



ACCD5000 - Computer Forensics
Mr. Maxime LE ROY-MEUNIER

End of April Computer Forensics Presentation Report

RESEARCH, CRITICALLY ANALYSE AND PRESENT



Summary

Part 1 :

What are Digital &
Computer Forensics

Part 2

Tools used in Digital &
Computer Forensics

Part 3

Research on Real-
world use cases

Part 4

Chain of Custody,
Gathering evidences,
Resolving study case

Part 5

Live demonstration
with autopsy and
virtual machine lab

Part 6

Conclusion



What are Digital and Computer Forensics

First years of a new era

Digital Forensics is an area that has developed with the emergence of digital devices in our lives, during 1970-1990. It concerns the recovery, investigation, examination, and analysis of data found in digital devices after a cybercrime. A cybercrime is a crime committed through the internet / digital tools.

Digital Forensics

Digital forensics is simply the process of investigation and recovery of material found in digital devices, which are commonly related to computer crimes.

Computer forensics

Some people interchange the terms "computer forensics" and "digital forensics," yet there are differences between them. Computer Forensics is a subbranch of Digital Forensics. It concerns the investigation on computing devices only (Computers, Servers, Hard Drives recovery...).

Other Subbranches, like Computer Forensics, exist

- Smartphone Forensics
- Network Forensics
- Database Forensics
- IoT Forensics

And many others...

DIGITAL & COMPUTER FORENSICS

Some Tools Used



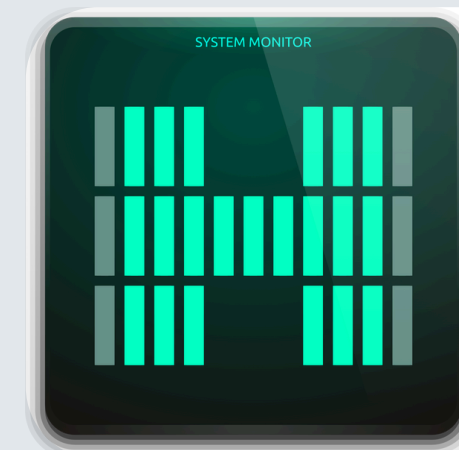
Autopsy®

Open, Analyse, recover,
investigate any disk image



ImHex

A Hex Editor for Reverse
Engineers, Programmers



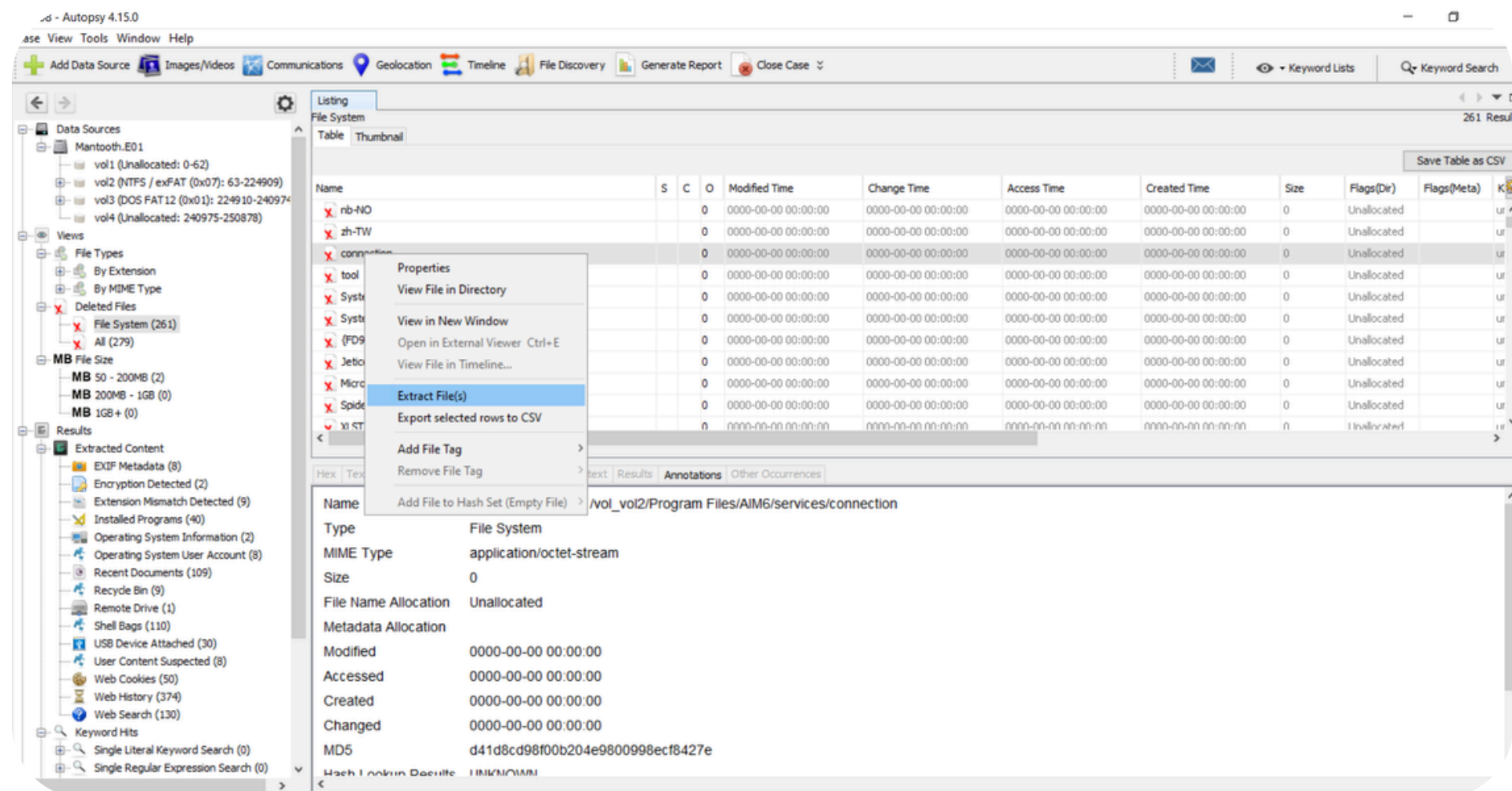
HTOP

A UNIX live system monitor



Autopsy®

Open, Analyse, recover, investigate
any disk image
Originally based on algorithms from
CGSecurity (TestDisk & PhotoRec)



Pros

Open-source and free to use

Comprehensive feature set for in-depth analysis

Regular updates from a community of developers

Extensible through plugins and modules

Widely used and trusted in the forensic community

Cons

Complex interface for new users

Performance can lag with large data sets

Support primarily community-driven, not official

Requires significant system resources

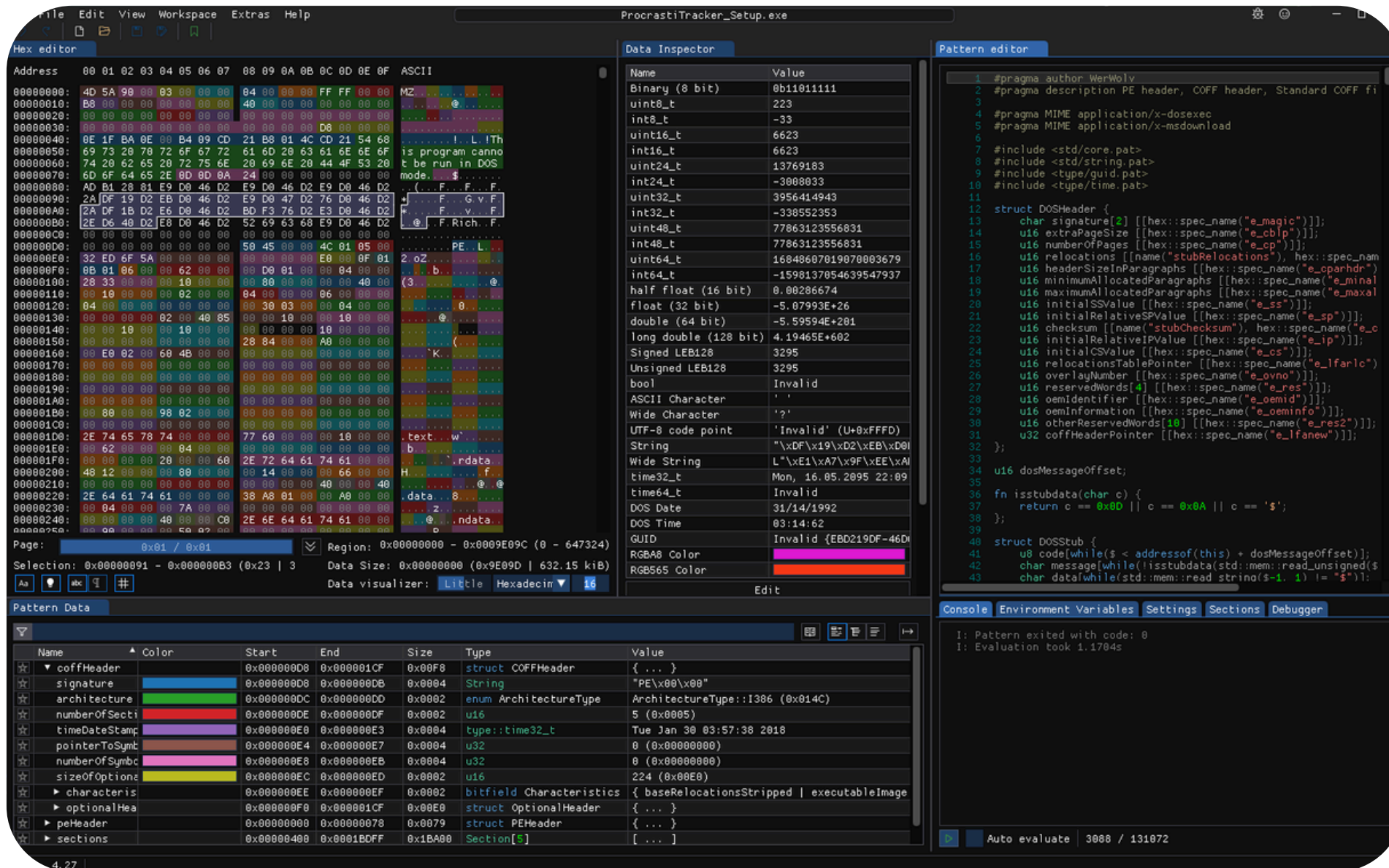
Setup and configuration can be complex



ImHex

A Hex Editor for Reverse Engineers,
Programmers

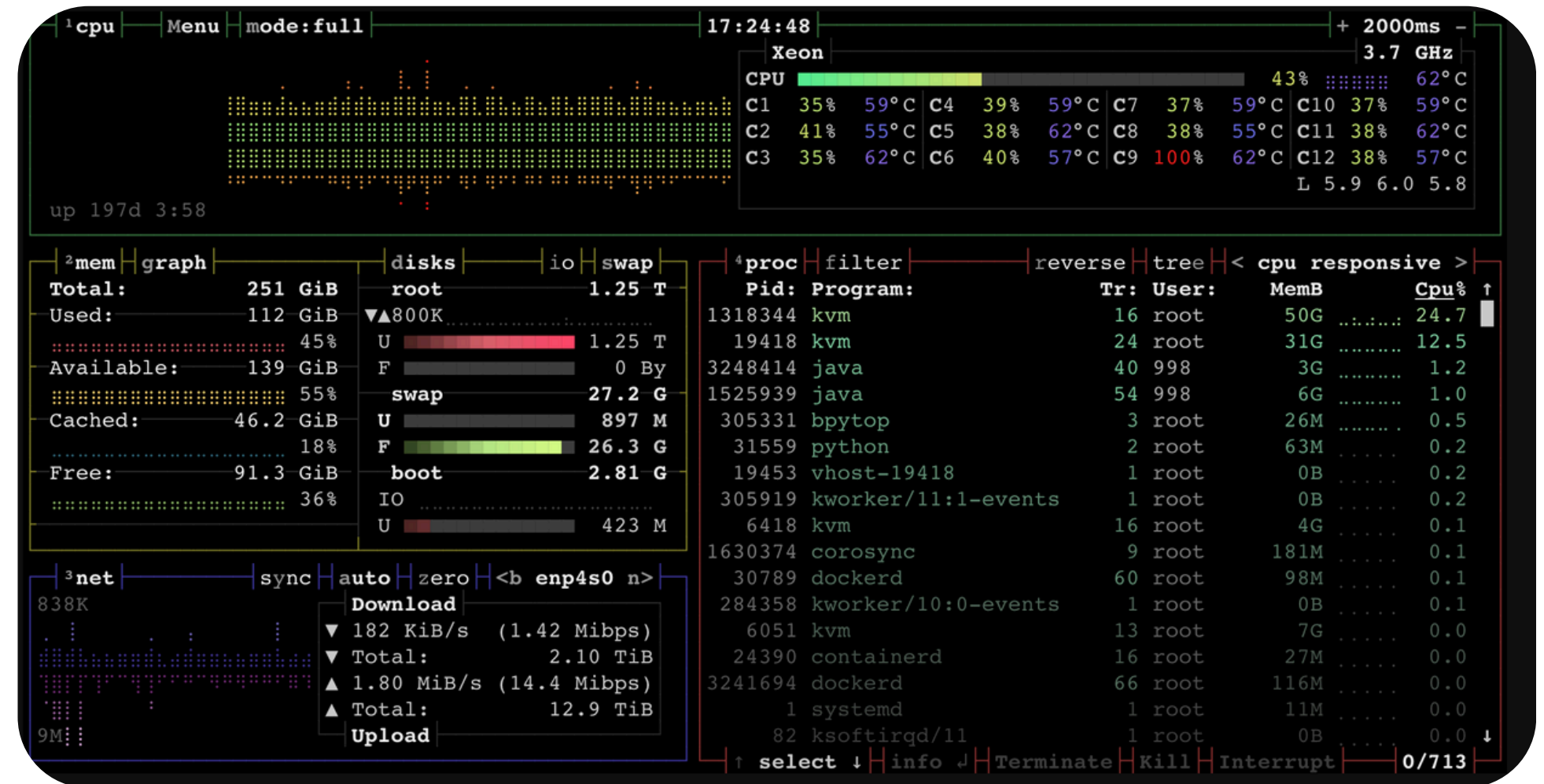
This software is Open-Source and has more than 33k stars on its github repository





HTOP

A UNIX live system monitor



This software can be installed on Linux and MacOS.

Real-World cases

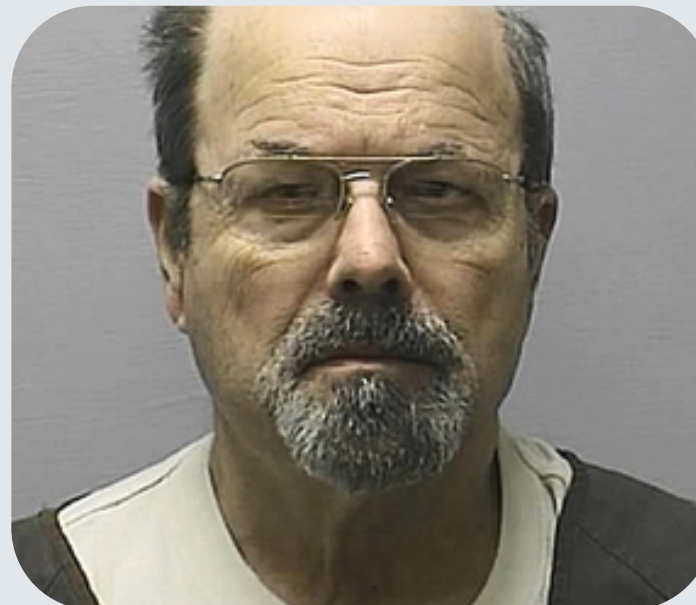
- The Capture of Serial Killer Dennis Rader, BTK.

Denis Rader, known as BTK

Dennis Lynn Rader (born March 9, 1945), also known as BTK (an abbreviation he gave himself, for "bind, torture, kill"), is an American serial killer who murdered at least ten people

A close relationship with the media

Denis Rader liked to send letters to some medias to maybe let the police catch him. He was playing with them.



Too much of this self confidence...

One day, BTK sent a Floppy Disc to KensasTV television. Metadata from this storage support were enough to find him. He was judged in 2005 and was sentenced to life imprisonment without the possibility of parole for 175 years.

Chain Of Custody

The chain of custody is a documentation process that tracks the movement and handling of evidence from the time it is collected until it is presented in court. It serves to establish the integrity and security of evidence by providing a documented history of who handled it, when, and under what circumstances.

Chain of Custody

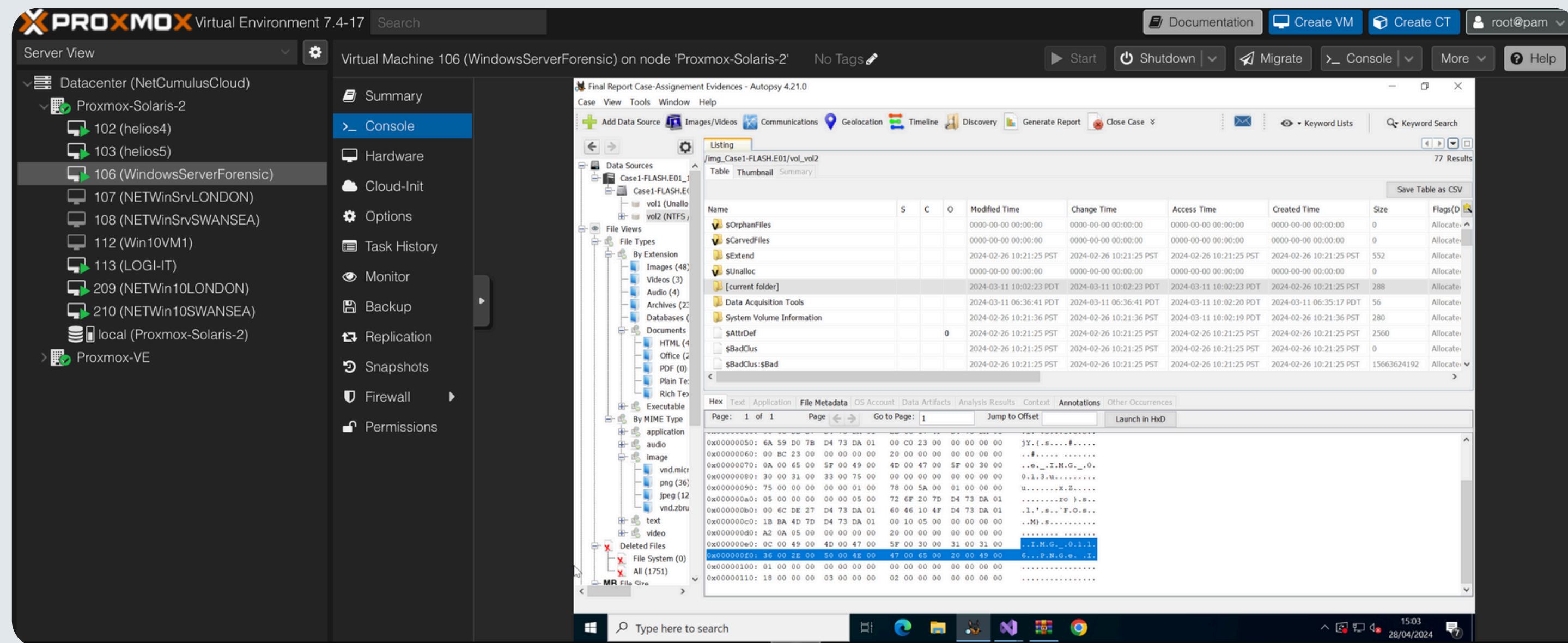


- custody
- control
- transfer
- analysis
- results



Gathering Evidences

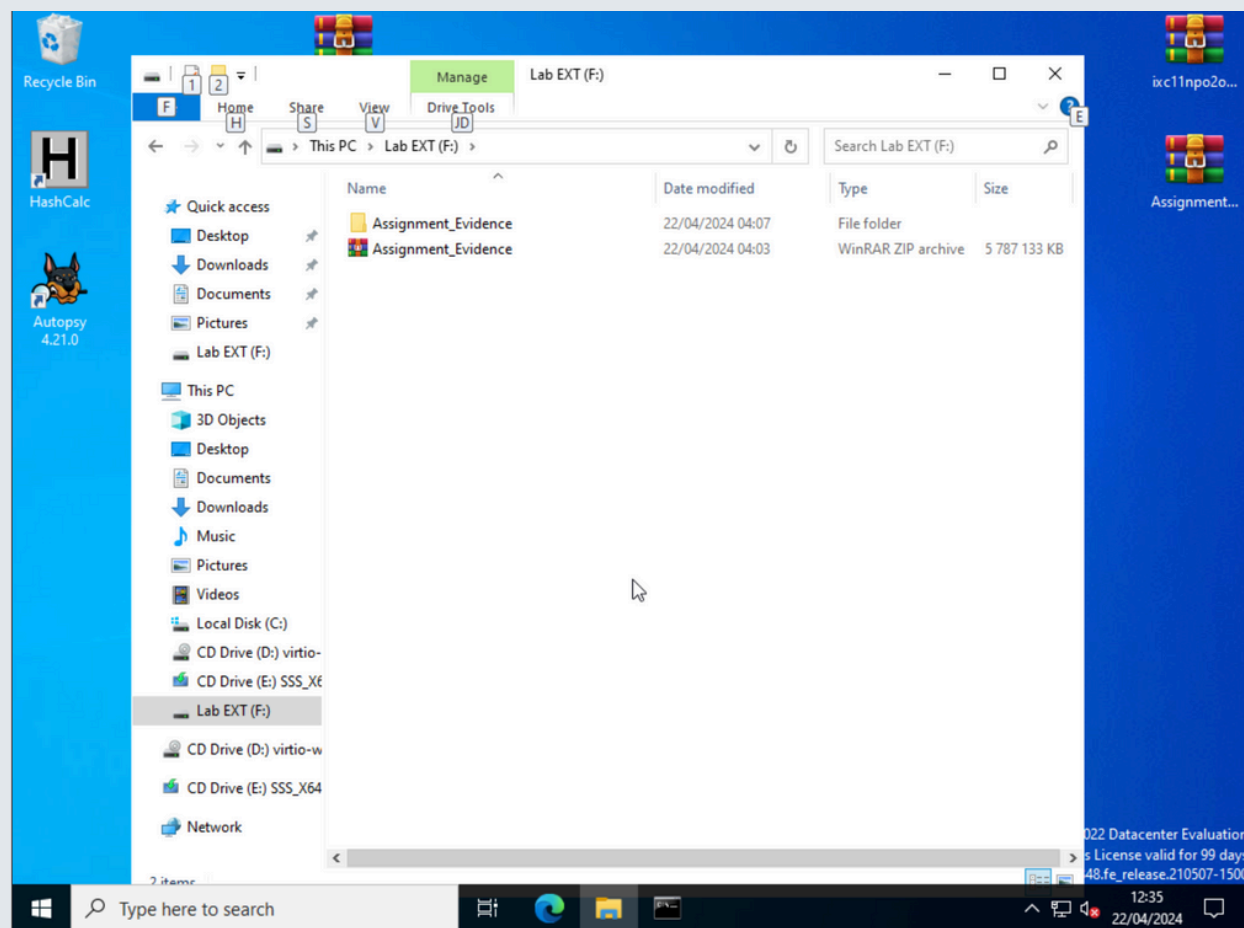
Using Autopsy and Microsoft Visual Studio



Using Proxmox installed on a dedicated server, isolated VM for forensics operations, Windows Server 2022.

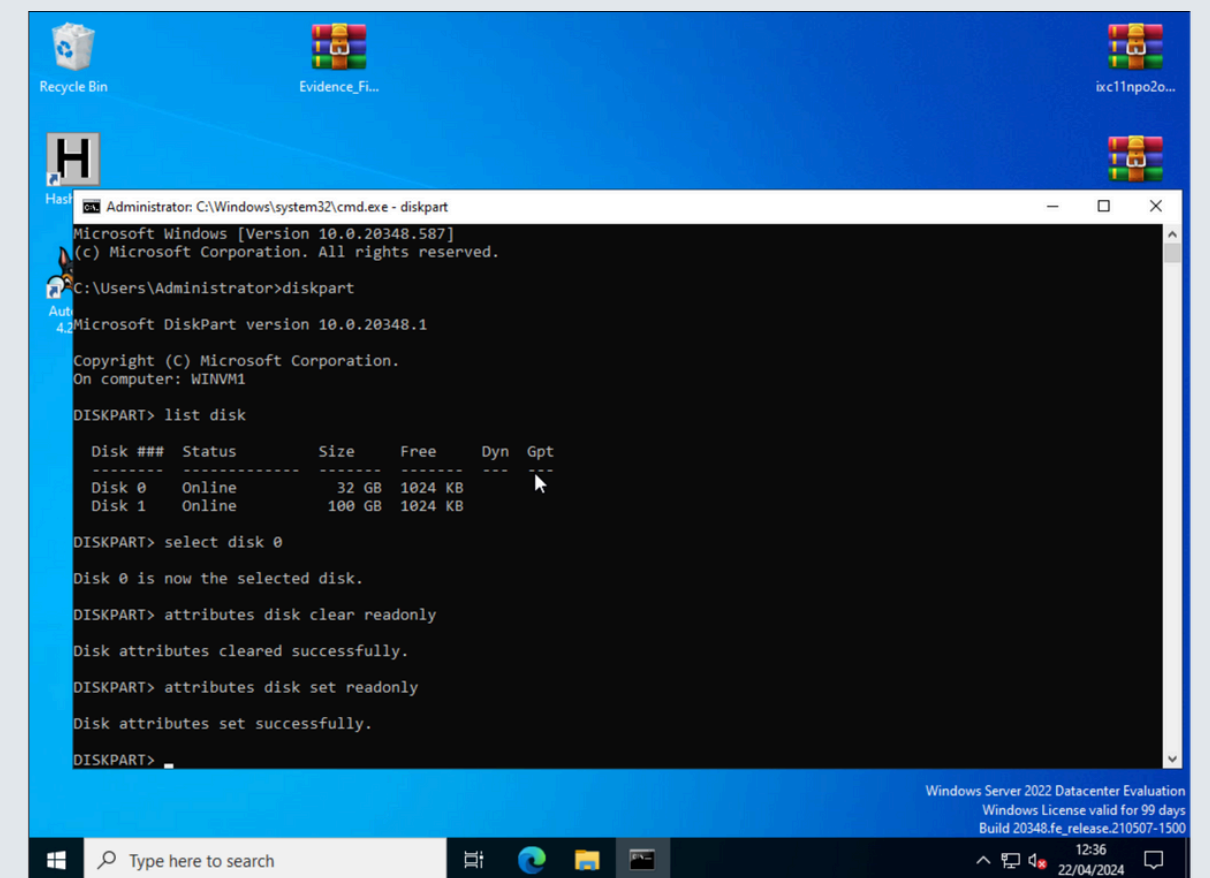
Gathering Evidences

Using Autopsy and Microsoft Visual Studio



Extracting the evidence archive

Downloading disc image

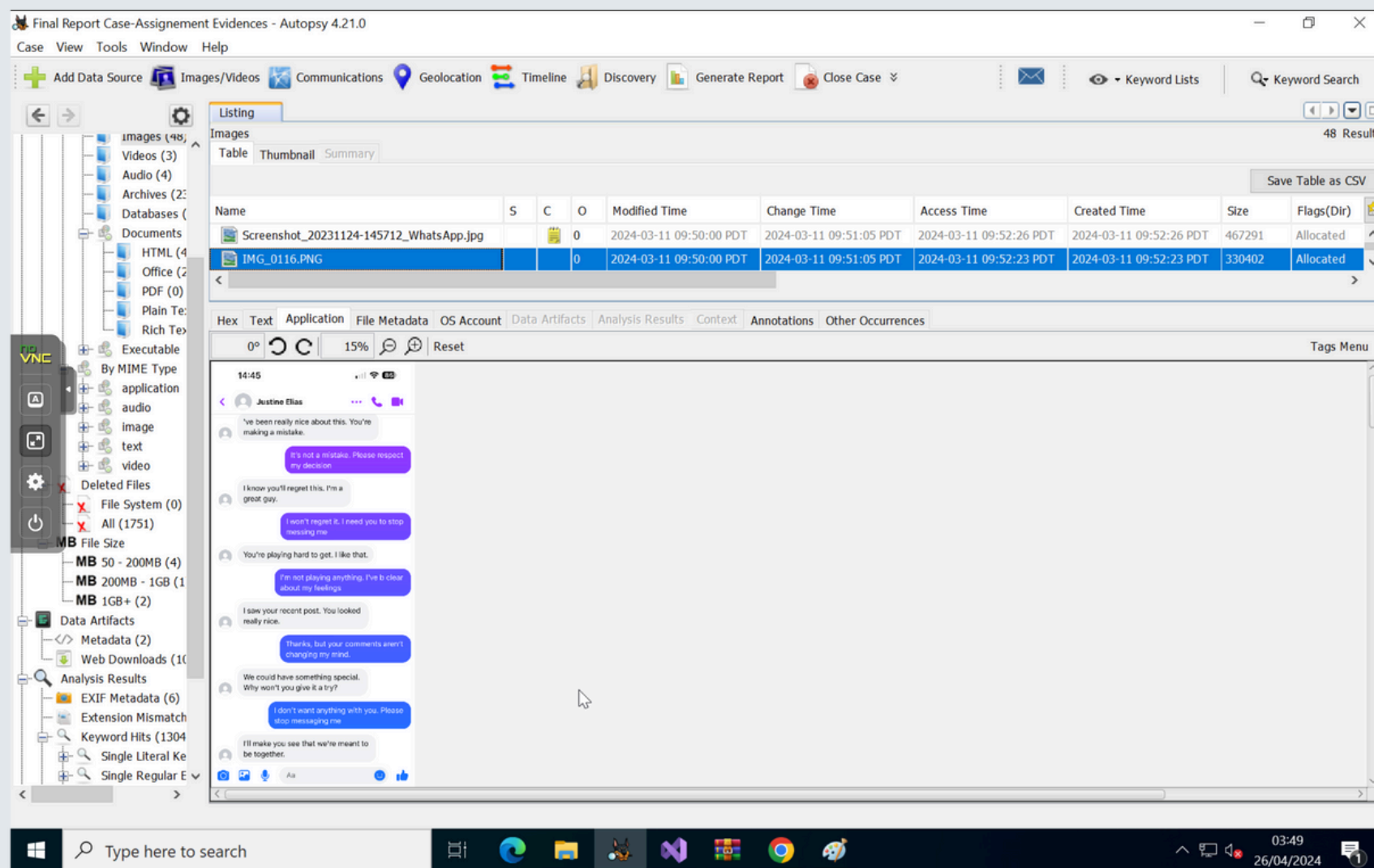


Locking external disk with diskpart, where evidence is stored

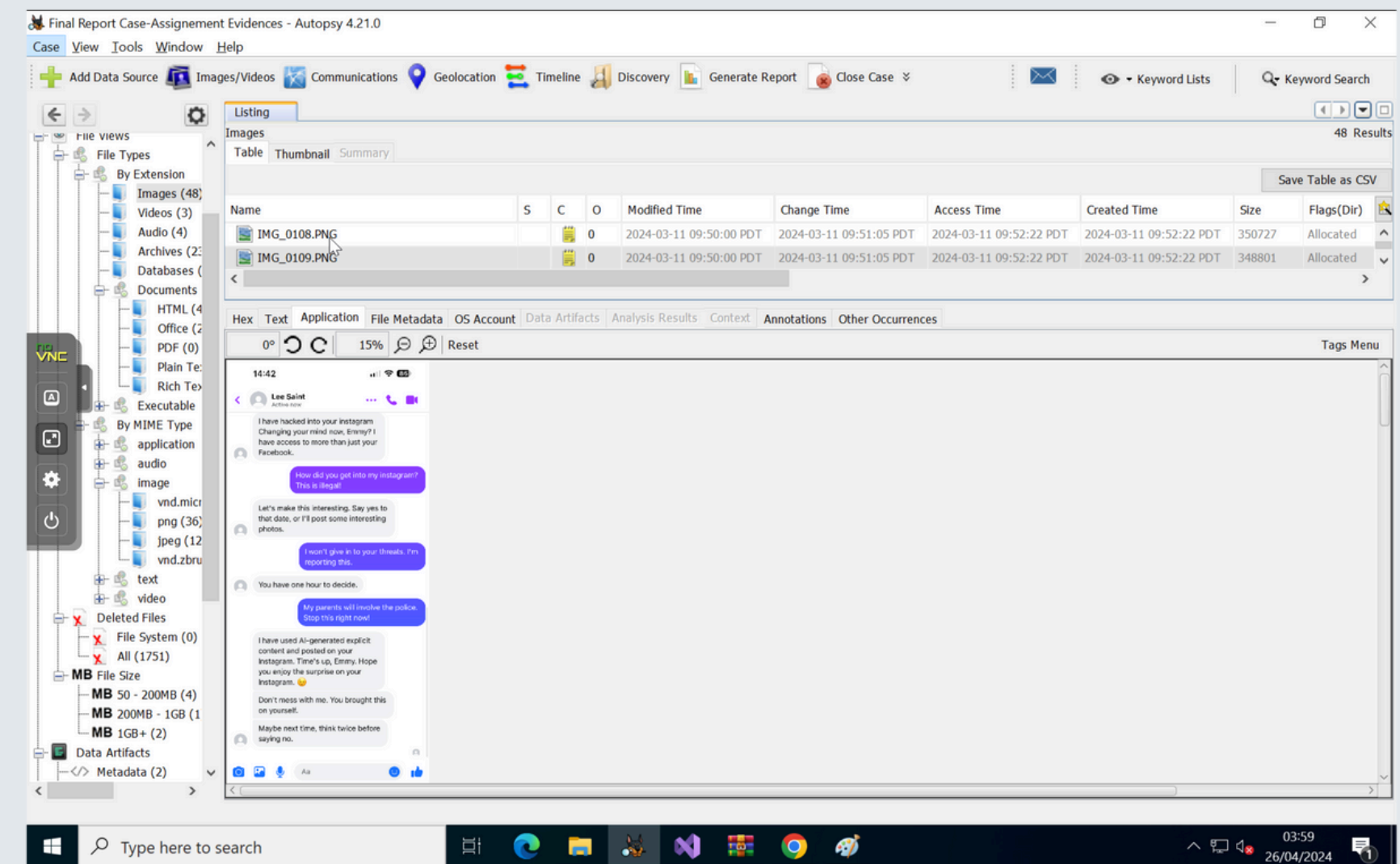
Locking the drive

Gathering Evidences

Using Autopsy and Microsoft Visual Studio

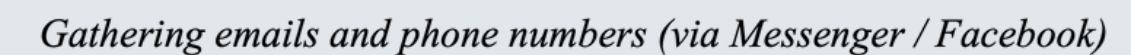


Threats by Justine Elias



AI Threatening. Hacked accounts on several platforms.

Using Autopsy and Microsoft Visual Studio



Resolving this case

Police report encrypted found in the disk image



EDR POLICE, UNITED KINGDOM
SN20 NAX, Liverpool, England, United Kingdom

info@edrpolicy.uk
016-514698, 016-452589
CASE NUMBER: CS-032949

Complainant
Lucy Alden
19/05/1996
20 Astra Street, Liverpool, Uk
0725854682
Alden.astra@gmail.com

Details of Case
20/04/2021 – 10:32pm UK Time
Cyberbullying: [Threats, Harassment,]
Platform/Method Used: [Twitter, Instagram]
Engaging in illicit activities on social media, ultimately leading to a campaign of harassment against Emily and her family.

Suspects Details
Name: Justine Elias
AKA: [Egos_dark]
69 Lone Street, Wine street, Liverpool, UK
elias.J@gmail.com
0706064908

Screenshots of offensive messages and social posts.
URL below is a link to all evidence files about the crime.
<https://shorturl.at/anF89>

Witness Information:
Jessy Orio
Graceland avenue, Liverpool

Action Taken by Complainant:
Complainant tried to cut off communication with the suspect by blocking the suspects on all social media platform, but suspects continued stalking her by opening new fake accounts.

Law Enforcement Action:
The security apprehended the suspects, and an investigation was conducted on the suspects online activities, after the investigation, the suspects plead to the case and was issued a restraining order after paying a fine £2,000.

Investigating Officer:
ISP Danzel Alfred
Badge/ID Number: PS-09102012
Contact Information:
Phone: 0731235689
Email: denzel.A@officer.MSpolice.uk

Live Demo : Decrypting police Report

VIDEO LINK : https://www.canva.com/design/DAGDttDZ2Pc/zbQ6aXoWIGMRWoJpeuwqmQ/view?utm_content=DAGDttDZ2Pc&utm_campaign=designshare&utm_medium=link&utm_source=editor

The screenshot displays the Proxmox Virtual Environment (VE) interface. On the left, the 'Server View' sidebar shows a list of virtual machines under the 'Proxmox-Solaris-2' node. The VM '106 (WindowsServerForensic)' is selected. The main console area shows the Windows desktop environment. A 'Police Report.rar (evaluation copy)' window is open, displaying a list of files extracted from the RAR archive. The files are:

Name	Size	Packed	Type	Modified	CRC32
File folder					
e.PoliceR...	1,009	948,576	File	24/11/20...	4255...
e.PoliceR...	711,680	659,136	File	24/11/20...	4880...

The bottom of the interface shows the 'Tasks' tab with a table of recent operations:

Start Time	End Time	Node	User name	Description	Status
Apr 29 10:04:46		Proxmox-VE	root@pam	VM/CT 106 - Console	
Feb 05 11:31:19		Proxmox-VE	root@pam	Shell	
Feb 12 17:20:51		Proxmox-VE	root@pam	Shell	
Apr 29 06:56:03	Apr 29 06:56:06	Proxmox-VE	root@pam	Update package database	OK
Apr 29 05:39:10	Apr 29 05:54:12	Proxmox-VE	root@pam	VM/CT 106 - Console	OK

Conclusion

Resources used for this report

Web, Youtube, Books

- Micode, French computer genius, investigating on hard drive and internet identity : <https://www.youtube.com/@Micode/videos>
- - Kruse II, Warren G., and Jay G. Heiser. *_Computer Forensics: Incident Response Essentials_*. Addison-Wesley, 2002.
- - Casey, Eoghan. *_Digital Evidence and Computer Crime_*. Academic Press, 2004.
- - ABC News. "BTK serial killer's daughter: 'We were living our normal life. ... Then everything upended on us'". ABC News, 22 January 2019.
- Dooley, Sean. "The Capture of Serial Killer Dennis Rader, BTK." *_Psychology Today_*, 17 March 2023.
- Operation Pacifier : [https://en.wikipedia.org/wiki/Playpen_\(website\)](https://en.wikipedia.org/wiki/Playpen_(website))
- <https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/>
- Chain of Custody, Wikipedia UK, https://en.wikipedia.org/wiki/Chain_of_custody
- Autopsy®, digital forensics software, <https://www.autopsy.com/download/>
- Windows Server 2022, Operating System, isolated in homelab for investigation, <https://www.microsoft.com/en-us/windows-server>
- PhotoRec, TestDisk https://www.cgsecurity.org/wiki/Main_Page