acquire the system event log. This file is named system.evt (Windows 2000/2003 and XP) or system.evtx (Windows 2008 / Vista and up). Open the image using your preferred tool (i use FTK Imager) and browse to the following location:

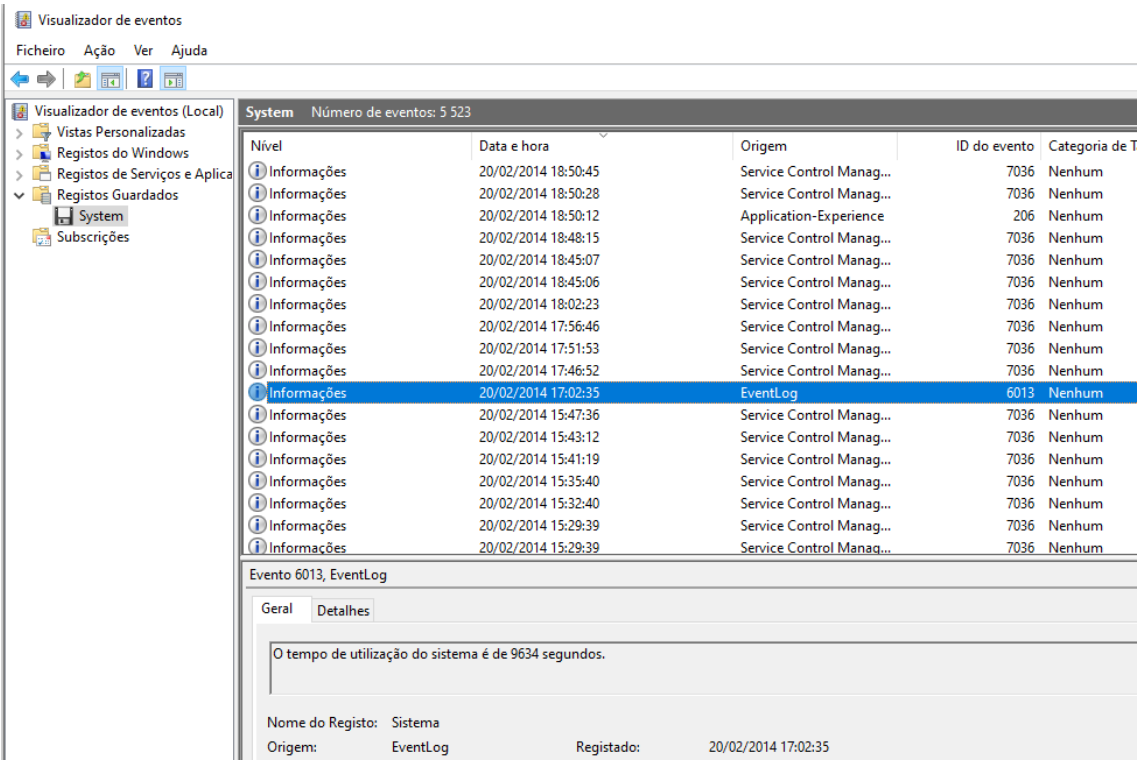
Windows 2000, 2003 and XP

[root]\Windows\System32\Config\SysEvent.Evt

Windows 2008, Vista and up

[root]\Windows\system32\winevt\logs\system.evtx


Analise_Bruno_Silva_2020JimmyWilson - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Listing
/img_2020JimmyWilson.E01/vol_vol6/Windows/System32/winevt/Logs
Table
Thumbnail
Summary
Data Sources
2020JimmyWilson.E01_1 Host
2020JimmyWilson.E01
vol1 (Unallocated: 0-33)
vol4 (Microsoft reserved partition: 34-65569)
vol5 (Unallocated: 65570-65663)
vol6 (Basic data partition: 65664-1736831)
$OrphanFiles (56)
$CarvedFiles (1)
$Extend (6)
$RECYCLE.BIN (6)
$Unalloc (1)
Documents and Settings (2)
USERS (7)
Users (4)
Windows (38)
addins (2)
AppCompat (3)
Name
S
C
O
Modified Time
Microsoft-Windows-WindowsSystemAssessmentTo
Microsoft-Windows-WindowsUpdateClient%4Oper
Microsoft-Windows-Winlogon%4Operational.evtx
Microsoft-Windows-WLAN-AutoConfig%4Operatio
Security.evtx
Setup.evtx
System.evtx
Windows Pow
Microsoft-Wir
Microsoft-Wir
[parent folder
2015-05-26 14:00:40 WES
2015-05-26 14:00:40 WES
2015-05-26 14:00:40 WES
2015-05-26 14:00:40 WES
2015-05-26 14:00:40 WES
2015-05-26 14:00:40 WES
2015-05-26 14:00:40 WES
2015-05-26 14:00:40 WES
2015-05-26 13:57:51 WES
2015-05-26 13:57:51 WES
2015-05-26 13:57:27 WES
View File in Timeline...
View Item in New Window
Open in External Viewer Ctrl+E
Extract File(s)


Visualizador de eventos
Ficheiro Ação Ver Ajuda
Visualizador de eventos (Local)
Vistas Personalizadas
Registos do Windows
Registos de Serviços e Aplica
Registos Guardados
System
Subscrições
System Número de eventos: 5 523
Nível
Data e hora
Origem
ID do evento
Categoria de T
Informações 20/02/2014 18:50:45 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 18:50:28 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 18:50:12 Application-Experience 206 Nenhum
Informações 20/02/2014 18:48:15 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 18:45:07 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 18:45:06 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 18:02:23 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 17:56:46 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 17:51:53 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 17:46:52 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 17:02:35 EventLog 6013 Nenhum
Informações 20/02/2014 15:47:36 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 15:43:12 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 15:41:19 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 15:35:40 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 15:32:40 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 15:29:39 Service Control Manag... 7036 Nenhum
Informações 20/02/2014 15:29:39 Service Control Manag... 7036 Nenhum
Evento 6013, EventLog
Geral
Detalhes
O tempo de utilização do sistema é de 9634 segundos.
Nome do Registo: Sistema
Origem: EventLog
Registado: 20/02/2014 17:02:35