Report

Title: Forensic Acquisition of Hard Drive in E01 Evidence Format

Riphah International University Islamabad

Name	Sap Id
Saad Naveed	43973
Muhammad Masab Qayyum	46472
Course	Digital Forensics
Course Instructor	Mr. Humayun Raza
Submission Date	12th May 2025

Contents

Introduction

This project is about learning how to investigate digital evidence using forensics. The main goal is to find changes made to a computer system after some activity has happened. For this, we used a virtual machine (VM) with **Windows 11** installed on it through **VMware Workstation**.

First, we took a **clean disk image** (without any changes or activity) using **FTK Imager**. After that, we did some actions on the system that could be suspicious, like opening files, changing settings, or installing tools. Then we took another **disk image after those activities**.

To analyze both images, we used a tool called **Autopsy** on the host system. This helped us compare the clean and affected images and find out what was changed or added.

Objective

To learn how to take a disk image of a Windows 11 virtual machine using **FTK Imager**.

To do some basic or suspicious activities inside the VM to simulate a real-world scenario.

To take another disk image **after the activities**.

To compare both images and find differences using **Autopsy**.

To identify changes such as:

- New or deleted files,
- Modified system settings,
- User activity (like opened files),
- Any signs of malware or persistence methods.

Tools used

FTK imager for disk dump.

Autopsy for analysis

Figure 1 Showing not connect internet

Start 1 dump.

I open FTK imager.

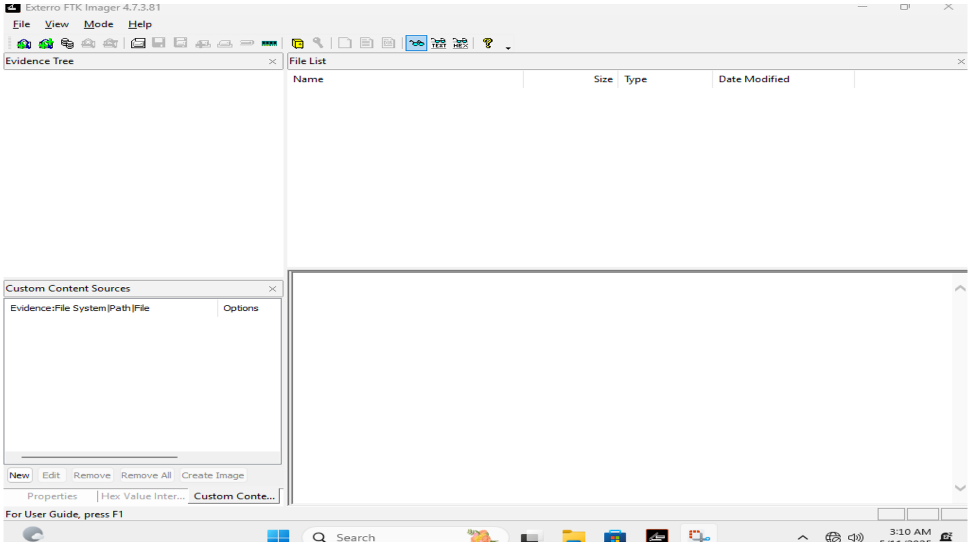


Figure 2 Open FTK imager

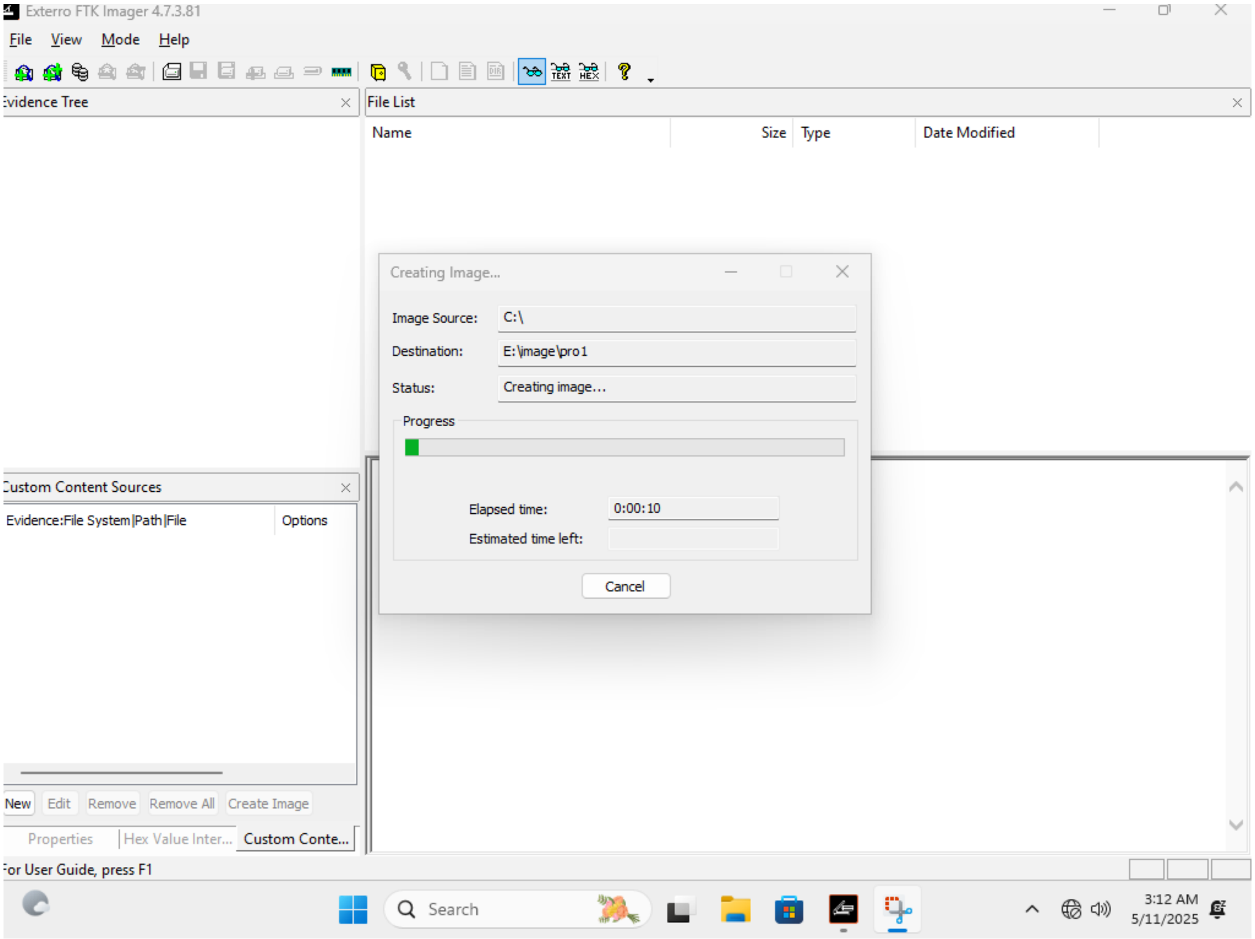


Image Source: C:\

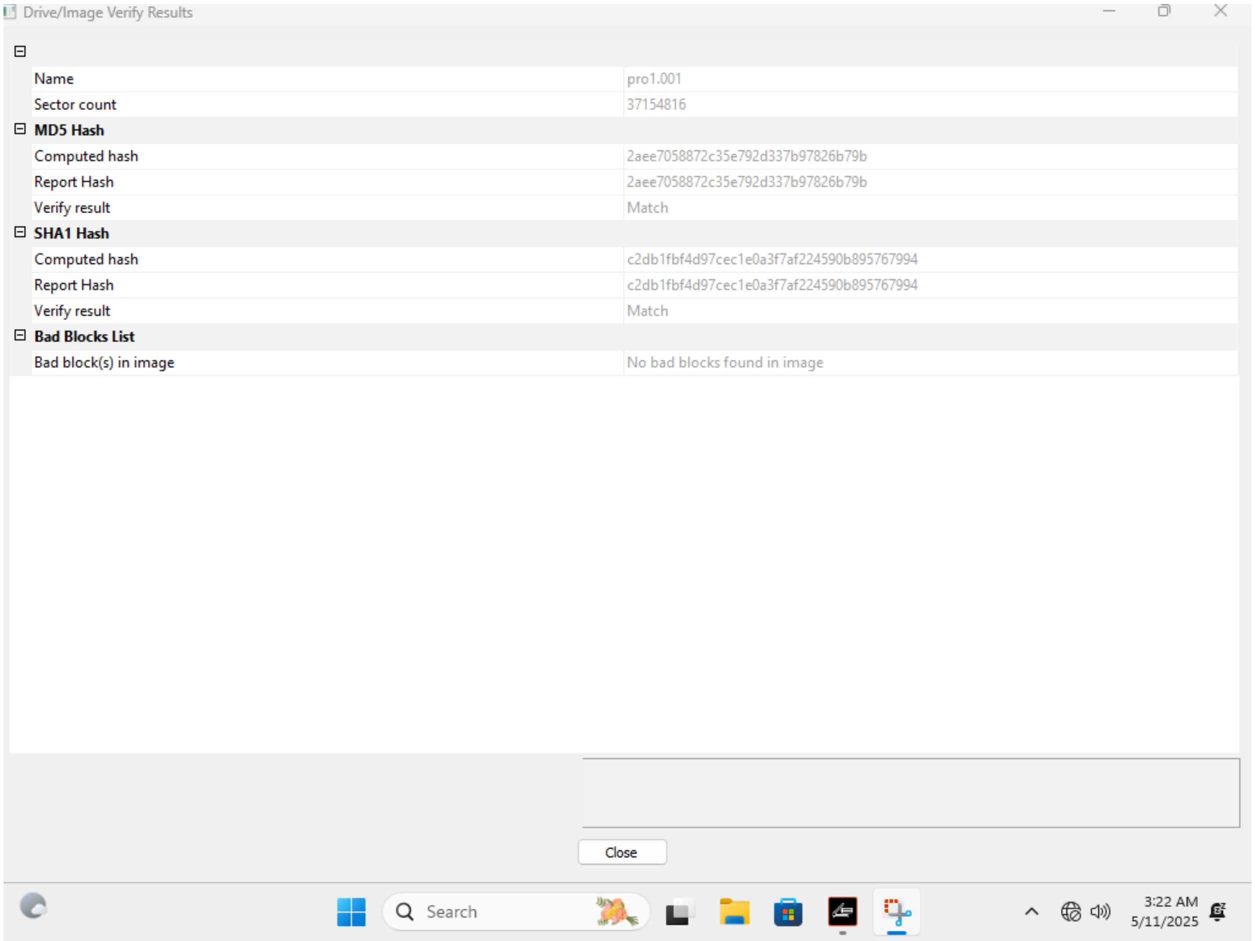
Destination: E:\image\pro1

Status: Creating image...

Elapsed time: 0:00:10

Estimated time left:

Figure 3 Taking dump

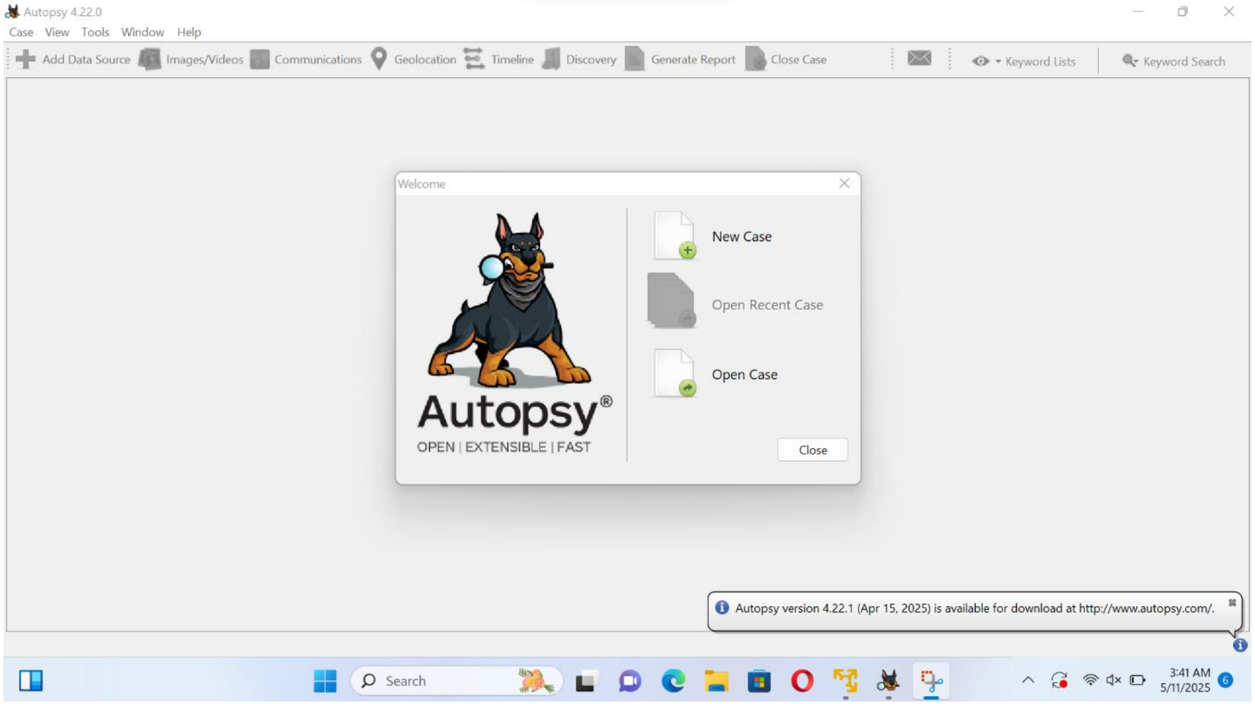


Drive/Image Verify Results

⊟	
Name	pro1.001
Sector count	37154816
⊟ **MD5 Hash**	
Computed hash	2aee7058872c35e792d337b97826b79b
Report Hash	2aee7058872c35e792d337b97826b79b
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	c2db1fbf4d97cec1e0a3f7af224590b895767994
Report Hash	c2db1fbf4d97cec1e0a3f7af224590b895767994
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

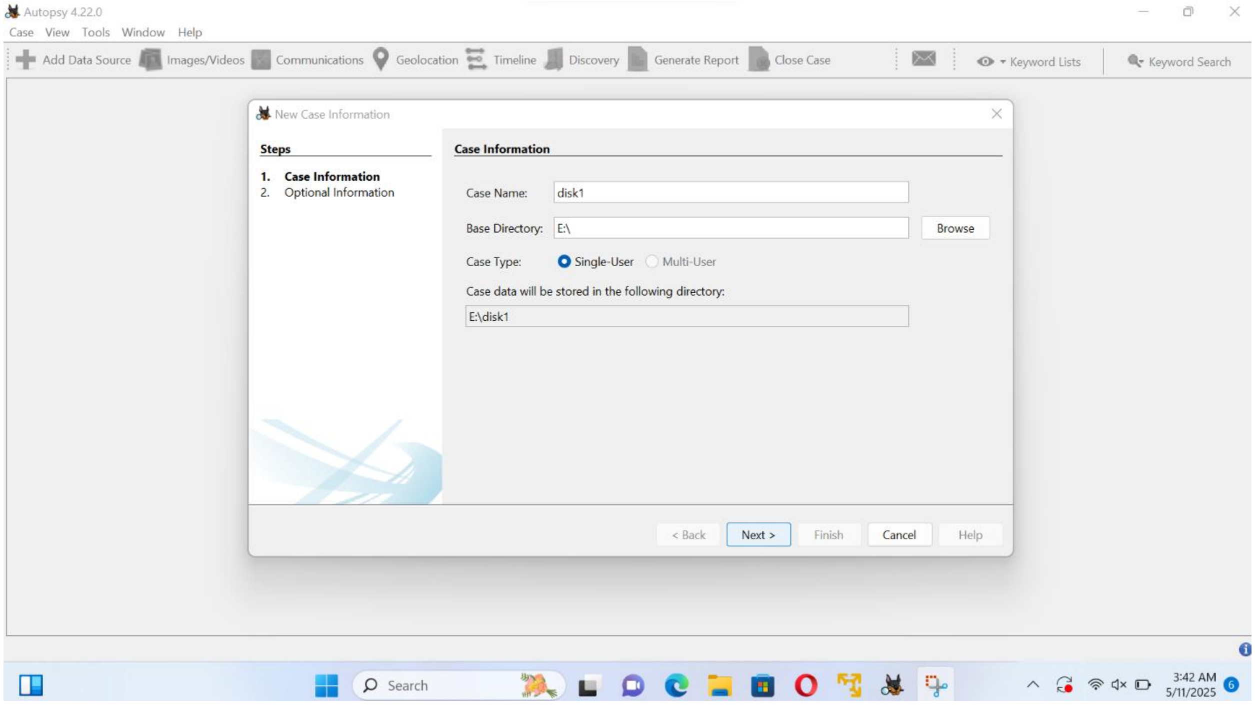
Figure 4 Dump summary

After the dump complete I open autopsy for image analysis.



Autopsy version 4.22.1 (Apr 15, 2025) is available for download at http://www.autopsy.com/.

Figure 5 Open Autopsy



Case Name: disk1

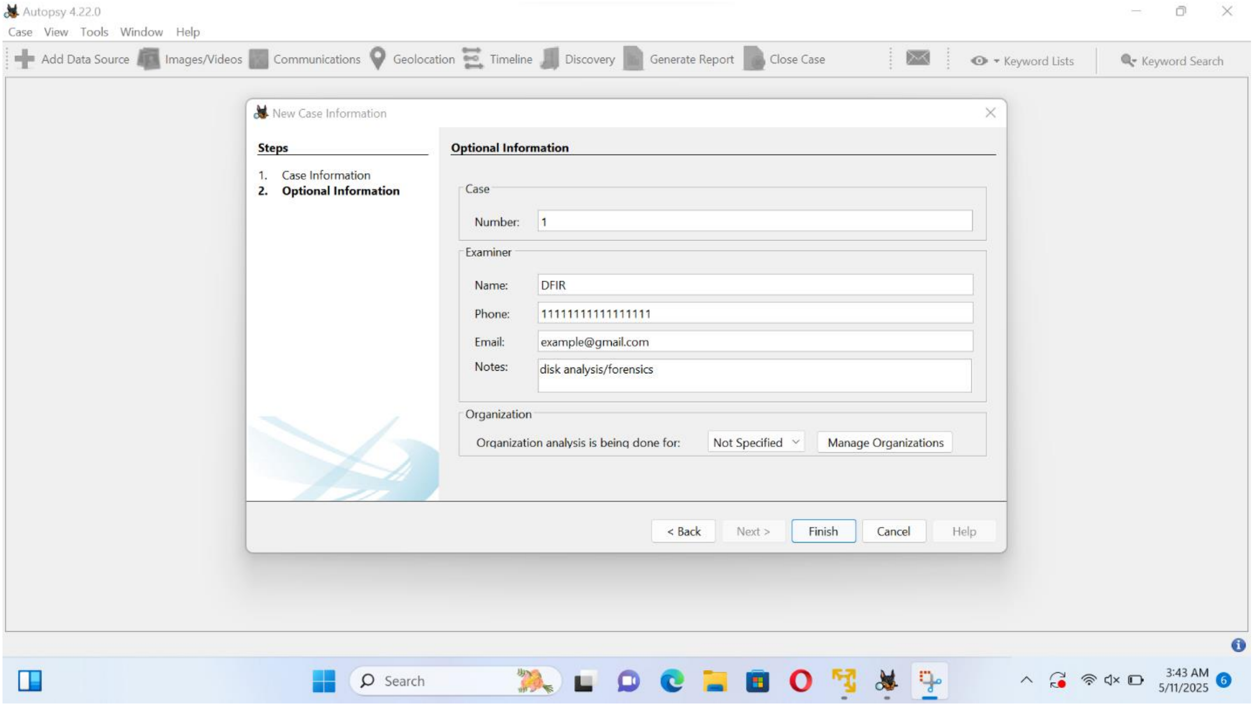
Base Directory: E:\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

E:\disk1

Figure 6 Set case name



Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 1

Examiner

Name: DFIR

Phone: 1111111111111111

Email: example@gmail.com

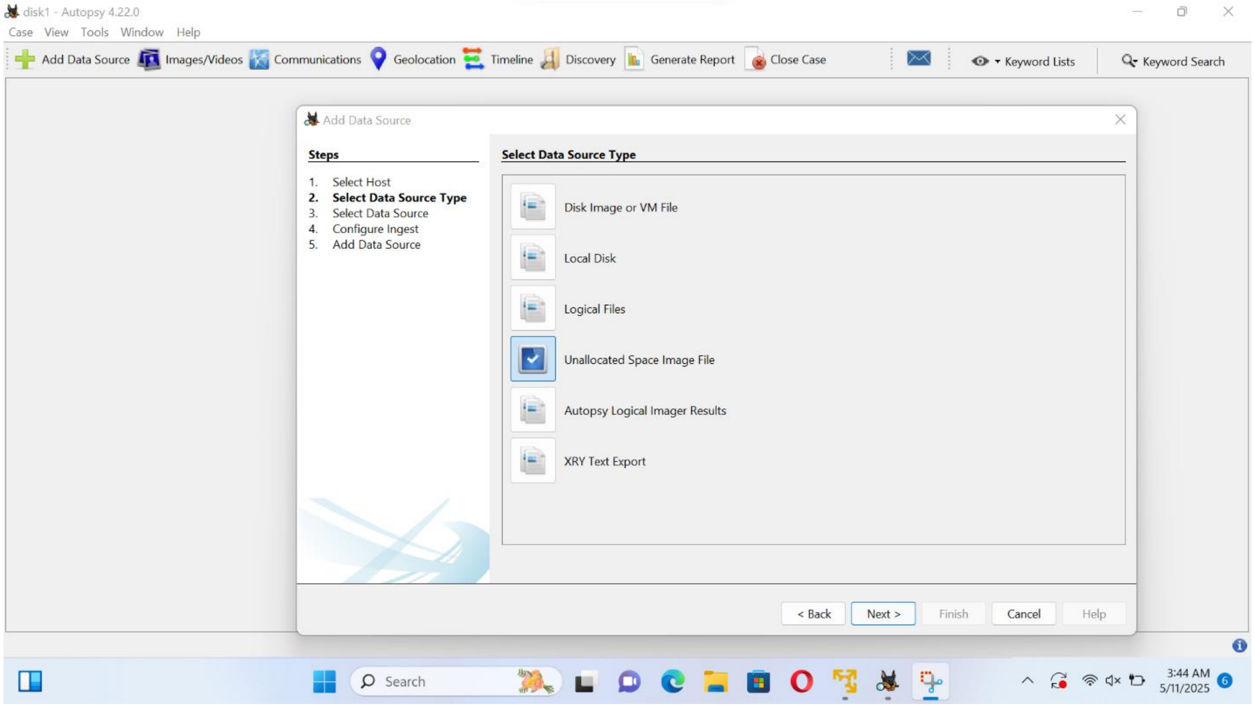
Notes: disk analysis/forensics

Organization

Organization analysis is being done for: Not Specified

Manage Organizations

Figure 7 Add random information



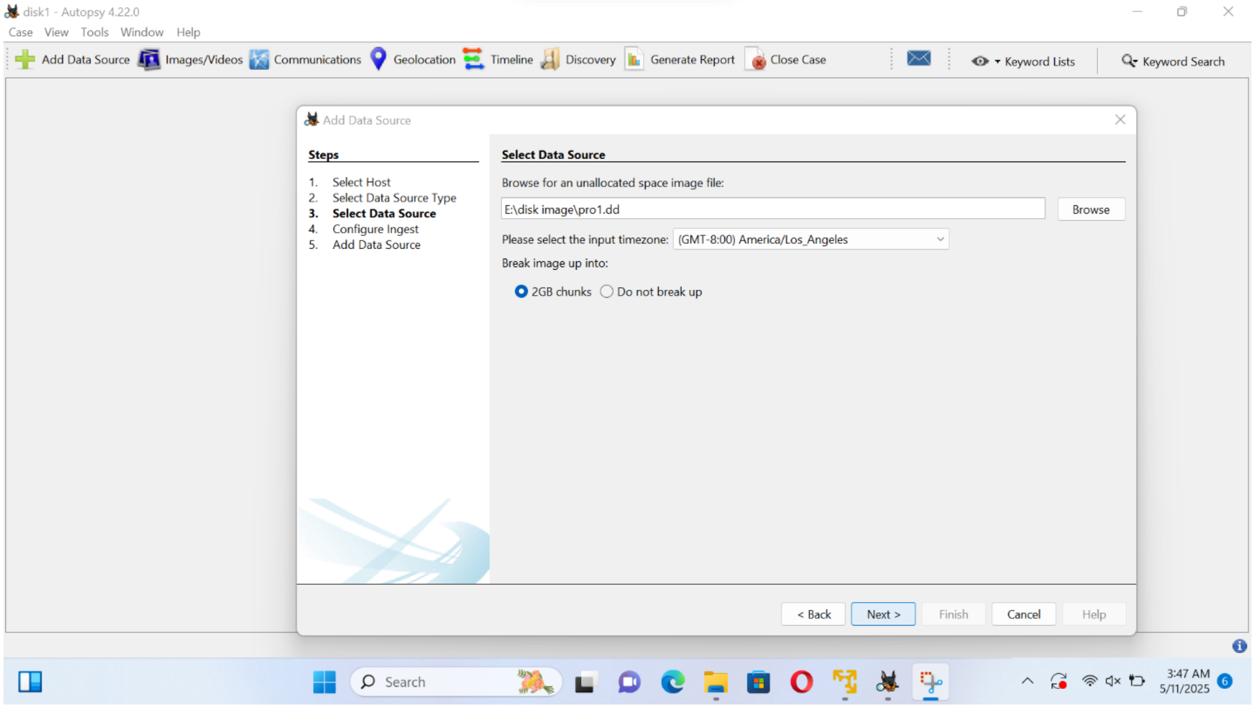
Steps

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
- Logical Files
- ☑ Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

Figure 8 Select image file icon



Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

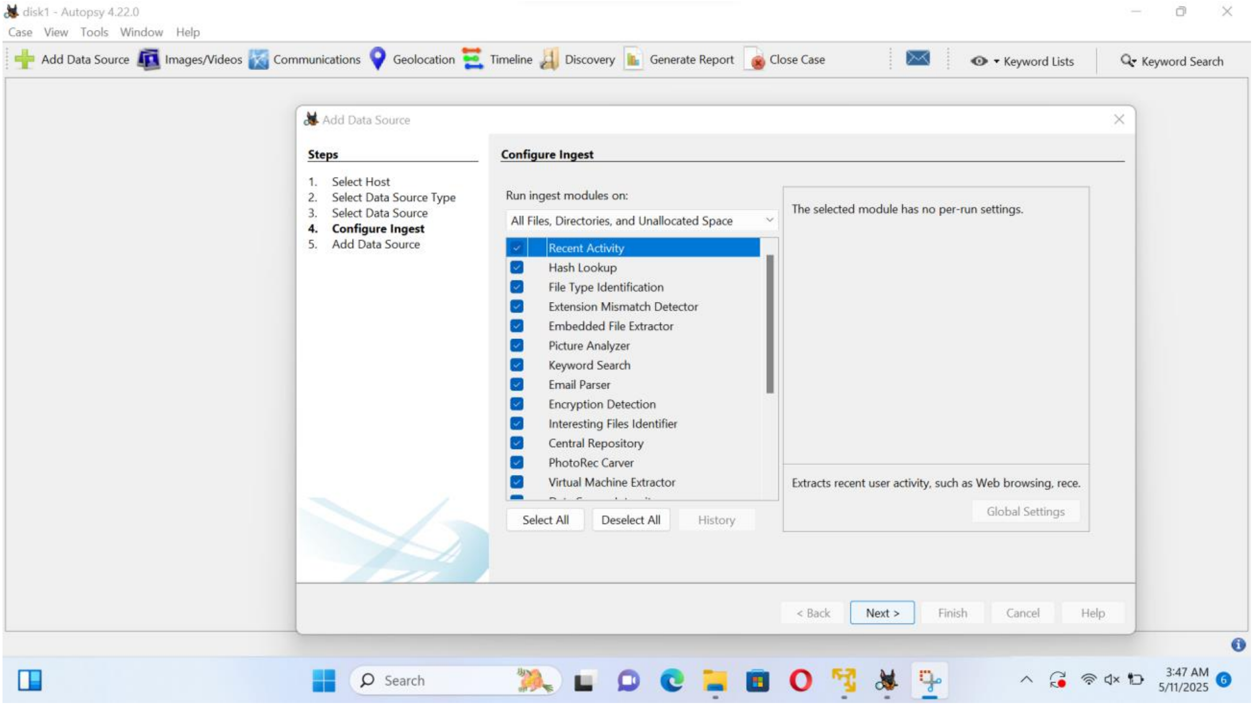
Browse for an unallocated space image file: E:\disk image\pro1.dd

Please select the input timezone: (GMT-8:00) America/Los_Angeles

Break image up into:

● 2GB chunks ○ Do not break up

Figure 9 Set image path



Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

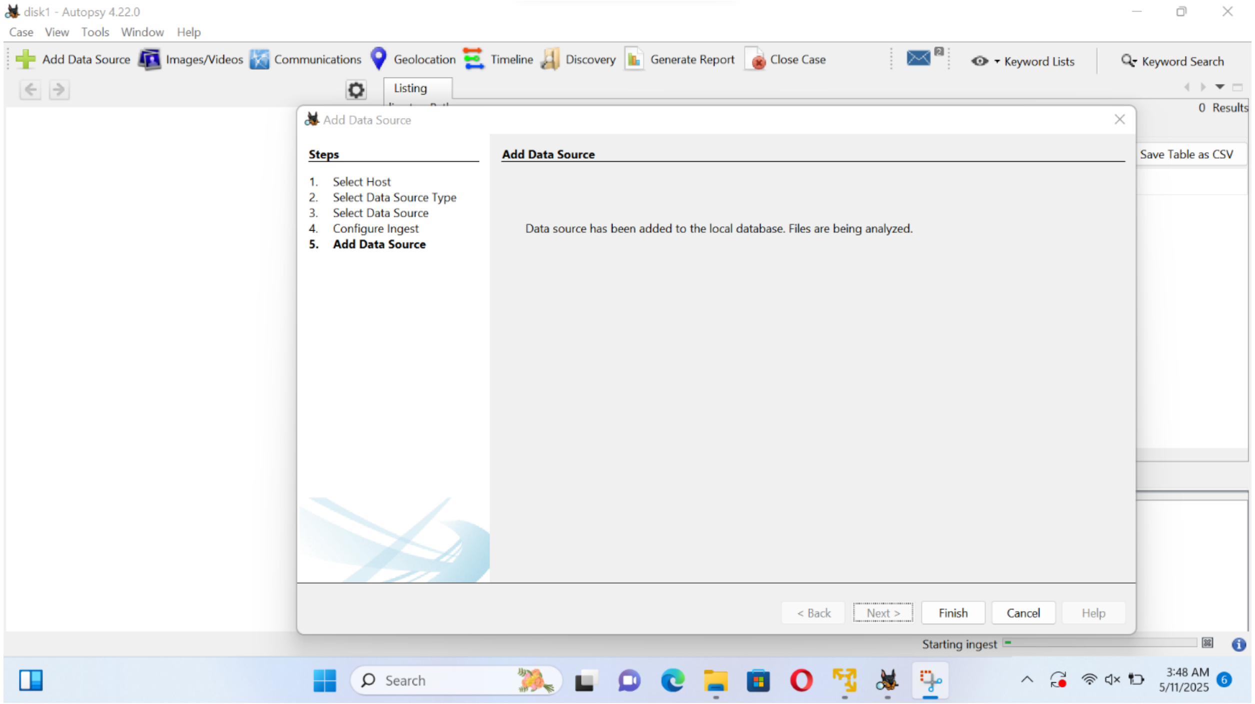
Run ingest modules on: All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, rece.

Figure 10 Setup configuration



Add Data Source

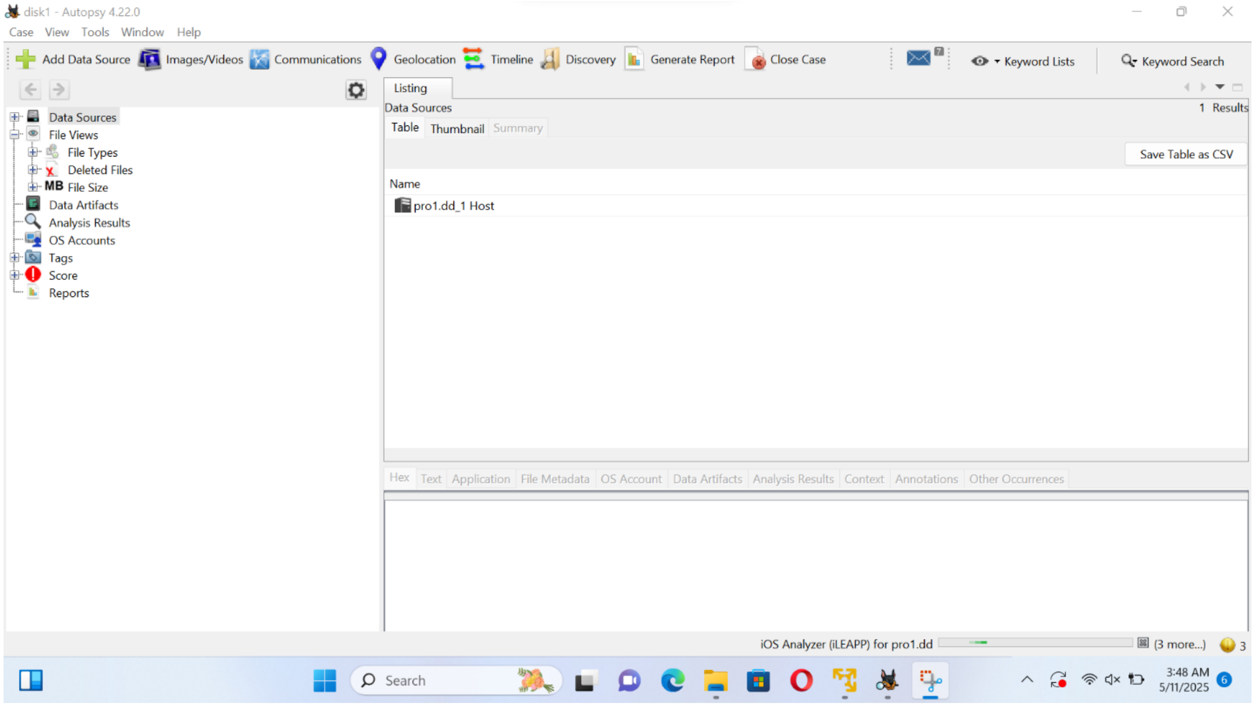
Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

Figure 11 Add data source



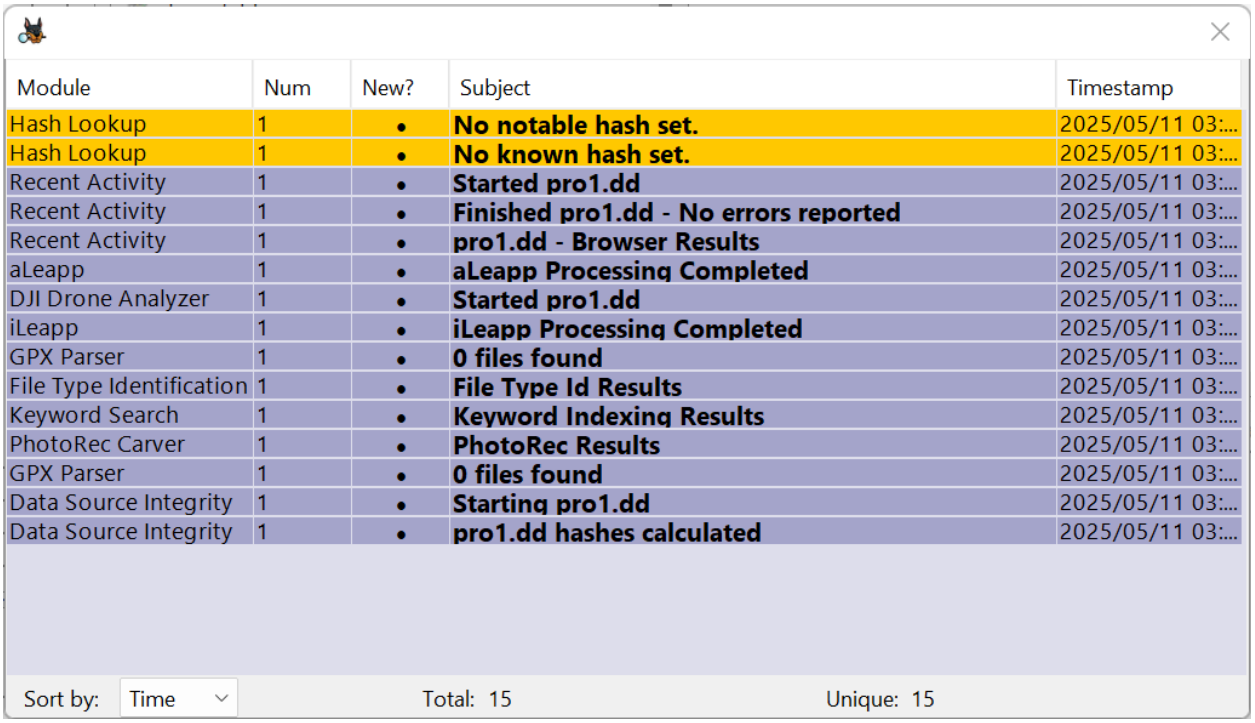
- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
- Analysis Results
- OS Accounts
- Tags
- Score
- Reports

Data Sources

Name
pro1.dd_1 Host

iOS Analyzer (iLEAPP) for pro1.dd

Figure 12 Start process



Module	Num	New?	Subject	Timestamp
Hash Lookup	1	•	**No notable hash set.**	2025/05/11 03:...
Hash Lookup	1	•	**No known hash set.**	2025/05/11 03:...
Recent Activity	1	•	**Started pro1.dd**	2025/05/11 03:...
Recent Activity	1	•	**Finished pro1.dd - No errors reported**	2025/05/11 03:...
Recent Activity	1	•	**pro1.dd - Browser Results**	2025/05/11 03:...
aLeapp	1	•	**aLeapp Processing Completed**	2025/05/11 03:...
DJI Drone Analyzer	1	•	**Started pro1.dd**	2025/05/11 03:...
iLeapp	1	•	**iLeapp Processing Completed**	2025/05/11 03:...
GPX Parser	1	•	**0 files found**	2025/05/11 03:...
File Type Identification	1	•	**File Type Id Results**	2025/05/11 03:...
Keyword Search	1	•	**Keyword Indexing Results**	2025/05/11 03:...
PhotoRec Carver	1	•	**PhotoRec Results**	2025/05/11 03:...
GPX Parser	1	•	**0 files found**	2025/05/11 03:...
Data Source Integrity	1	•	**Starting pro1.dd**	2025/05/11 03:...
Data Source Integrity	1	•	**pro1.dd hashes calculated**	2025/05/11 03:...

Sort by: Time   Total: 15   Unique: 15

Figure 13 This modules ran

Hash Lookup (Yellow Rows)

- **No notable hash set:** The system did not have a list of bad files (like malware), so it couldn't check for them.
- **No known hash set:** The system also didn't have a list of safe files, so it couldn't check which files are safe.

Recent Activity

- **Started pro1.dd:** The tool started working on the disk image file named pro1.dd.
- **Finished pro1.dd - No errors reported:** The tool finished the work with no errors.

aLeapp & iLeapp (Mobile Tools)

- **aLeapp / iLeapp Processing Completed:** These tools looked at mobile data (Android and iPhone) and finished their work.

DJI Drone Analyzer

- **Started pro1.dd:** This tool started checking if there was any drone data in the file.

GPX Parser

- **0 files found:** No GPS location files were found.

File Type Identification

- **File Type Id Results:** It checked what types of files (like pictures, documents) are inside the disk.

Keyword Search

- **Keyword Indexing Results:** It prepared a list of words to make it easy to search in the files.

PhotoRec Carver

- **PhotoRec Results:** It tried to recover deleted files.

Data Source Integrity

- **Starting pro1.dd / pro1.dd hashes calculated:** It created a hash (a kind of digital fingerprint) to make sure the image is not changed or damaged.

Simple Summary

- 15 tools were used.
- Everything worked fine.

Start 2 dump of disk.

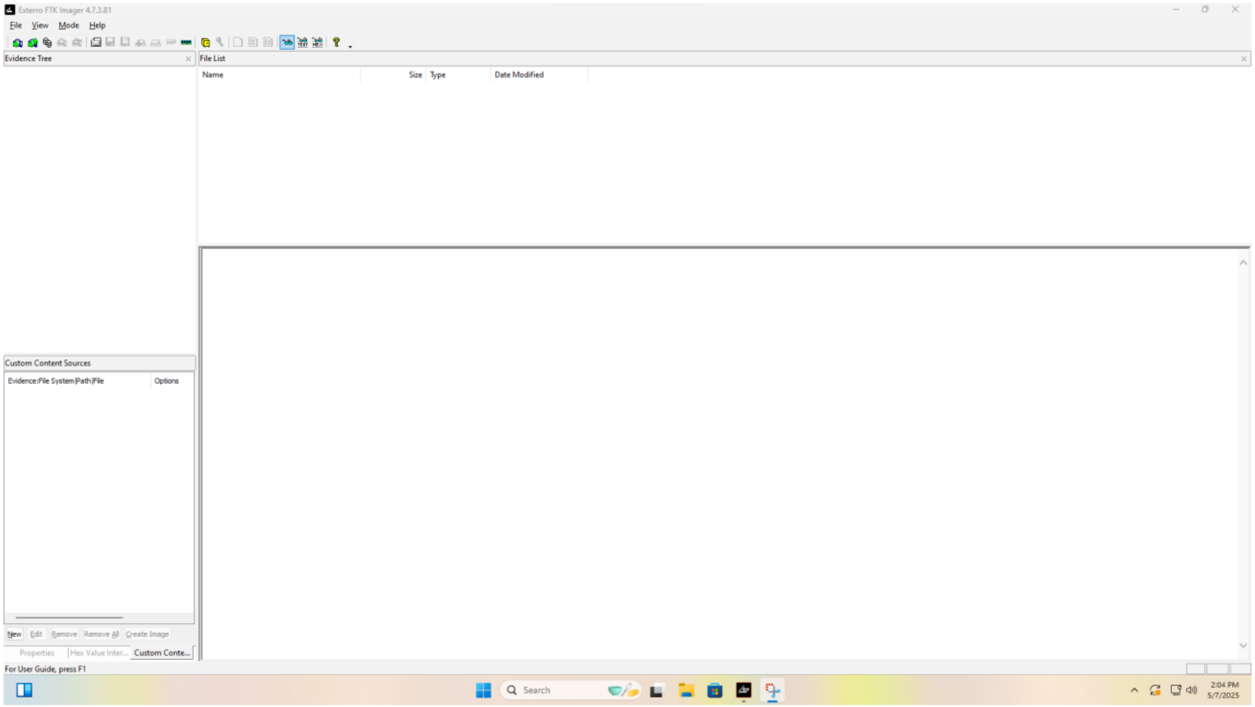


Figure 14 open FTK

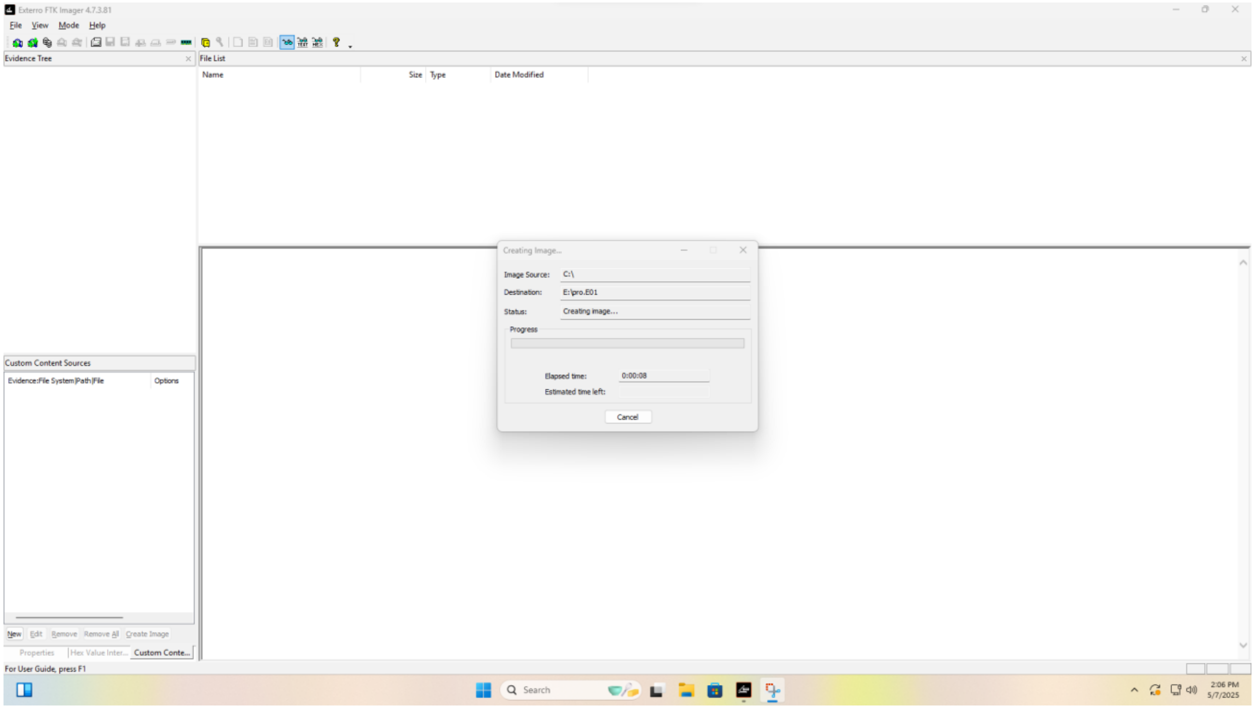
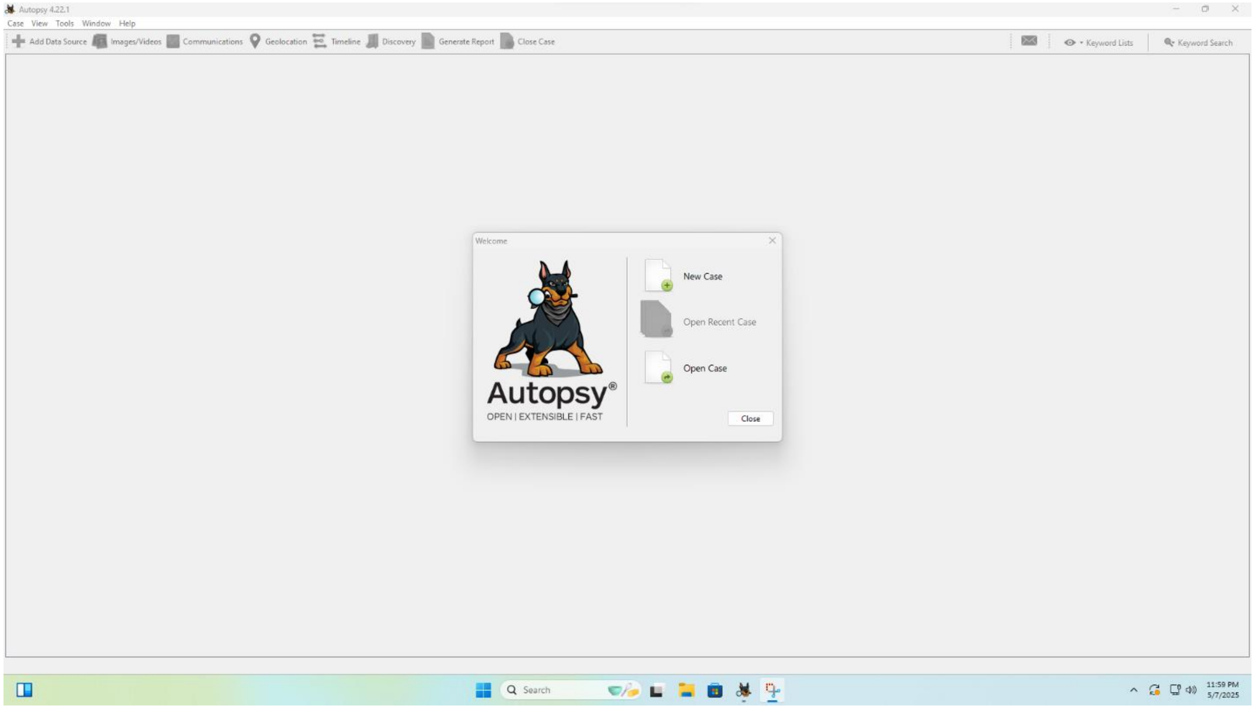


Image Source: C:\
Destination: E:\pro.E01
Status: Creating image...
Elapsed time: 0:00:08
Estimated time left:

Figure 15 Strating dump

After the dump complete and I used Autopsy for analysis dump.

I run Autopsy.



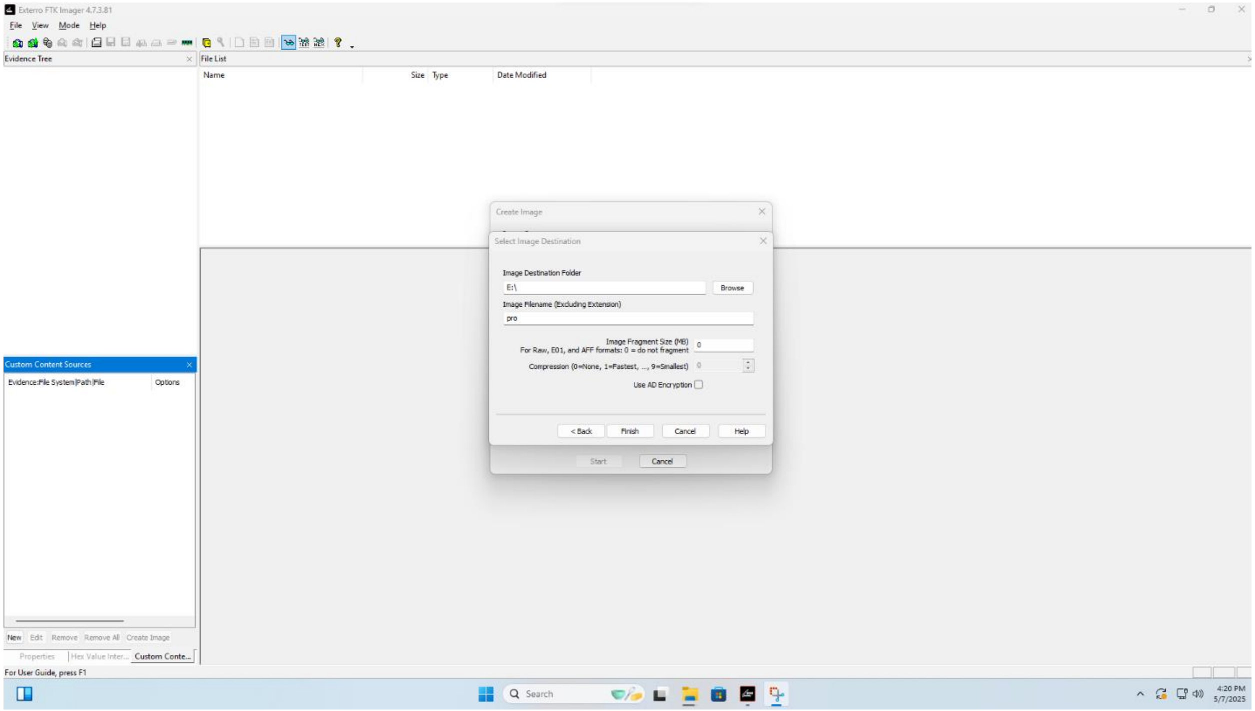


Image Destination Folder: E:\

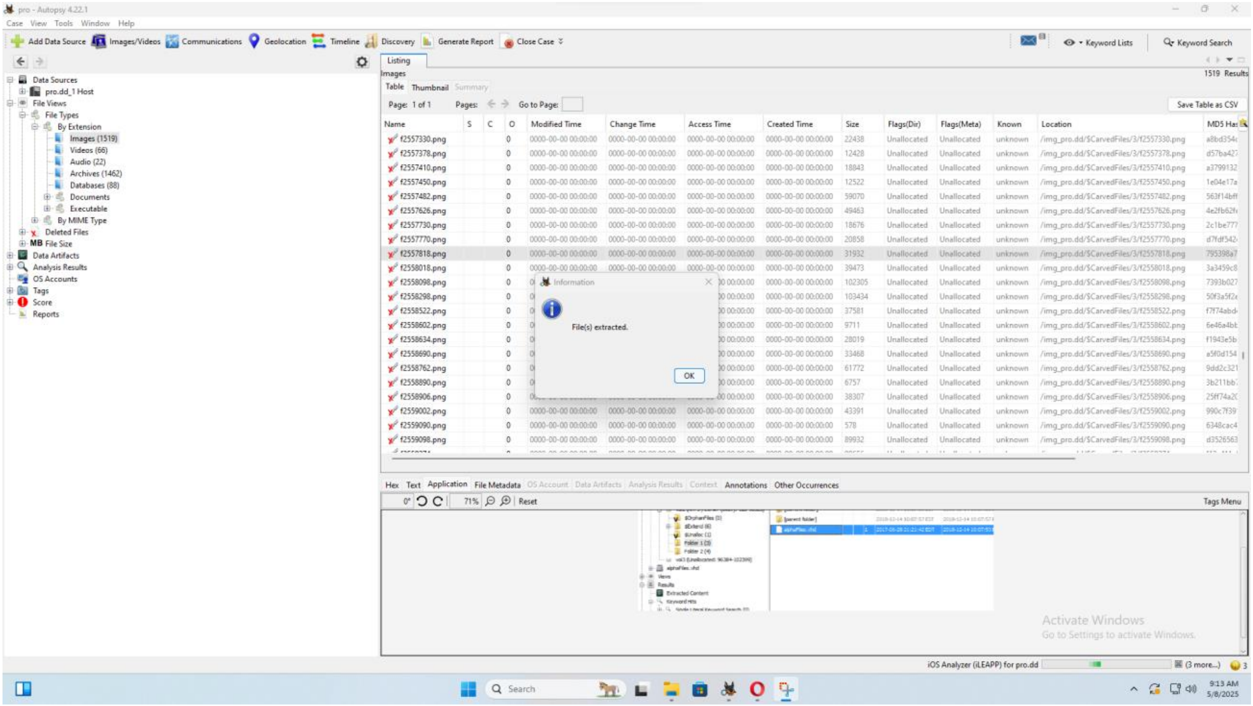
Image Filename (Excluding Extension): pro

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption ☐

When I successful load dump file.



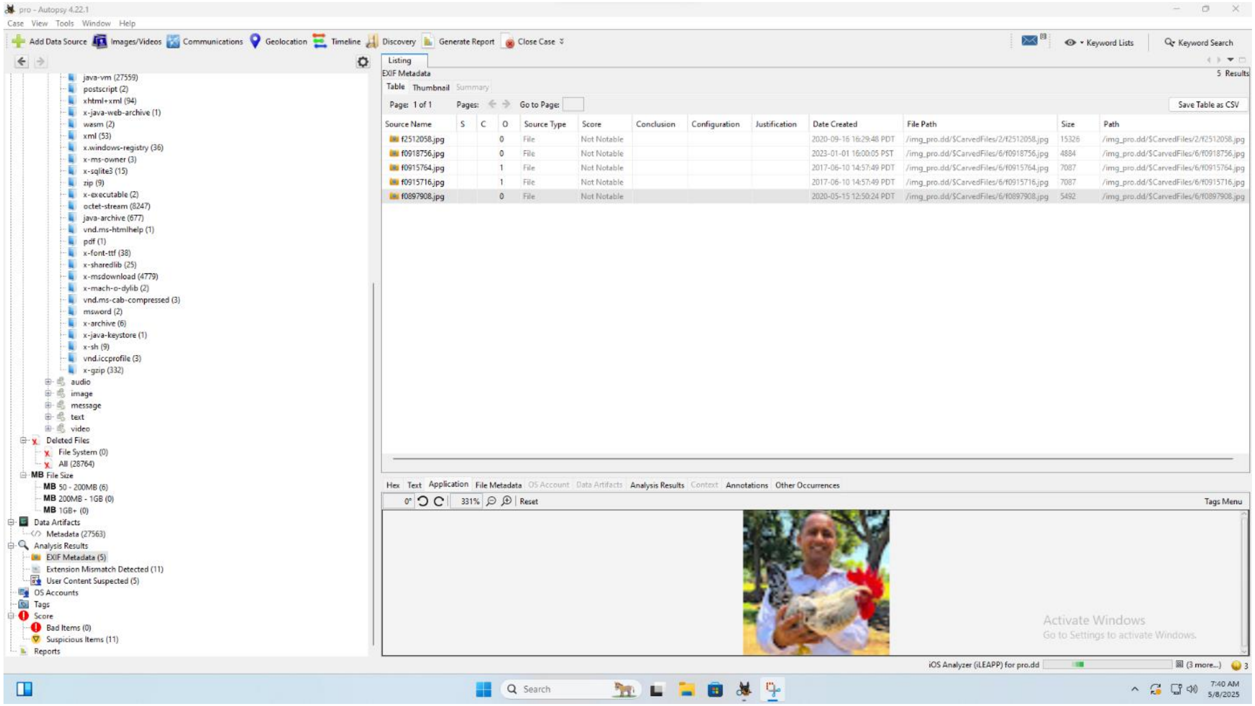
Information

File(s) extracted.

OK

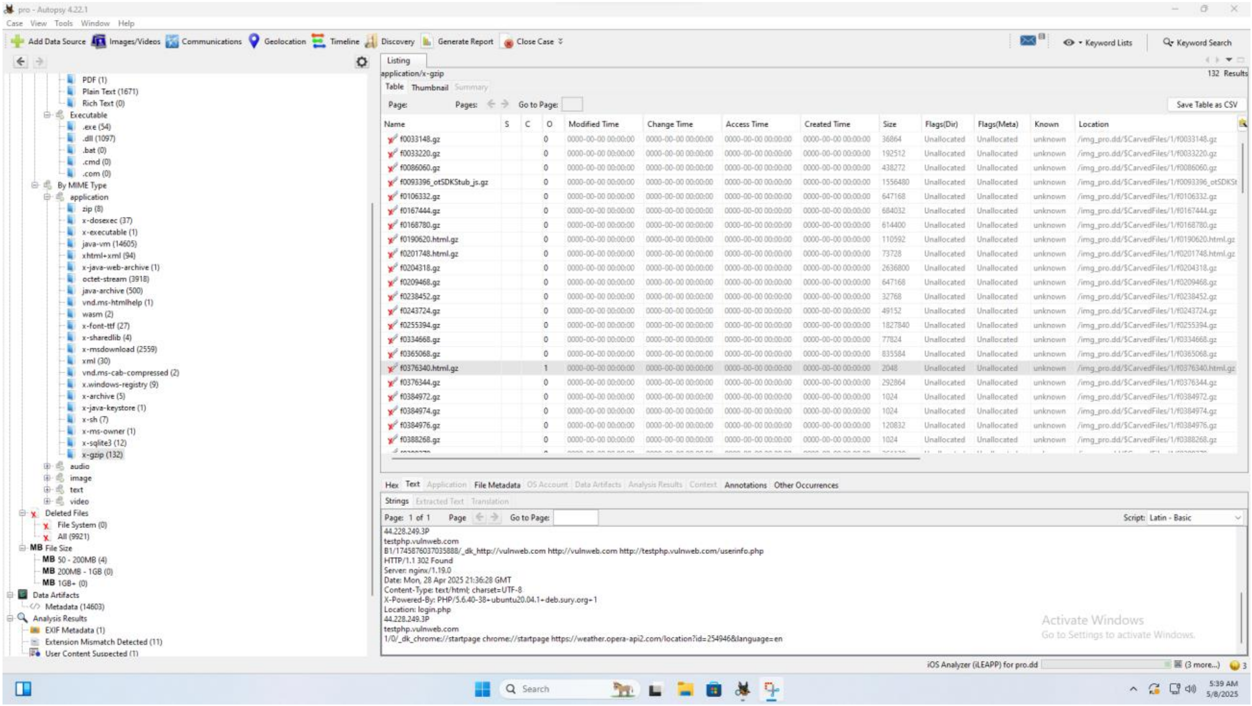
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Has
f2557330.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22438	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557330.png	a8bd354
f2557378.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12428	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557378.png	d57ba42
f2557410.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18843	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557410.png	a379913
f2557450.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12522	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557450.png	1e04e17a
f2557482.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	59070	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557482.png	563f14bff
f2557626.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49463	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557626.png	4e2fb62f
f2557730.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18676	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557730.png	2c1be77
f2557770.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20858	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557770.png	d7fdf542
f2557818.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	31932	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2557818.png	795398a7
f2558018.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	39473	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558018.png	3a3459c8
f2558098.png			0	0		00:00:00	0000-00-00 00:00:00	102305	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558098.png	7393b027
f2558298.png			0	0		00:00:00	0000-00-00 00:00:00	103434	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558298.png	50f3a5f2
f2558522.png			0	0		00:00:00	0000-00-00 00:00:00	37581	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558522.png	f7f74abd
f2558602.png			0	0		00:00:00	0000-00-00 00:00:00	9711	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558602.png	6e46a4bb
f2558634.png			0	0		00:00:00	0000-00-00 00:00:00	28019	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558634.png	f1943e5b
f2558690.png			0	0		00:00:00	0000-00-00 00:00:00	33468	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558690.png	a5f0d154
f2558762.png			0	0		00:00:00	0000-00-00 00:00:00	61772	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558762.png	9dd2c321
f2558890.png			0	0		00:00:00	0000-00-00 00:00:00	6757	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558890.png	3b211bb
f2558906.png			0	0		00:00:00	0000-00-00 00:00:00	38307	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2558906.png	25ff74a2
f2559002.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	43391	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2559002.png	990c7f39
f2559090.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	578	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2559090.png	6348cac4
f2559098.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	89932	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f2559098.png	d3526563

Figure 16 Show files



Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	File Path	Size	Path
f2512058.jpg			0	File	Not Notable				2020-09-16 16:29:48 PDT	/img_pro.dd/$CarvedFiles/2/f2512058.jpg	15326	/img_pro.dd/$CarvedFiles/2/f2512058.jpg
f0918756.jpg			0	File	Not Notable				2023-01-01 16:00:05 PST	/img_pro.dd/$CarvedFiles/6/f0918756.jpg	4884	/img_pro.dd/$CarvedFiles/6/f0918756.jpg
f0915764.jpg			1	File	Not Notable				2017-06-10 14:57:49 PDT	/img_pro.dd/$CarvedFiles/6/f0915764.jpg	7087	/img_pro.dd/$CarvedFiles/6/f0915764.jpg
f0915716.jpg			1	File	Not Notable				2017-06-10 14:57:49 PDT	/img_pro.dd/$CarvedFiles/6/f0915716.jpg	7087	/img_pro.dd/$CarvedFiles/6/f0915716.jpg
f0897908.jpg			0	File	Not Notable				2020-05-15 12:50:24 PDT	/img_pro.dd/$CarvedFiles/6/f0897908.jpg	5492	/img_pro.dd/$CarvedFiles/6/f0897908.jpg

Figure 17 found pic



application/x-gzip

132 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0033148.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	36864	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0033148.gz
f0033220.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	192512	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0033220.gz
f0086060.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	438272	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0086060.gz
f0093396_otSDKStub_js.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1556480	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0093396_otSDKSt
f0106332.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	647168	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0106332.gz
f0167444.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	684032	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0167444.gz
f0168780.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	614400	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0168780.gz
f0190620.html.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	110592	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0190620.html.gz
f0201748.html.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	73728	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0201748.html.gz
f0204318.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2636800	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0204318.gz
f0209468.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	647168	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0209468.gz
f0238452.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32768	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0238452.gz
f0243724.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49152	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0243724.gz
f0255394.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1827840	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0255394.gz
f0334668.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	77824	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0334668.gz
f0365068.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	835584	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0365068.gz
f0376340.html.gz			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0376340.html.gz
f0376344.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	292864	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0376344.gz
f0384972.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1024	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0384972.gz
f0384974.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1024	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0384974.gz
f0384976.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	120832	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0384976.gz
f0388268.gz			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1024	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0388268.gz

```
44.228.249.3P
testphp.vulnweb.com
B1/1745876037035888/_dk_http://vulnweb.com http://vulnweb.com http://testphp.vulnweb.com/userinfo.php
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Mon, 28 Apr 2025 21:36:28 GMT
Content-Type: text/html; charset=UTF-8
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
44.228.249.3P
testphp.vulnweb.com
1/0/_dk_chrome://startpage chrome://startpage https://weather.opera-api2.com/location?id=254946&language=en
```

Analysis of Gzip Files in Autopsy

File Type and Context:

MIME Type: application/x-gzip

Total Files Identified: 132 .gz files

Location: /img_prod.dd/SCARvedFiles/

Status: Most files are marked as **Unallocated**, indicating they were likely **deleted** and later recovered during forensic carving.

Notable Files:

f0201438.html.gz

f0376340.html.gz
These may contain web content such as scripts or malicious payloads.

Extracted Artifact Highlights:

Table 1 important artifacts

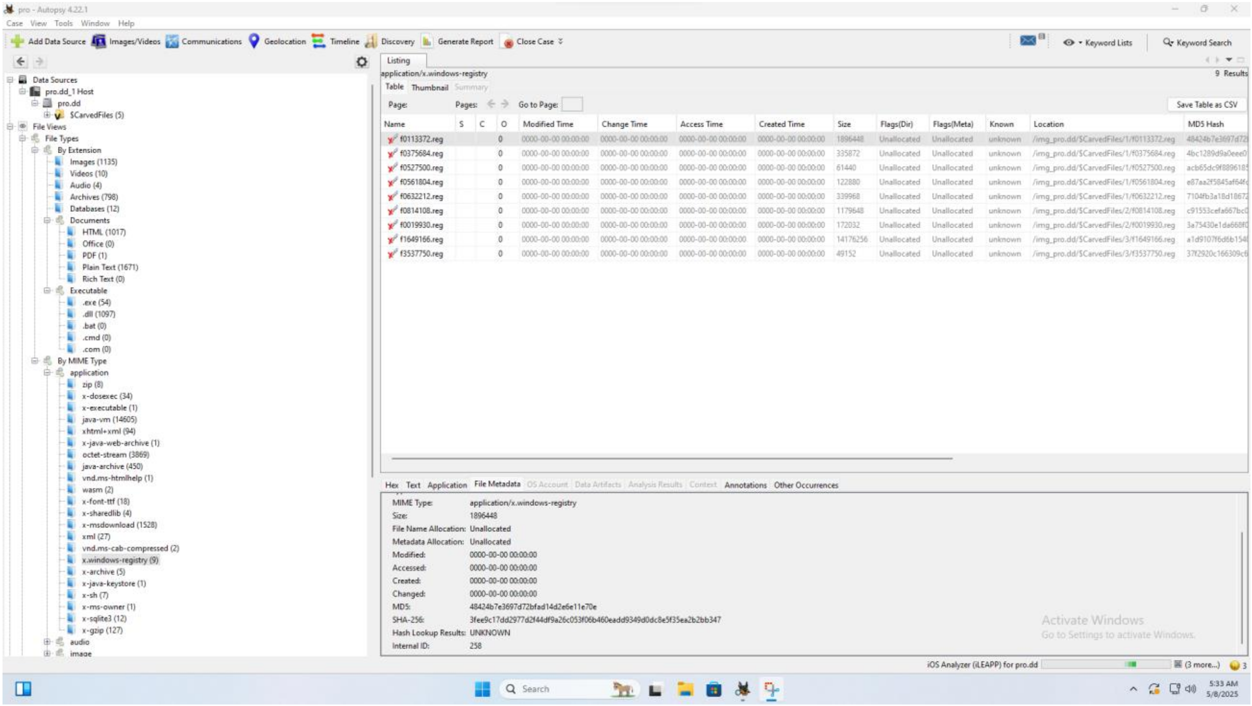
Attribute	Value
URL Identified	http://vulnweb.com/testphp.vulnweb.com/userinfo.php
IP Address	142.228.249.39
User-Agent	Opera on Linux (chrome/startpage chrome/)
HTTP Response	HTTP/1.1 302 Found (Redirection detected)
Server	nginx/1.19.0
Powered By	PHP 5.6.40

Interpretation:

The URL and server headers indicate interaction with a known vulnerable web application possibly used for exploitation, testing, or red team activities.

IP 142.228.249.39 may represent a source or attacker system.

Presence of .html.gz and PHP reference (userinfo.php) points to potential web shell, data exfiltration, or injection script activity.



application/x.windows-registry

9 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
f0113372.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1896448	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0113372.reg	48424b7e3697d72
f0375684.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	335872	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0375684.reg	4bc1289d9a0eee0
f0527500.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61440	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0527500.reg	acb65dc9f889618
f0561804.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	122880	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0561804.reg	e87aa2f5845af64f
f0632212.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	339968	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/1/f0632212.reg	7104fb3a18d1867
f0814108.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1179648	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/2/f0814108.reg	c91553cefa667bc
f0019930.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	172032	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/2/f0019930.reg	3a75430e1da668f
f1649166.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14176256	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f1649166.reg	a1d9107f6d6b154
f3537750.reg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49152	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/3/f3537750.reg	37f2920c166309c

MIME Type:	application/x.windows-registry
Size:	1896448
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	48424b7e3697d72bfad14d2e6e11e70e
SHA-256:	3fee9c17dd2977d2f44df9a26c053f06b460eadd9349d0dc8e5f35ea2b2bb347
Hash Lookup Results:	UNKNOWN
Internal ID:	258

Figure 18

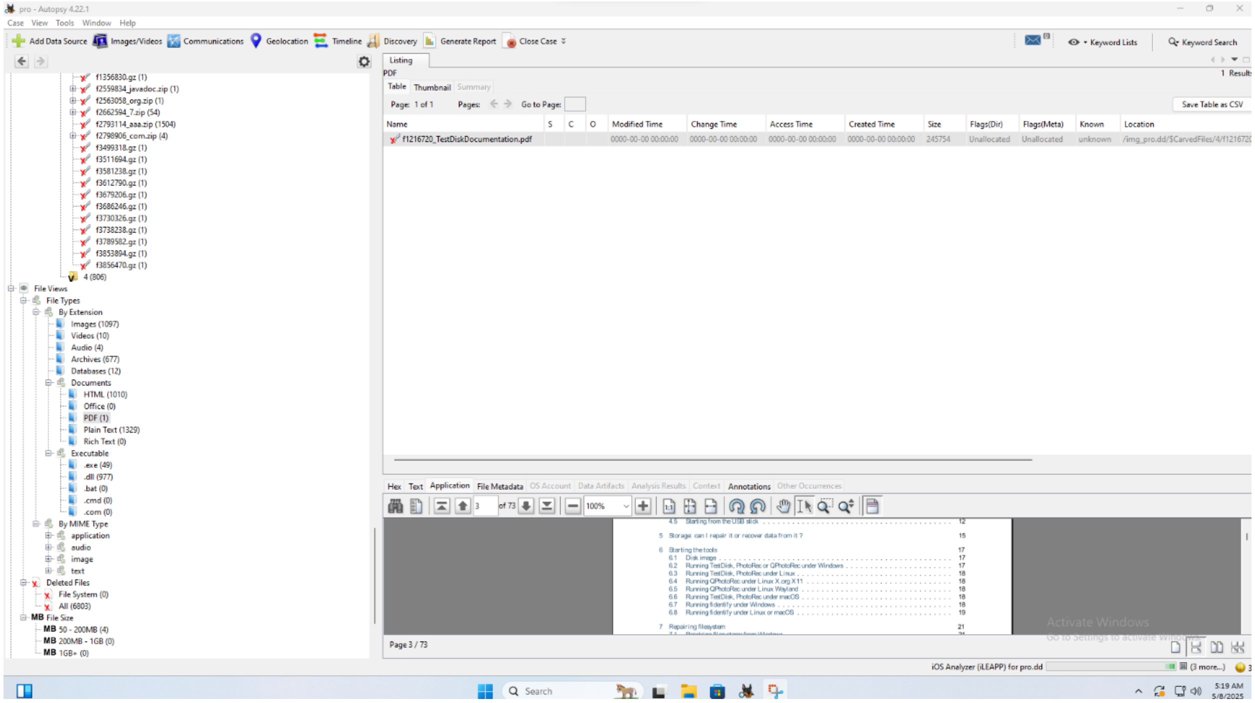
File Type and Context:

- MIME Type: application/x.windows-registry
- Total Files Identified: 9 registry export files (.reg)
- Location: /img_prod.dd/SCARvedFiles/
- Status: All files marked Unallocated, suggesting they were deleted and recovered from unallocated disk space.

Table 2

File Name	Size (Bytes)	Location	MD5 Hash
f0113372.reg	1,896,448	/img_prod.dd/SCARvedFiles/1/f0113372.reg	4842ab7c697f27fbad14da2e6e117e0e
f0375864.reg	338,772	/img_prod.dd/SCARvedFiles/1/f0375864.reg	acb12839dbeee8cf...
f0628124.reg	1,228,880	/img_prod.dd/SCARvedFiles/1/f0628124.reg	a7e8a25a188...

f0814102.reg	1,170,624	/img_prod.dd/SCARvedFiles/2/f0814102.reg	43e5a1646d6...
f0191030.reg	772,032	/img_prod.dd/SCARvedFiles/2/f0191030.reg	91c3d5ba466...



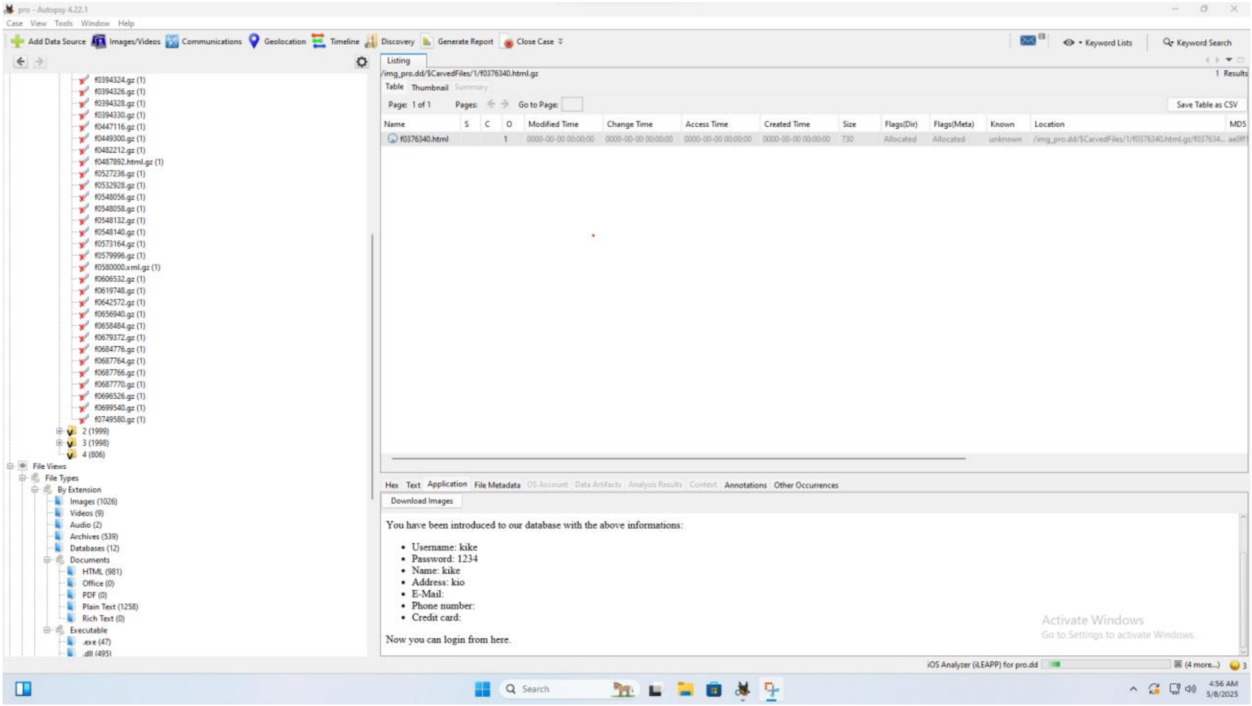
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f1216720_TestDiskDocumentation.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	245754	Unallocated	Unallocated	unknown	/img_pro.dd/$CarvedFiles/4/f121672

```
    4.5   Starting from the USB stick . . . . . . . . . . . . . . . . . . . . . . .   12
5   Storage: can I repair it or recover data from it ?                            15
6   Starting the tools                                                            17
    6.1   Disk image . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .   17
    6.2   Running TestDisk, PhotoRec or QPhotoRec under Windows . . . . . . . . .   17
    6.3   Running TestDisk, PhotoRec under Linux . . . . . . . . . . . . . . . . .   18
    6.4   Running QPhotoRec under Linux X.org X11 . . . . . . . . . . . . . . . .   18
    6.5   Running QPhotoRec under Linux Wayland . . . . . . . . . . . . . . . . .   18
    6.6   Running TestDisk, PhotoRec under macOS . . . . . . . . . . . . . . . . .   18
    6.7   Running fidentify under Windows . . . . . . . . . . . . . . . . . . . .   18
    6.8   Running fidentify under Linux or macOS . . . . . . . . . . . . . . . . .   19
7   Repairing filesystem                                                          21
```

Figure 19

File Type and Context:

- **File Name:** f1216720_TestDiskDocumentation.pdf
- **File Type:** PDF Document
- **MIME Type:** application/pdf
- **Size:** 245,754 bytes (~240 KB)
- **Location:** /img_prod.dd/SCARvedFiles/4/f1216720_TestDiskDocumentation.pdf
- **Status: Unallocated** Indicates the file was deleted and recovered from unallocated disk space.,



/img_pro.dd/$CarvedFiles/1/f0376340.html.gz — 1 Results

Page: 1 of 1 Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5
f0376340.html			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	730	Allocated	Allocated	unknown	/img_pro.dd/$CarvedFiles/1/f0376340.html.gz/f037634...	ae0ff

You have been introduced to our database with the above informations:

- Username: kike
- Password: 1234
- Name: kike
- Address: kio
- E-Mail:
- Phone number:
- Credit card:

Now you can login from here.

Figure 20

Recovered Credential Leak

File Information:

- File Name: f0376340.html
- Parent Archive: f0376340.html.gz (Gzip-compressed file)
- Location: /img_prod.dd/SCARvedFiles/1/f0376340.html.gz/f0376340.html
- Size: 730 bytes

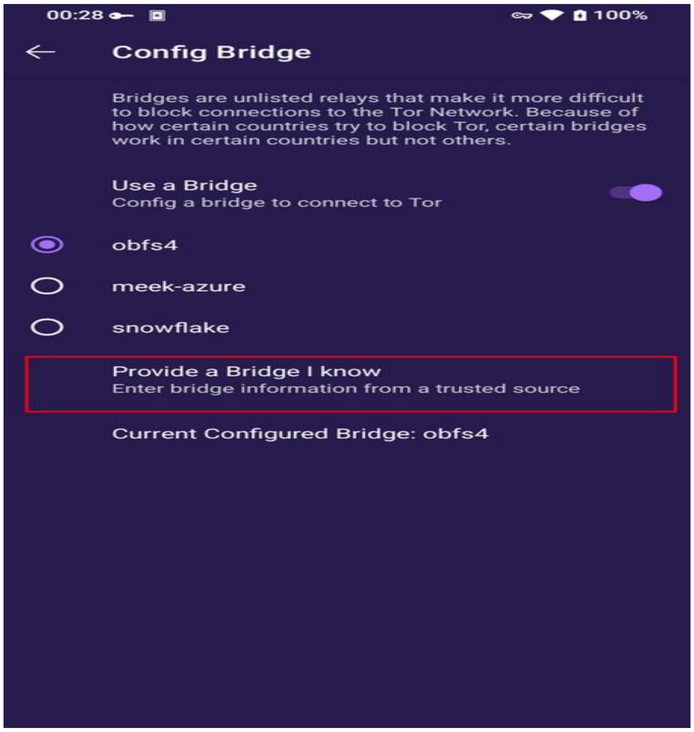
Extracted Text Content (Sensitive Data Found):

Username: kike

Password: 1234

Name: kike

Address: kio



Config Bridge

Bridges are unlisted relays that make it more difficult to block connections to the Tor Network. Because of how certain countries try to block Tor, certain bridges work in certain countries but not others.

Use a Bridge
Config a bridge to connect to Tor

● obfs4

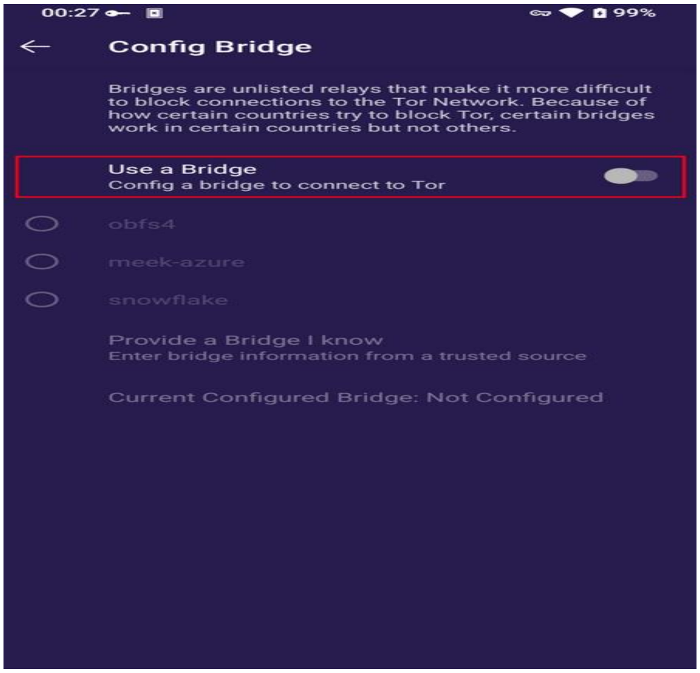
○ meek-azure

○ snowflake

Provide a Bridge I know
Enter bridge information from a trusted source

Current Configured Bridge: obfs4

Figure 21



Config Bridge

Bridges are unlisted relays that make it more difficult to block connections to the Tor Network. Because of how certain countries try to block Tor, certain bridges work in certain countries but not others.

Use a Bridge
Config a bridge to connect to Tor

○ obfs4

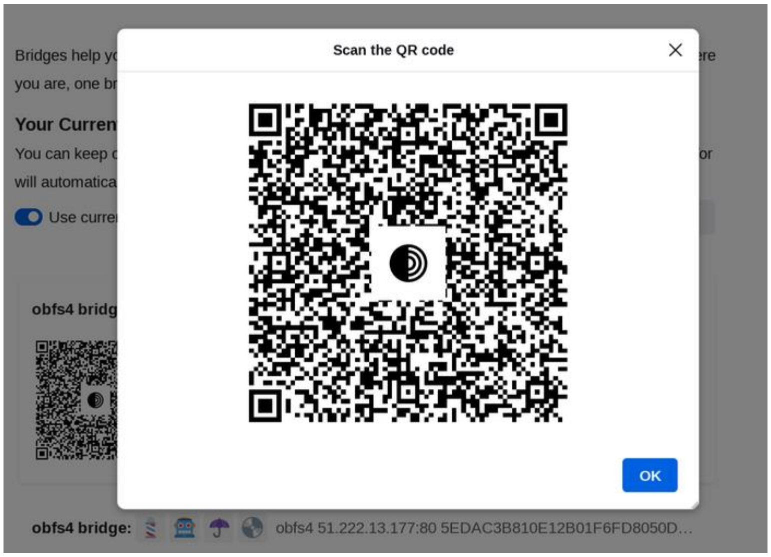
○ meek-azure

○ snowflake

Provide a Bridge I know
Enter bridge information from a trusted source

Current Configured Bridge: Not Configured

Figure 22



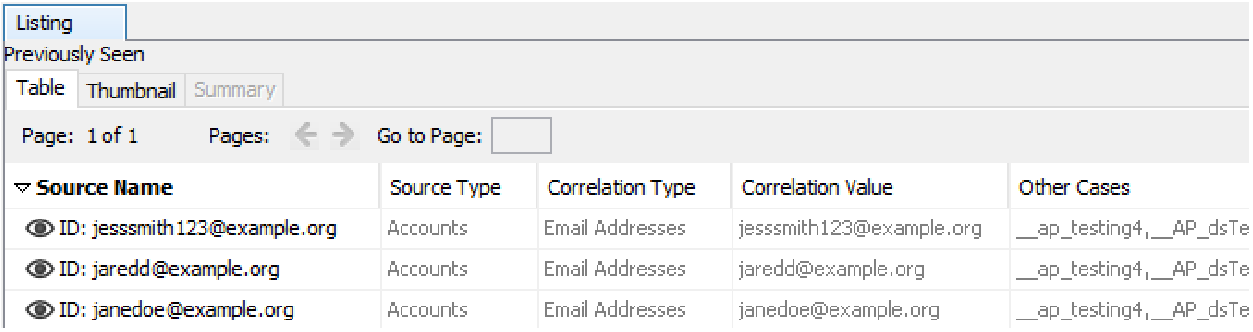
obfs4 bridge: obfs4 51.222.13.177:80 5EDAC3B810E12B01F6FD8050D…

Bridge Type: obfs4 – Obfuscated bridge that hides Tor traffic patterns

IP Address: 51.222.13.177

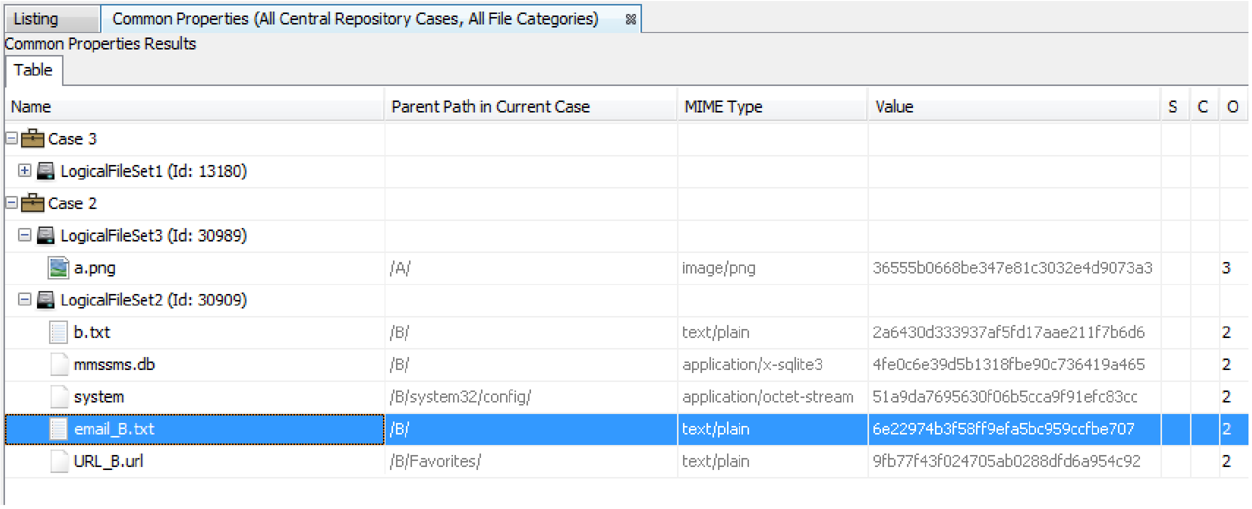
Port: 80

Fingerprint: Starts with 5EDAC3B810E12B01...



Source Name	Source Type	Correlation Type	Correlation Value	Other Cases
ID: jesssmith123@example.org	Accounts	Email Addresses	jesssmith123@example.org	__ap_testing4,__AP_dsTe
ID: jaredd@example.org	Accounts	Email Addresses	jaredd@example.org	__ap_testing4,__AP_dsTe
ID: janedoe@example.org	Accounts	Email Addresses	janedoe@example.org	__ap_testing4,__AP_dsTe

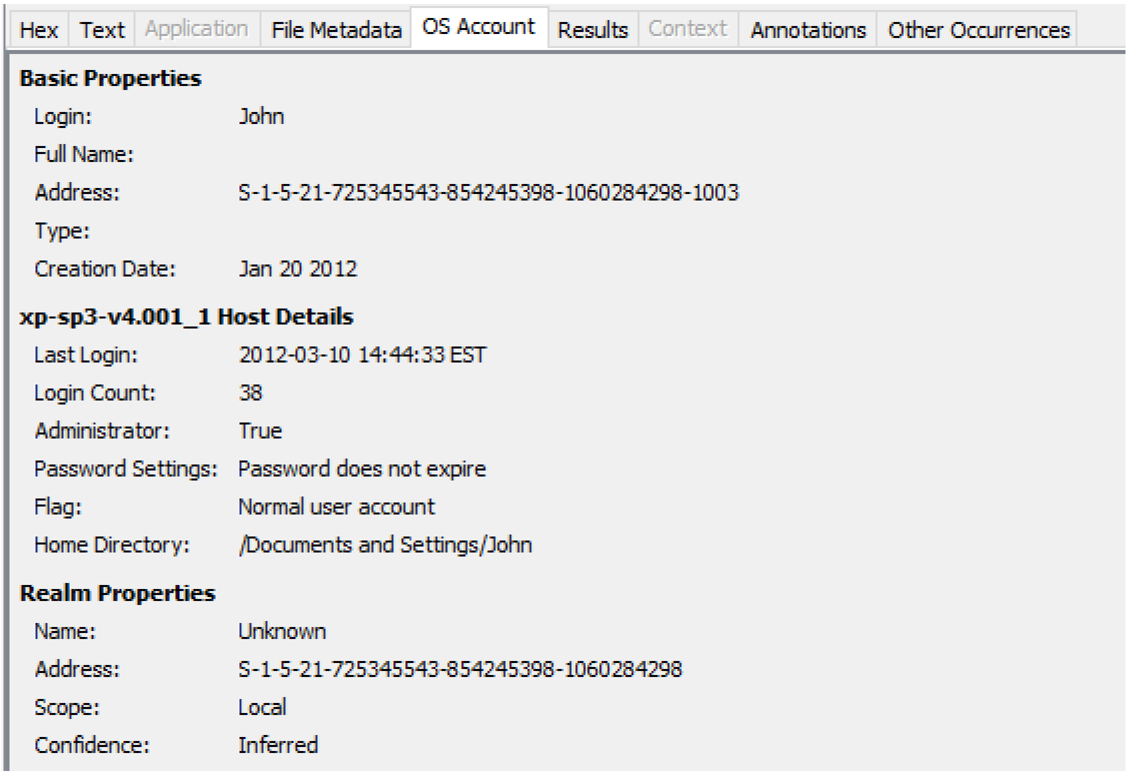
Figure 23 Get email address



Listing
Common Properties (All Central Repository Cases, All File Categories)
Common Properties Results
Table

Name	Parent Path in Current Case	MIME Type	Value	S	C	O
Case 3						
LogicalFileSet1 (Id: 13180)						
Case 2						
LogicalFileSet3 (Id: 30989)						
a.png	/A/	image/png	36555b0668be347e81c3032e4d9073a3			3
LogicalFileSet2 (Id: 30909)						
b.txt	/B/	text/plain	2a6430d333937af5fd17aae211f7b6d6			2
mmssms.db	/B/	application/x-sqlite3	4fe0c6e39d5b1318fbe90c736419a465			2
system	/B/system32/config/	application/octet-stream	51a9da7695630f06b5cca9f91efc83cc			2
email_B.txt	/B/	text/plain	6e22974b3f58ff9efa5bc959ccfbe707			2
URL_B.url	/B/Favorites/	text/plain	9fb77f43f024705ab0288dfd6a954c92			2

Figure 24 Get email related



Basic Properties

Login:	John
Full Name:	
Address:	S-1-5-21-725345543-854245398-1060284298-1003
Type:	
Creation Date:	Jan 20 2012

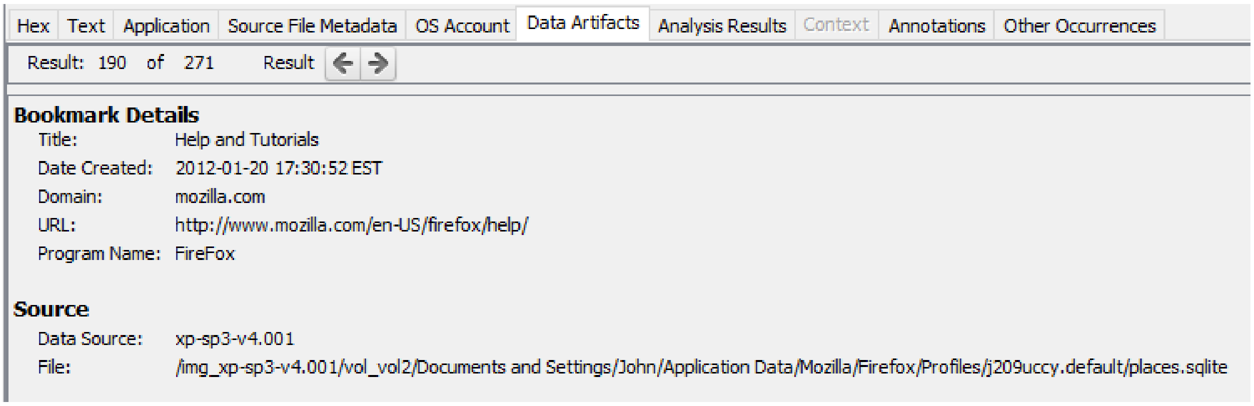
xp-sp3-v4.001_1 Host Details

Last Login:	2012-03-10 14:44:33 EST
Login Count:	38
Administrator:	True
Password Settings:	Password does not expire
Flag:	Normal user account
Home Directory:	/Documents and Settings/John

Realm Properties

Name:	Unknown
Address:	S-1-5-21-725345543-854245398-1060284298
Scope:	Local
Confidence:	Inferred

Figure 25 Basic properties



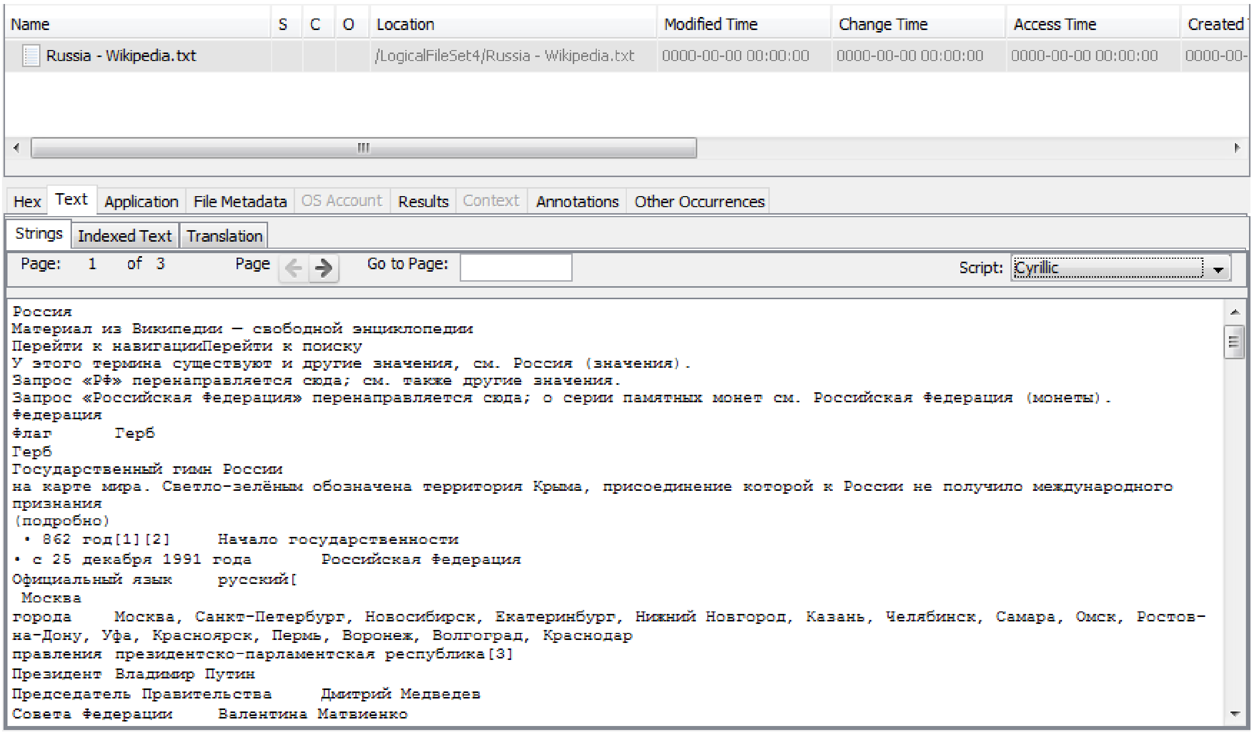
Bookmark Details

Title: Help and Tutorials
Date Created: 2012-01-20 17:30:52 EST
Domain: mozilla.com
URL: http://www.mozilla.com/en-US/firefox/help/
Program Name: FireFox

Source

Data Source: xp-sp3-v4.001
File: /img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/Application Data/Mozilla/Firefox/Profiles/j209uccy.default/places.sqlite

Figure 26 Showing book mark details

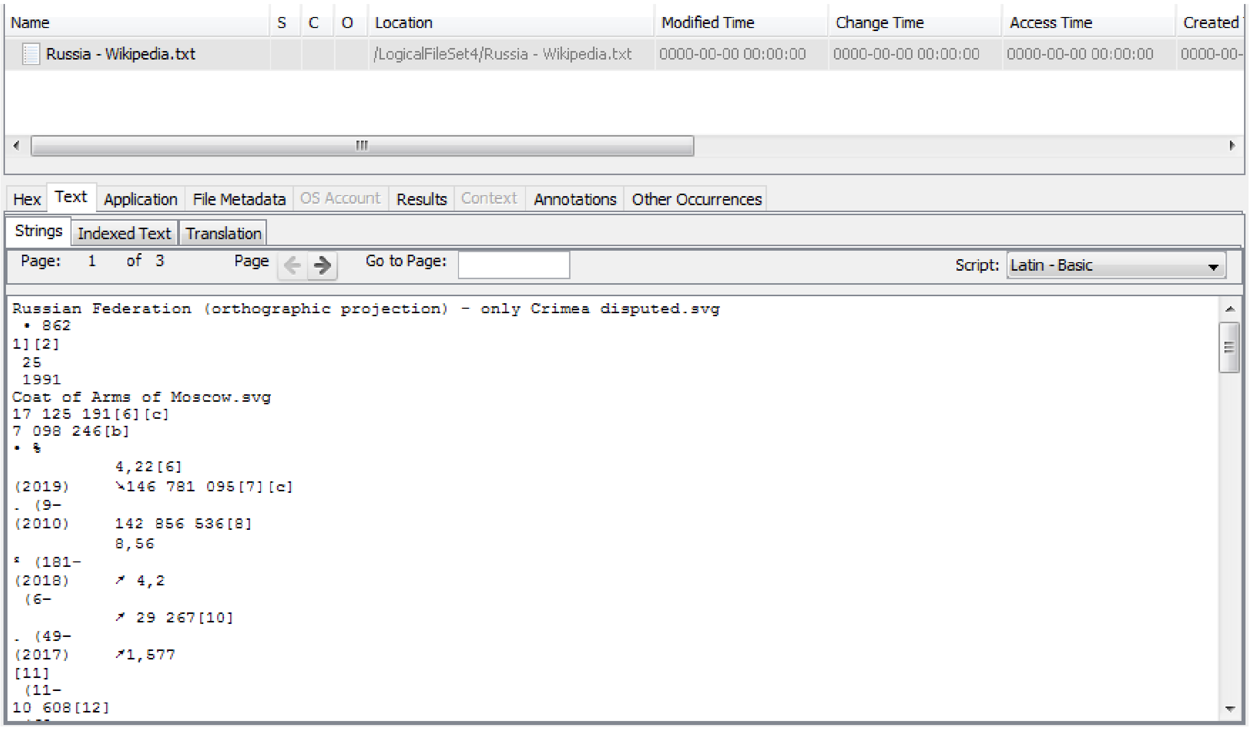


Name	S	C	O	Location	Modified Time	Change Time	Access Time	Created
Russia - Wikipedia.txt				/LogicalFileSet4/Russia - Wikipedia.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-

Script: Cyrillic

```
Россия
Материал из Википедии — свободной энциклопедии
Перейти к навигацииПерейти к поиску
У этого термина существуют и другие значения, см. Россия (значения).
Запрос «РФ» перенаправляется сюда; см. также другие значения.
Запрос «Российская федерация» перенаправляется сюда; о серии памятных монет см. Российская федерация (монеты).
федерация
Флаг      Герб
Герб
Государственный гимн России
на карте мира. Светло-зелёным обозначена территория Крыма, присоединение которой к России не получило международного
признания
(подробно)
 • 862 год[1][2]     Начало государственности
• с 25 декабря 1991 года        Российская федерация
Официальный язык     русский[
 Москва
города    Москва, Санкт-Петербург, Новосибирск, Екатеринбург, Нижний Новгород, Казань, Челябинск, Самара, Омск, Ростов-
на-Дону, Уфа, Красноярск, Пермь, Воронеж, Волгоград, Краснодар
правления президентско-парламентская республика[3]
Президент Владимир Путин
Председатель Правительства     Дмитрий Медведев
Совета федерации     Валентина Матвиенко
```

Figure 27 Russian text

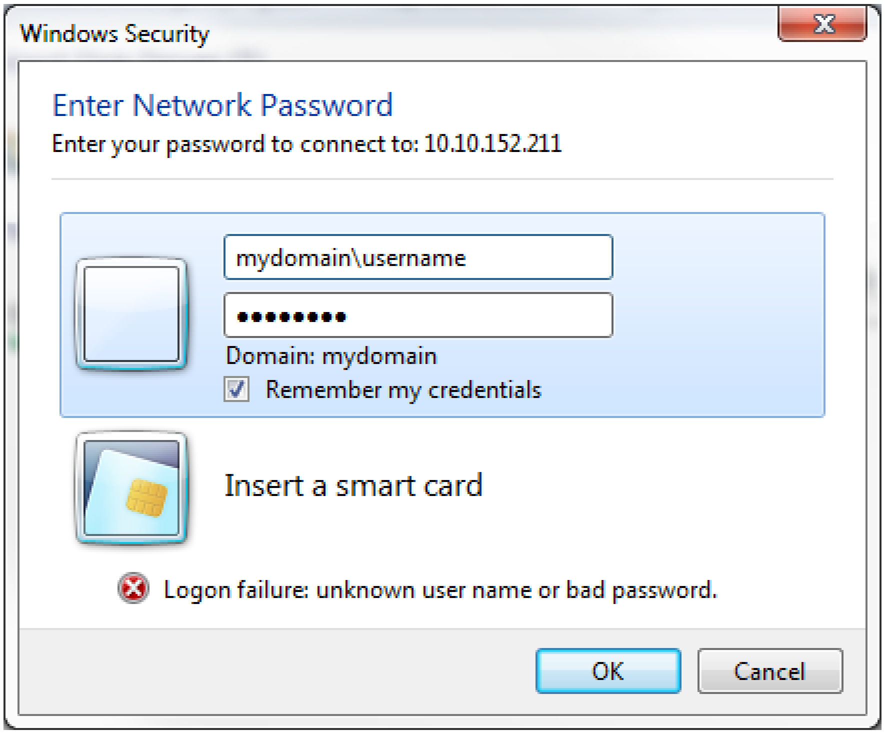


Name	S	C	O	Location	Modified Time	Change Time	Access Time	Created
Russia - Wikipedia.txt				/LogicalFileSet4/Russia - Wikipedia.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-

Script: Latin - Basic

```
Russian Federation (orthographic projection) - only Crimea disputed.svg
 • 862
1][2]
 25
 1991
Coat of Arms of Moscow.svg
17 125 191[6][c]
7 098 246[b]
• %
          4,22[6]
(2019)    ↘146 781 095[7][c]
. (9-
(2010)    142 856 536[8]
          8,56
* (181-
(2018)    ↗ 4,2
 (6-
          ↗ 29 267[10]
. (49-
(2017)    ↗1,577
[11]
 (11-
10 608[12]
```

Figure 28 Cost related



Enter Network Password

Enter your password to connect to: 10.10.152.211

mydomain\username

••••••••••

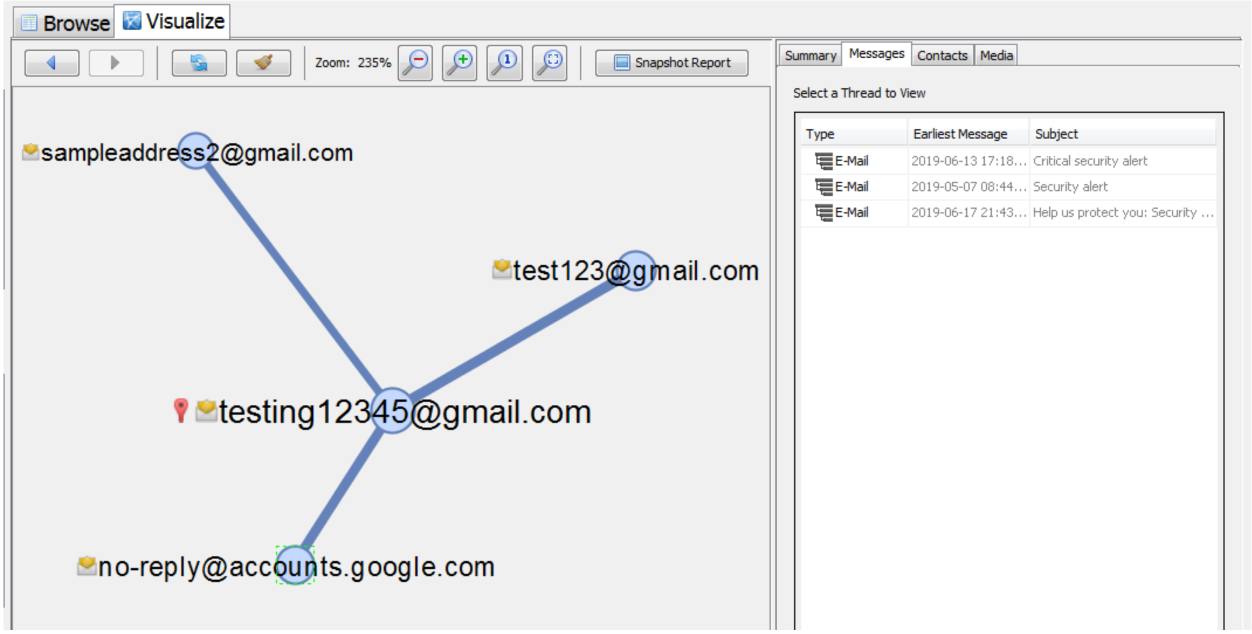
Domain: mydomain

☑ Remember my credentials

Insert a smart card

Logon failure: unknown user name or bad password.

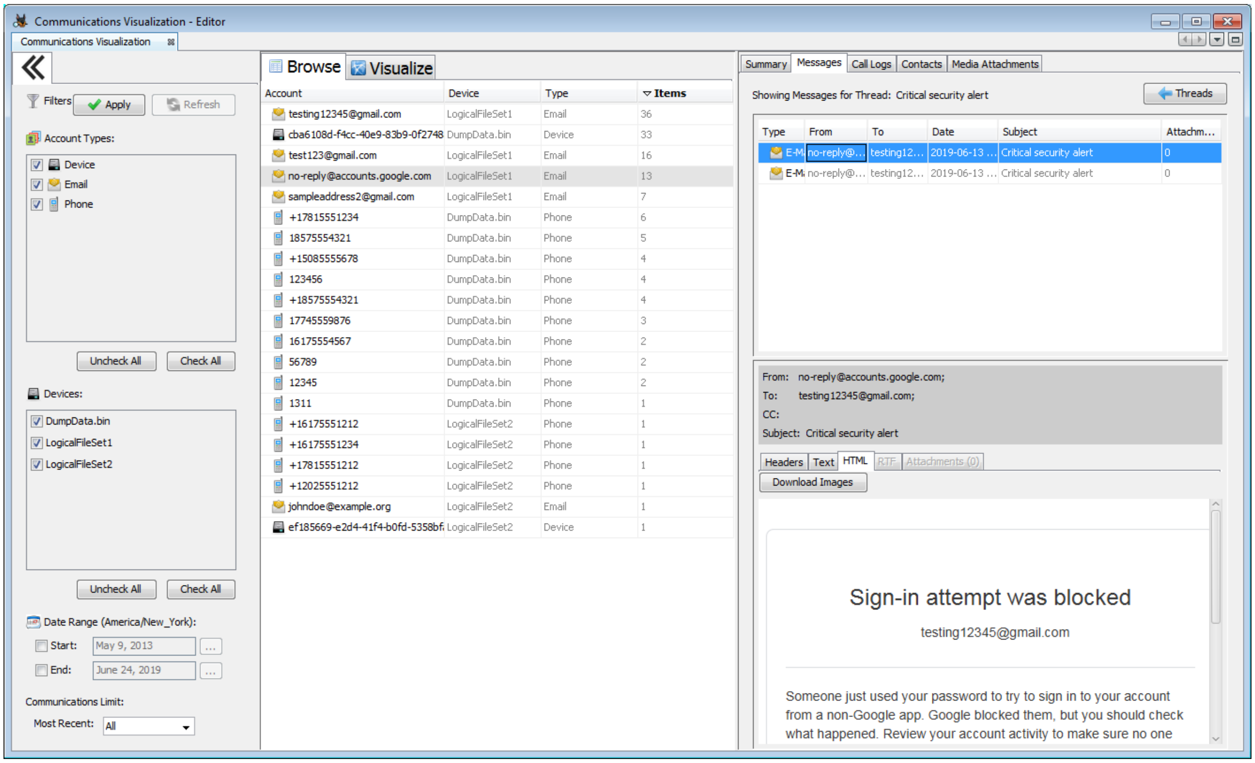
Figure 29 Get IP



Select a Thread to View

Type	Earliest Message	Subject
E-Mail	2019-06-13 17:18...	Critical security alert
E-Mail	2019-05-07 08:44...	Security alert
E-Mail	2019-06-17 21:43...	Help us protect you: Security ...

Figure 30 Email communication graph



Account Types:

- ☑ Device
- ☑ Email
- ☑ Phone

Devices:

- ☑ DumpData.bin
- ☑ LogicalFileSet1
- ☑ LogicalFileSet2

Date Range (America/New_York):

☐ Start: May 9, 2013

☐ End: June 24, 2019

Communications Limit:

Most Recent: All

Account	Device	Type	Items
testing12345@gmail.com	LogicalFileSet1	Email	36
cba6108d-f4cc-40e9-83b9-0f2748	DumpData.bin	Device	33
test123@gmail.com	LogicalFileSet1	Email	16
no-reply@accounts.google.com	LogicalFileSet1	Email	13
sampleaddress2@gmail.com	LogicalFileSet1	Email	7
+17815551234	DumpData.bin	Phone	6
18575554321	DumpData.bin	Phone	5
+15085555678	DumpData.bin	Phone	4
123456	DumpData.bin	Phone	4
+18575554321	DumpData.bin	Phone	4
17745559876	DumpData.bin	Phone	3
16175554567	DumpData.bin	Phone	2
56789	DumpData.bin	Phone	2
12345	DumpData.bin	Phone	2
1311	DumpData.bin	Phone	1
+16175551212	LogicalFileSet2	Phone	1
+16175551234	LogicalFileSet2	Phone	1
+17815551212	LogicalFileSet2	Phone	1
+12025551212	LogicalFileSet2	Phone	1
johndoe@example.org	LogicalFileSet2	Email	1
ef185669-e2d4-41f4-b0fd-5358bf	LogicalFileSet2	Device	1

Showing Messages for Thread: Critical security alert

Type	From	To	Date	Subject	Attachm...
E-M	no-reply@...	testing12...	2019-06-13 ...	Critical security alert	0
E-M	no-reply@...	testing12...	2019-06-13 ...	Critical security alert	0

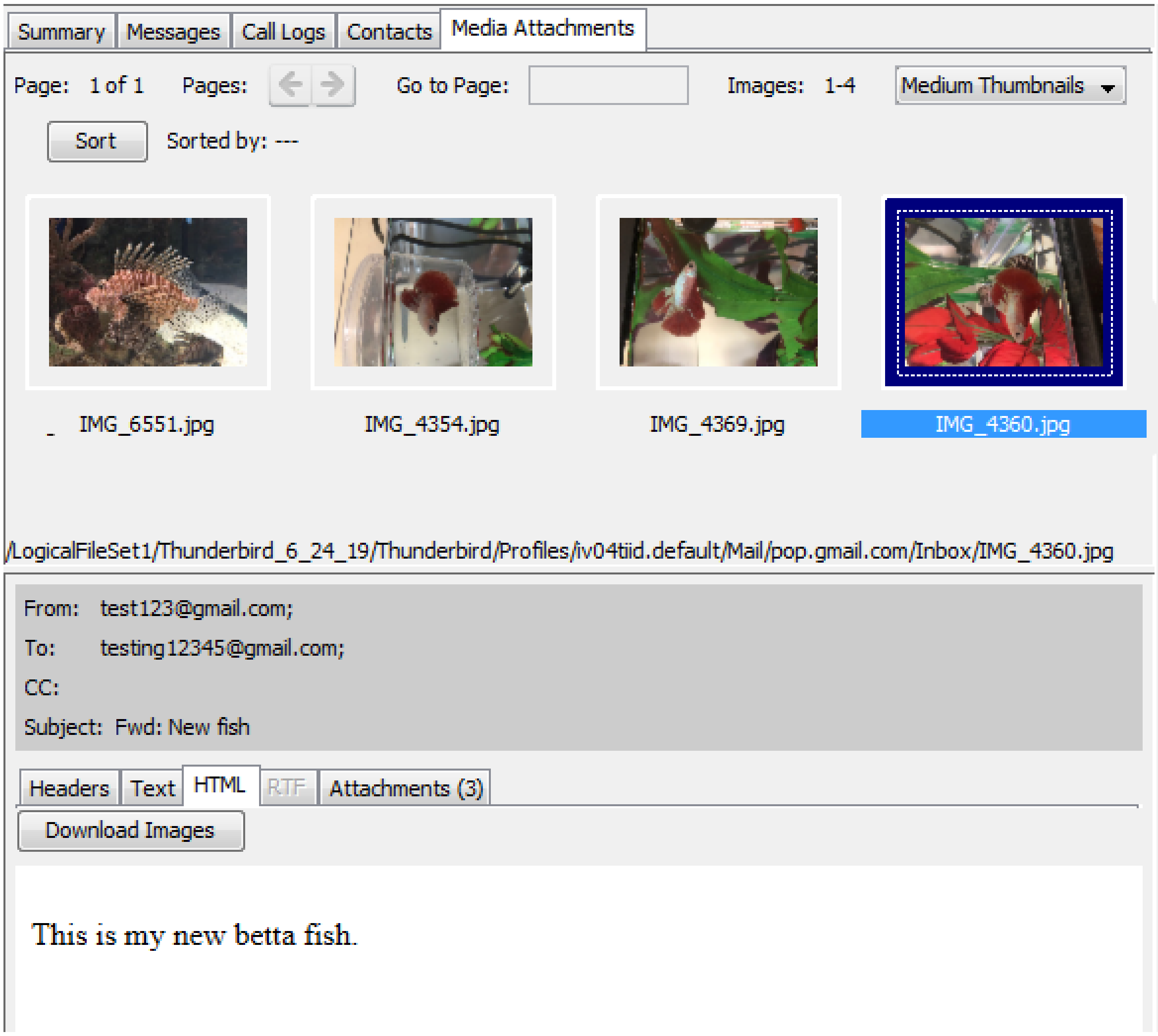
From: no-reply@accounts.google.com;
To: testing12345@gmail.com;
CC:
Subject: Critical security alert

Sign-in attempt was blocked

testing12345@gmail.com

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one

Figure 31 Get phone numbers and emails address

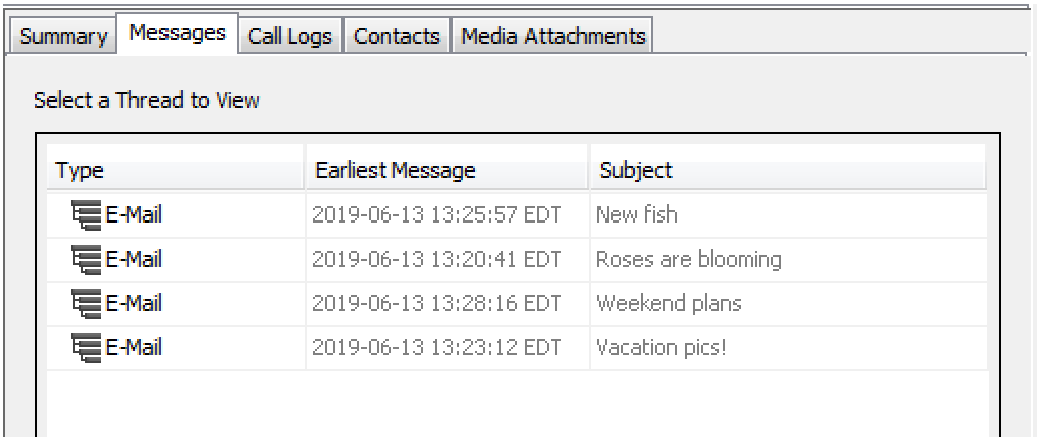


/LogicalFileSet1/Thunderbird_6_24_19/Thunderbird/Profiles/iv04tiid.default/Mail/pop.gmail.com/Inbox/IMG_4360.jpg

From: test123@gmail.com;
To: testing12345@gmail.com;
CC:
Subject: Fwd: New fish

This is my new betta fish.

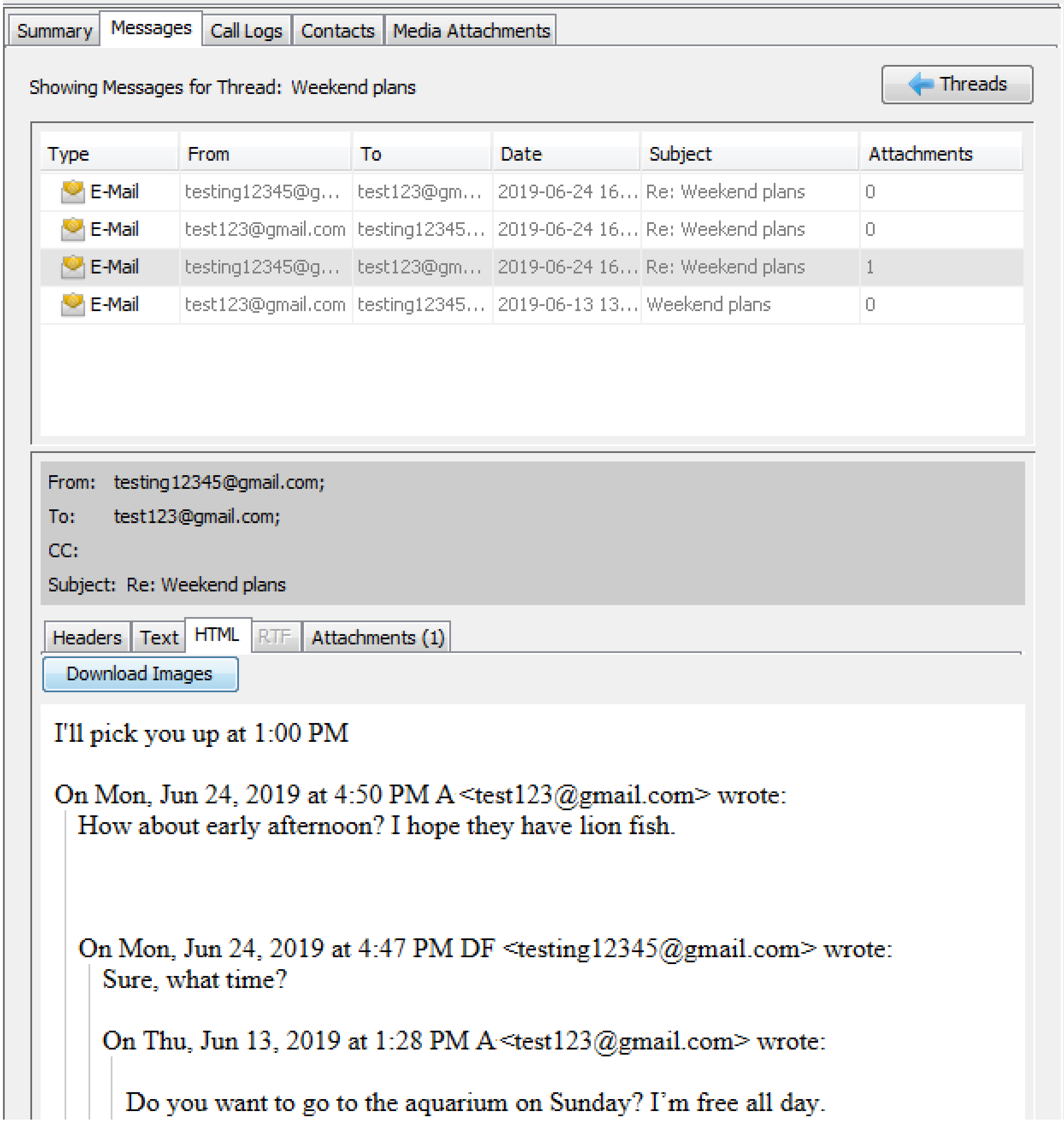
Figure 32 Sender and receiver emails



Select a Thread to View

Type	Earliest Message	Subject
E-Mail	2019-06-13 13:25:57 EDT	New fish
E-Mail	2019-06-13 13:20:41 EDT	Roses are blooming
E-Mail	2019-06-13 13:28:16 EDT	Weekend plans
E-Mail	2019-06-13 13:23:12 EDT	Vacation pics!

Figure 33 Emails subjects



Showing Messages for Thread: Weekend plans

Type	From	To	Date	Subject	Attachments
E-Mail	testing12345@g...	test123@gm...	2019-06-24 16...	Re: Weekend plans	0
E-Mail	test123@gmail.com	testing12345...	2019-06-24 16...	Re: Weekend plans	0
E-Mail	testing12345@g...	test123@gm...	2019-06-24 16...	Re: Weekend plans	1
E-Mail	test123@gmail.com	testing12345...	2019-06-13 13...	Weekend plans	0

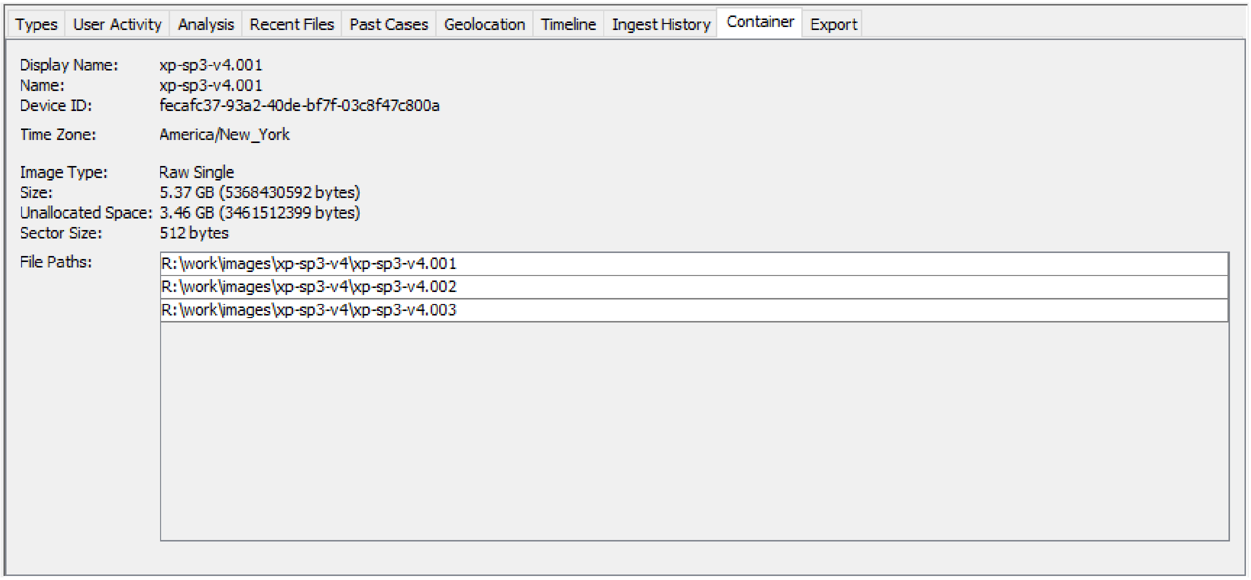
From: testing12345@gmail.com;
To: test123@gmail.com;
CC:
Subject: Re: Weekend plans

I'll pick you up at 1:00 PM

On Mon, Jun 24, 2019 at 4:50 PM A <test123@gmail.com> wrote:

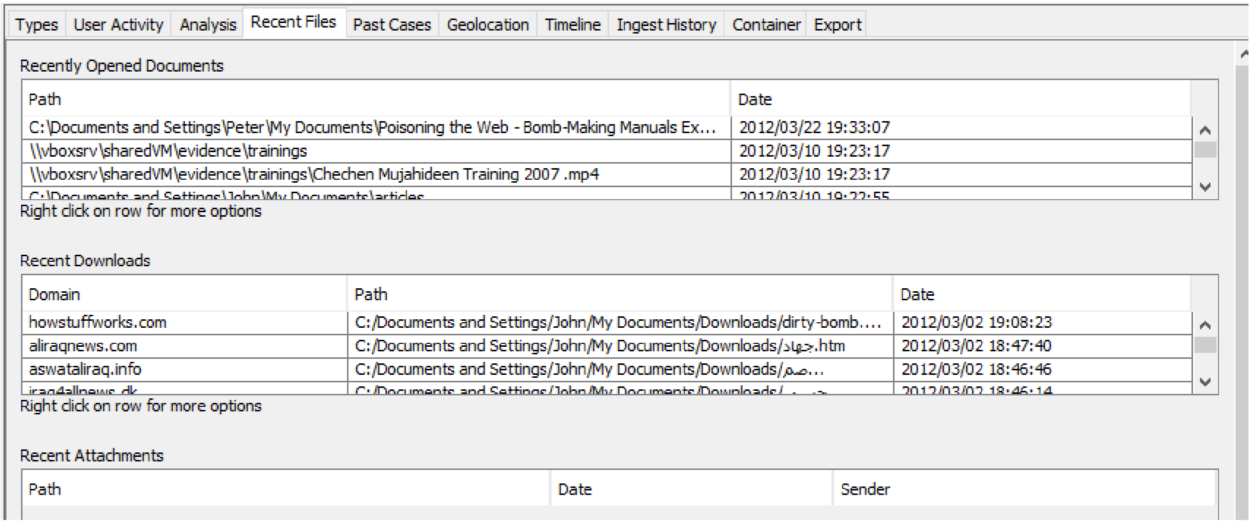
> How about early afternoon? I hope they have lion fish.
>
> On Mon, Jun 24, 2019 at 4:47 PM DF <testing12345@gmail.com> wrote:
>
> > Sure, what time?
> >
> > On Thu, Jun 13, 2019 at 1:28 PM A <test123@gmail.com> wrote:
> >
> > > Do you want to go to the aquarium on Sunday? I'm free all day.

Figure 34 Get email body



Display Name:	xp-sp3-v4.001
Name:	xp-sp3-v4.001
Device ID:	fecafc37-93a2-40de-bf7f-03c8f47c800a
Time Zone:	America/New_York
Image Type:	Raw Single
Size:	5.37 GB (5368430592 bytes)
Unallocated Space:	3.46 GB (3461512399 bytes)
Sector Size:	512 bytes
File Paths:	R:\work\images\xp-sp3-v4\xp-sp3-v4.001 R:\work\images\xp-sp3-v4\xp-sp3-v4.002 R:\work\images\xp-sp3-v4\xp-sp3-v4.003

Figure 35 Get file path



Recently Opened Documents

Path	Date
C:\Documents and Settings\Peter\My Documents\Poisoning the Web - Bomb-Making Manuals Ex...	2012/03/22 19:33:07
\\vboxsrv\sharedVM\evidence\trainings	2012/03/10 19:23:17
\\vboxsrv\sharedVM\evidence\trainings\Chechen Mujahideen Training 2007 .mp4	2012/03/10 19:23:17
C:\Documents and Settings\John\My Documents\articles	2012/03/10 19:22:55

Right click on row for more options

Recent Downloads

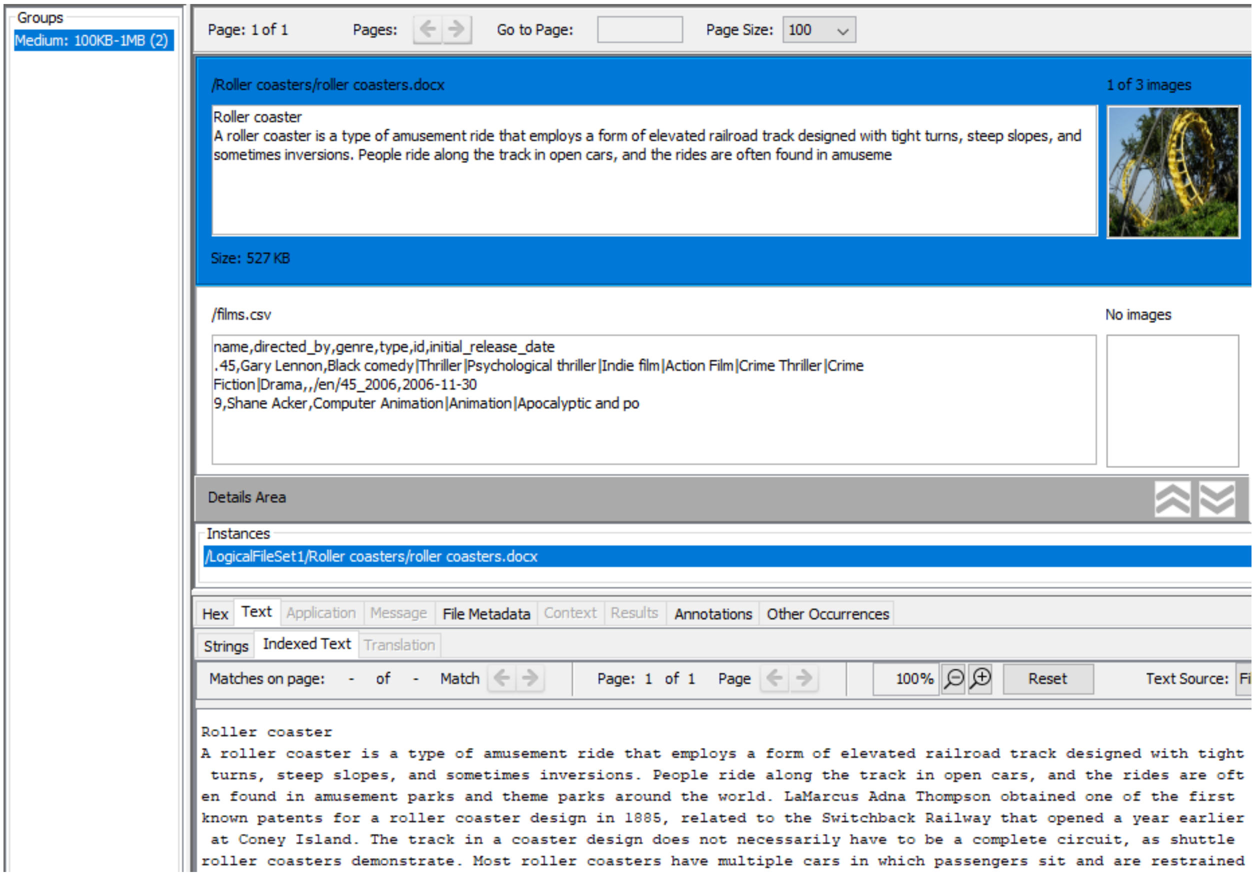
Domain	Path	Date
howstuffworks.com	C:/Documents and Settings/John/My Documents/Downloads/dirty-bomb....	2012/03/02 19:08:23
aliraqnews.com	C:/Documents and Settings/John/My Documents/Downloads/جهاد.htm	2012/03/02 18:47:40
aswataliraq.info	C:/Documents and Settings/John/My Documents/Downloads/صم...	2012/03/02 18:46:46
iraq4allnews.dk	C:/Documents and Settings/John/My Documents/Downloads/	2012/03/02 18:46:14

Right click on row for more options

Recent Attachments

Path	Date	Sender

Figure 36 Get domains



Roller coaster
A roller coaster is a type of amusement ride that employs a form of elevated railroad track designed with tight turns, steep slopes, and sometimes inversions. People ride along the track in open cars, and the rides are often found in amuseme

```
name,directed_by,genre,type,id,initial_release_date
.45,Gary Lennon,Black comedy|Thriller|Psychological thriller|Indie film|Action Film|Crime Thriller|Crime
Fiction|Drama,,/en/45_2006,2006-11-30
9,Shane Acker,Computer Animation|Animation|Apocalyptic and po
```

```
Roller coaster
A roller coaster is a type of amusement ride that employs a form of elevated railroad track designed with tight
 turns, steep slopes, and sometimes inversions. People ride along the track in open cars, and the rides are oft
en found in amusement parks and theme parks around the world. LaMarcus Adna Thompson obtained one of the first
known patents for a roller coaster design in 1885, related to the Switchback Railway that opened a year earlier
 at Coney Island. The track in a coaster design does not necessarily have to be a complete circuit, as shuttle
roller coasters demonstrate. Most roller coasters have multiple cars in which passengers sit and are restrained
```

Figure 37 Text

Comparison of Clean and Activity Disk Images.

Clean Disk Image (Before Any Activity)

Artifact / Category	Observation
Internet Access	No internet connection detected.
.gz Files	No .gz (compressed) files found.
Web URLs	No URLs or web activity recorded.
IP Address	No IPs captured or logged.
Browser Activity / User-Agent	No browser history or user-agent found.
Registry Files (.reg)	No exported registry files found.
Documents	No PDF or office documents found.
Credential Information	No usernames, passwords, or sensitive text found.
Tor Bridge / Obfuscation	No signs of Tor usage or hidden communication.
Email Artifacts	No emails (senders, receivers, or bodies) detected.
Bookmarks / Browser Content	Not available or recorded.
Contact Data	No names, addresses, or phone numbers extracted.
Deleted Files	Very few deleted files, mostly system-generated.
File Types Detected	Normal system files only.
PhotoRec Recovery	Minimal recovery – no significant user files recovered.
Hash Lookup	No known bad or good file hashes in the database.

Activity Disk Image (After Suspicious Tasks)

Artifact / Category	Observation
Internet Access	Internet activity detected; multiple web artifacts recovered.
.gz Files	132 .gz files found, many in unallocated space.
Web URLs	Found URL: http://vulnweb.com/testphp.vulnweb.com/userinfo.php
IP Address	Detected IP: 142.228.249.39 (possible attacker or test system).
Browser Activity / User-Agent	Opera browser on Linux; activity confirmed.
Registry Files (.reg)	9 deleted registry export files recovered.
Documents	Recovered PDF: TestDiskDocumentation.pdf from deleted space.
Credential Information	Username: kike, Password: 1234, Address: kio (from HTML file).
Tor Bridge / Obfuscation	Detected: Obfs4 Tor bridge, IP 51.222.13.177, port 80.
Email Artifacts	Multiple emails with senders, receivers, subjects, and bodies recovered.
Bookmarks / Browser Content	Bookmarks and Russian text found in analysis.
Contact Data	Names, phone numbers, addresses extracted from unallocated files.
Deleted Files	Many deleted files carved including .html, .reg, and documents.
File Types Detected	Mixed: system files, deleted web files, PDF, registry files.
PhotoRec Recovery	Successful carving of deleted and hidden files.
Hash Lookup	Hashing done, but no known hash sets loaded. Manual analysis done.

Conclusion

In this project, we focused on understanding how digital forensics works by taking and analyzing two disk images. One image was taken from a clean Windows 11 virtual machine, and the second was taken after performing some user activities that could seem suspicious. We used **FTK Imager** to capture both images and **Autopsy** to examine them.

The clean image didn’t show any major activity it had no internet usage, no strange files, and everything looked normal. It served as a reference point for us. But the second image clearly showed changes. We found over 130 .gz files, some deleted registry files, a PDF document, and even a leak of a username and password inside an HTML file. There was also a Tor bridge detected, which means the system might have been used to hide traffic, and several email artifacts and web activities were found.

By comparing both images, we were able to see how even simple activities can leave behind digital traces. This helped us understand how investigators use tools like Autopsy to recover deleted files and analyze system behavior. It also showed how important it is to take a clean snapshot before any activity, so changes can be tracked properly.

Overall, this project gave us hands-on experience in acquiring evidence, working with forensic tools, and understanding how digital traces are collected and examined. It made the concepts we learned in class feel more real and practical.