Erya Anom
Digital Forensic

Digital Forensics

Assessment 1

Outcomes covered: 1 and 2

Assessment instructions

You are required to produce short written answers based on a review of the case study scenario detailed below.

The short response answers are in two parts (in relation to outcomes 1 and 2), where you will be expected to carry out research and provide information on incident response procedures and how to manage digital evidence. Please provide your answers in the following assessment 1 pro forma.

The assessment is open book, however any resources that are used to answer questions must be suitably referenced at the end of the assessment. You must also take the necessary steps to ensure that any work being produced is your own.

Case study scenario

As part of a computer support team, you have been asked to conduct a forensic investigation of a PC within your company.

An employee of the company has come under suspicion of illegally downloading and sharing pirated software, movies and music using company computers. The employee has been suspended pending an investigation.

You are a qualified computing and ICT technician, however both you and the company is a little unsure of how to conduct a forensic investigation of a computer. Your company is also aware that there is the possibility of the investigation ending up in a court of law as the organisation whose software is being pirated has been alerted to the situation.

Consequently, the company has asked you to carry out research into conducting a forensic investigation of a PC and provide solutions as to the best approaches should the investigation become a police matter.

So far, you have been able to establish the following: the PC is switched on and connected to the company network but has been locked. There is a mouse and keyboard attached to the PC as well as a 1Tb storage drive. There is a USB pen drive, company mobile and desk diary in the desk drawer.

Erya Anom

Digital Forensic

In relation to the case study scenario, please consider the following questions.

Part 1 — Incident response procedures	**Completed/ Checked**
Q1. What should be considered when initially securing this crime scene? (100 words)	
Securing crime scene is first step crucial for criminal investigators, and it is involved a set of procedures purposes to protect an evidence and to make sure the digital evidence have to be protected from being changed or contaminated, or if the PC is off, any potential evidence can be lost that it's called forensically safe working environment that includes strict protocols and systems in place that to maintain the integrity of the evidence while investigators doing an examination and analysis. Such as physical drive and software as will be the crucial evidence. Additionally, using an investigation tools for data acquisition and analysis.	
Q2. What do you consider to be sources of digital evidence? (100 words)	
When collecting digital evidence, it's important to do so systematically. This includes devices like PCs, 1TB storage drives, USB pen drives, and company mobile phones. As an investigator, it's crucial to secure unauthorised access and confirm that the devices are operational to prevent data loss due to improper shutdown procedures. The general tasks an investigator needs to perform include identifying digital information that can be used as evidence, collecting, preserving and documenting evidence to provide a visual record of the system, analysing, identifying and organising evidence. Lastly, rebuilding evidence or repeating a situation to verify that the results can be reproduced reliably.	

Erya Anom

Digital Forensic

Q3. Name at least two methods that can be used to securely record actions whilst recording evidence? (100 words)	
Firstly, to record actions, take video recordings or photographs of the area around PC, including close up shots. Keep a journal to document activities and updated it as it processes the scene, including the date and time, as this is an important task to improve the performance of the investigations. Secondly, Forensic Collection Logbook to track every piece of the evidence from the moment it is collected. Including information on who information collected it and how it was stored or transferred. This is to make sure that an integrity of the evidence and confirm its authenticity throughout the investigation.	
Q4. Why do you think it is important to securely record evidence? (100 words)	
Evidence must be identified, collected, secured and maintained correctly. Recording evidence securely is important in terms of its integrity and reliability in legal proceedings. Investigations protect identity and safety, minimise the risk of contamination and preserve the authenticity of the evidence. For instance, the image is currently on but locked. Any steps taken to access it must be securely documented before proceeding. Ensuring that any actions are taken and the evidence is recorded and reported while preserving the evidence is crucial. In conclusion, secure evidence recording is fundamental to the justice system as it ensures that the truth can be established and that justice can be effectively served.	
Q5. What is meant by ‘chain of custody’ and how can you ensure that chain of custody is being implemented? (150 words)	

Erya Anom

Digital Forensic

The process of keeping track of evidence from the moment it is being collected until its presented in court is called Chain of Custody. This is helps make sure that the evidence remains unchanged and reliable for potential legal proceedings. For example, based on the image's investigation. It's important to maintain the chain of custody because it provides a clear record of how evidence such as files from locked PC/data on the USB pen drive was collected, preserved and accessed. For example, of chain of custody been implemented was document everything such as created log detailing each piece of evidence (PC, USB pen drive, mobile phone). Furthermore, control access, keep the evidence in secure location, limiting access to authority personal only and require sign in/out records, lastly, use evidence bags or containers, store items securely in tamper proof containers and label them properly. This is potential legal actions for an investigator.	
Q6. Name at least two current items of legislation that play an important role in the digital forensics process. (50 words)	
The Computer Misuse Act 1990 deals with unauthorised entry into computer system and data. Its important role when dealing with illegal download and sharing content. Data Protection Act 2018 the handling of personal data and ensures the safety of any evidence collection. Its respects privacy rights of users during forensics investigations. Both of acts are crucial in set up a legal framework when handling evidence from employee's PC.	
Q7. What is meant by the term 'forensically safe working environments'? (150 words)	
This means during an investigation, it ensures that digital evidence is protected from being changed, contaminated or lost. It includes strict protocols and systems in place to maintain the integrity of the evidence while allowing for a thorough examination	

and analysis. For example, based on the scenario and images. Including, restricted access, documented protocols and using a forensic tool that very crucial role. Maintaining the details record of all action taken, controlling access to the computer and any connected with the evidence such as USB, any devices that could be important evidence. Only authority individuals handle with the equipment protocols. Lastly, using a reputable forensic tool that not any modify with the original data of the collected evidence. This concept is not just technically but also fundamental aspect based on of conducting a comprehensive and credible, and following standard procedure and make sure every steps transparency during investigation's and can be reviewed by others.	
Q8. What is meant by the term 'forensic acquisition' and why is it important in the digital forensics process? (150 words)	
Forensic acquisition is how data is being collected, using methods such as surveys or gathering data by asking quest to certain of group, or observing the environment of the crime scene. For example, evidence is purpose for data integrity was collected by creating bit for bit copy of the PC's storage and any devices that are attached, such as USB pen drive. Furthermore, the employee's PC is turned on and locked. This has potential data loss or remote access, and acquiring data promptly helps safeguards it from being tampered with intentionally and accidently. Lastly, advanced facilitating further investigation, with a completed forensic image, allows the investigator to analyse and test against the data without further interacting with original evidence. In conclusion, forensic acquisition is a foundational step in digital forensics that maximise the reliability and admissibility of the evidence. This case's legal implications must involve the suspected illegal downloading and sharing of pirated content.	
Q9. Briefly describe some of the current tools and techniques used for obtaining digital evidence. (150 words)	
To begin with, many computer forensics tools vendors have developed that run for Windows to help improve the performance of digital evidence, such as FTK Forensic toolkit. This feature is beneficial for forensic investigation and provides data carving, imaging and extensive report generation features. The techniques gain performance, such as data collection by creating a forensic image, using disk imaging tools to create a detailed, written blocked image of the storage drive, and any removable media (like the USB	

drive). This image should be stored on a secure drive to maintain integrity. Lastly, capture volatile data, and if possible, use tools to capture the concepts of RAM before shutting down the PC to preserve any running processes or logged-in sessions. Analysis file system analysis uses forensic software to analyse the storage drive, focusing on file types associated with media and software piracy, such as media formats.	
Q10. What is meant by system, volatile and non-volatile information? (150 words)	
Volatile data is information that is lost when a device is turned off. It is crucial to capture this data during a forensic investigation, including data stored in RAM, active network connections, and running processes. Volatile data provides real-time insights into activities, but it is temporary. On the other hand, non-volatile data remains intact even when the device is powered down. This includes hard drives, USB drives, and other storage media for storing files, logs, and software installations. This encompasses files stored on the hard drive or USB drive and any logs or installed software that could provide evidence of pirated content activities. For instance, if the PC in question is on but locked and the RAM contents such as currently running applications and open documents, are considered volatile. This information could reveal recent activities related to pirated content's alleged downloading or sharing.	
Q11. Besides physical hardware, what other sources would you consider for forensic data analysis? (100 words)	
It is crucial to have multiple sources, such as software and mobile devices, for conducting forensic data analysis in cases involving potential illegal downloading and sharing of pirated content or related activities. Operating systems and applications often store details about software usage, including installation dates, last access time, and updates, which may indicate unauthorised usage. Furthermore, network logs and cloud storage may contain uploaded files or backup data, revealing previously deleted files or logs	

related to the suspected activities if the company has backup systems. Email accounts and browser cache, as well as cookies stored by web browsers, can provide information about recent site visits, search queries, and downloaded files, offering insight into the employee's online activities.	

References:

Phillips, N. and Enfinger, S. (2009). Guide to computer forensics and investigations. Clifton Park, N.Y.: Delmar ; Andover.
Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.

Assessment 2

Outcome covered: 3

Assessment instructions

In this assessment you are required to consider the output of your findings from assessment 1 (parts 1 and 2) and how you can use this information as a basis for a forensic report to your company and possibly a court of law.

Your report should follow a standard formal report format and include a title page, author, headings, appropriate line spacing, fonts, page numbers, introduction and conclusion/recommendations. You may also want to consider using tables to format the layout of your information.

The assessment is open book, however any resources that are used to answer questions must be suitably referenced at the end of the assessment. You must also take the necessary steps to ensure that any work being produced is your own.

Erya Anom

Digital Forensic

You should consider the following within your report.

- Details and qualifications of the forensic examiner(s)
- Background to the investigation
- Initial questions about the crime scene
- Scene description and how it was secured
- Inventory of devices
- Sources of evidence
- How evidence was gathered securely and stored
- Details of the forensically safe environment
- Any forensic analysis performed, and tools used
- Forensic analysis output and findings

You should finalise your report with any recommendations that you have for the company.

Erya Anom

Digital Forensic

Pro-Forma for Forensics Report

Forensics Report

Requested by:	Investigator details	
Paul Holmes	Name	Erya Puput Anom
	Position	IT Technician Forensic Investigation
	Telephone	075-198-1090
	Employment Duration	2 years
	Qualifications	B.Eng. Cybersecurity/ Forensic Computer Analyst

Background

As part of the computer support team at Motherwell Technology Ltd. It's had been tasked with conducting a forensic investigation on a company owned pc attributed to an employee under suspicion of illegally downloading and sharing pirated software. Additionally, it had the outcomes may have legal implications for both the employee and organisation. Additionally, the investigation was prompting, and it is indicating unusual network activity arising from the suspect's workstation. Leading management to believe that the employee might being engaging in unauthorised download and sharing or distribution copyrighted materials.

Examiner Details

Erya Anom

Digital Forensic

Name	Erya Puput Anom	Investigation Number	2024-56789
Position	Digital Forensic Investigation	Time	10:30 AM
Telephone	075-198-1090	Location	Motherwell Technology Ltd/ North Lanarkshire
Email	eryaanom@motherwell.ac.uk	Witness	Jennifer Thomson

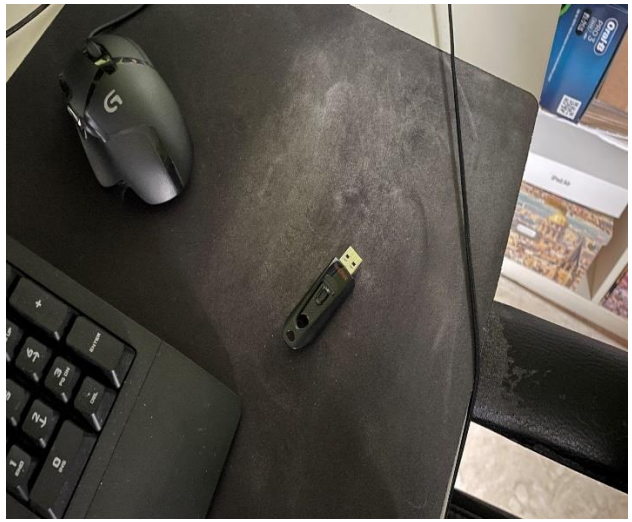
Initial Questions
1. What is the date and time of the investigation? 2. Who is conducting the investigation? 3. What is the current status of the PC ? (switching on, locked and connected to the network) 4. What is additional and storage devices are connected to the PC? 5. What are specific allegations against the employee? 6. What steps had been taken to secure the scene and preserve the evidence? 7. What tools and methods will be used to collect and analysis the digital forensic? 8. Are there any legal consideration or permission required for the investigation?

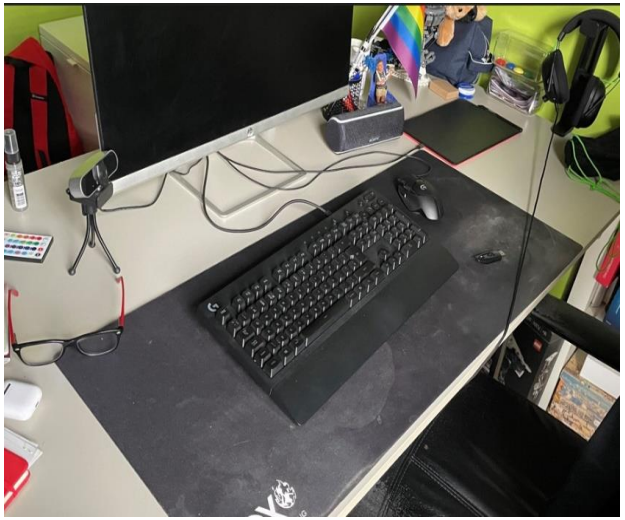
Scene Description
The PC is switched on and connected to the company's network. However, it is locked, that indicating the access to the operating systems is restricted without the proper user credentials. This presents a challenging system for determining the nature of the files and activities conducted by the user. Attached to the

Erya Anom

Digital Forensic

PC are a mouse, keyboard, camera, speaker and earphone. Which will allow for physical interaction once access is gained. In contrast, there is a 1TB USB drive connected to the PC. Accessing this drive for any illicit content is crucial, as it may contain downloaded files that are central to the investigation. the company also has a mobile phone and desk diary from the employee. That increased potentially containing additional evidence or context regarding the suspected activities.





Inventory List	Sources of evidence

Erya Anom

Digital Forensic

- PC UNIT; Status is powered on, network connection that connected to the company network, lock status is locked that need requires password to access. - Mouse - Keyboard - External Storage; 1TB and USB Pen Drive - Camera - Air pods - Remote - Speaker - Earphone - Desktop - Books - Passport - iPad	PC Unit External Storage; 1TB and USB Pen Drive Camera Company Mobile Phone Desktop iPad

Erya Anom

Digital Forensic

Contemporaneous Notes
To begin with, I arrived to the crime scene location date and Time: Friday, 4th October 2024, 10.30 am Location: Motherwell Technology Ltd Actions Taken: 1. I have arrived at the scene. And observing the location, and room that make sure nothing contamination. Observed the PC Unit and any related devices such as 1TB Storage and USB Pen Drive. 2. using an equipment that make sure there nothing contamination and transfer the fingerprint. 3. starting with using forensic software to create a bit by bit copy of the hard drive 4 taken photograph and videos of the room and around the crime scene, make sure taken photograph of the PC Unit, USB pen drive, any devices that related to devices. 5. the PC Unit contain several suspicious files 6. external hard drives appeared to contain backups of the PC’s data.

Chain of Custody Process

Erya Anom

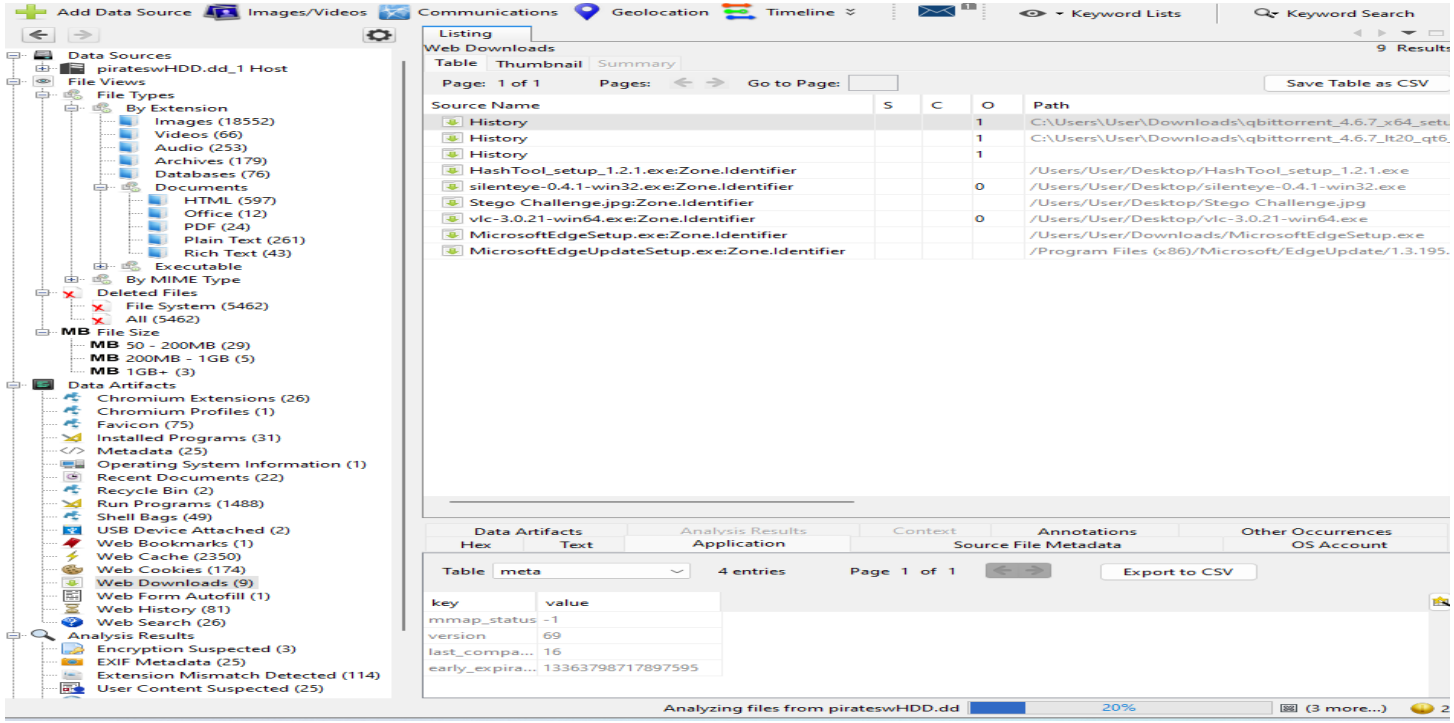
Digital Forensic

Timeline of Action Taken:

Date and Time: Friday, 4th October 2024, 10.30 am
Location: Motherwell Technology Ltd

10.30 am arrived the crime scene. Finding evidence collection: PC Unit, PC was switched on but locked on, 1TB storage and USB Pen drive

10.40 am evidence examination using Forensic Tools Software (Autopsy) Actions Taken: verified the integrity of the image, videos, any files or data that downloading and sharing illegally and analysis the files for relevant data. Finding: 18552 images, 66 videos, 253 audios, illegally web download and any recovered sensitive information



Forensic Tools Used

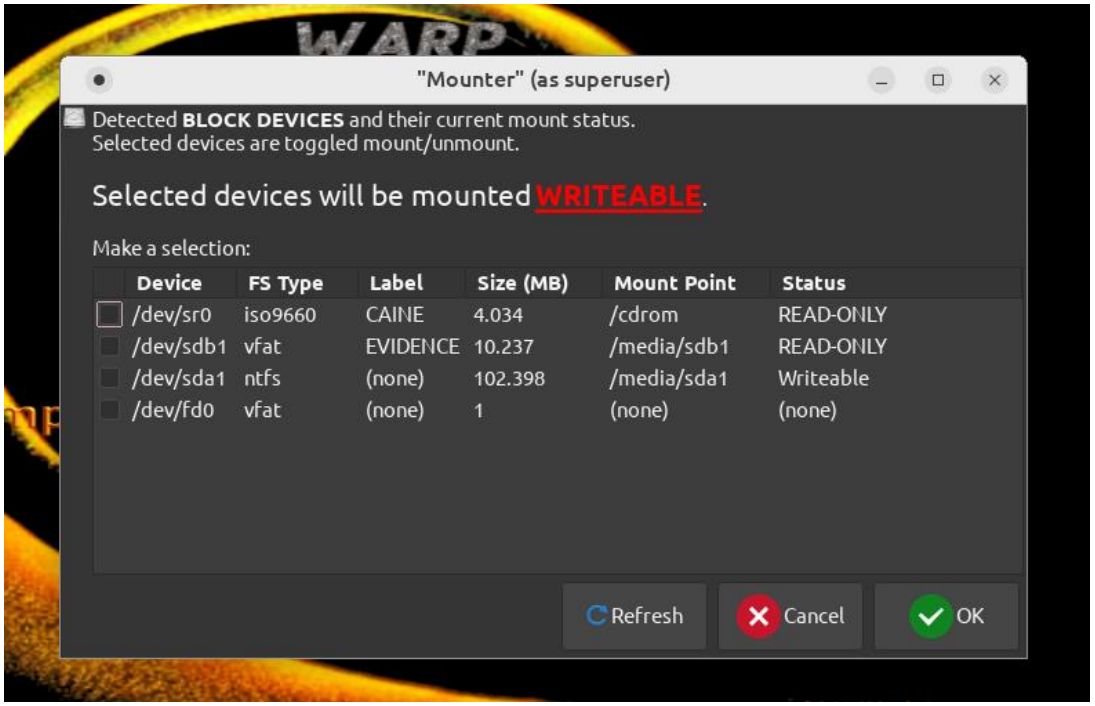
Erya Anom

Digital Forensic

Autopsy
Virtual Box (CAIN)
Photograph and Videography
Documentation such as notes

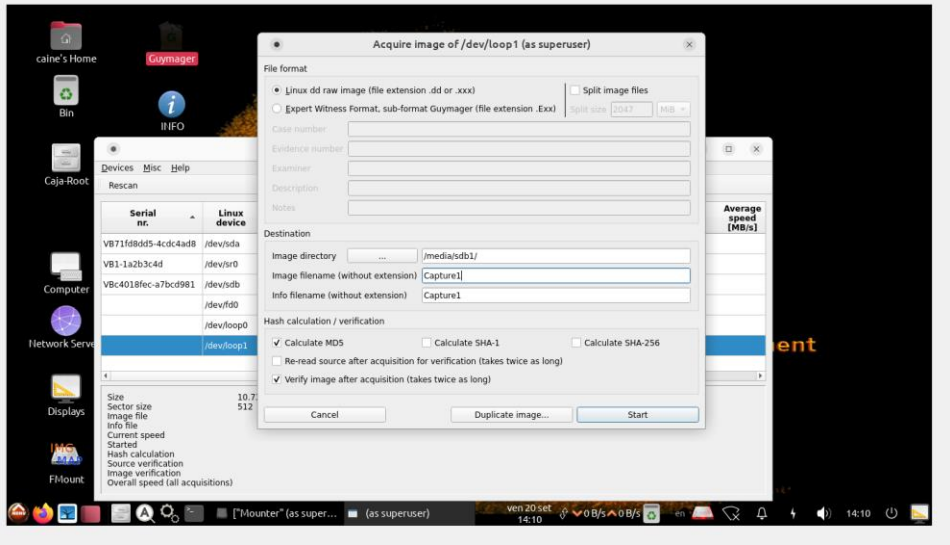
Forensic acquisition and analysis
using a virtual box (CAIN) to identification all potential sources of digital evidence in PC Computer and any related devices. And make sure that the original data is preserved without alteration, that often involves creating bit by bit of forensic images of the storage data. Documentation every evidence by using

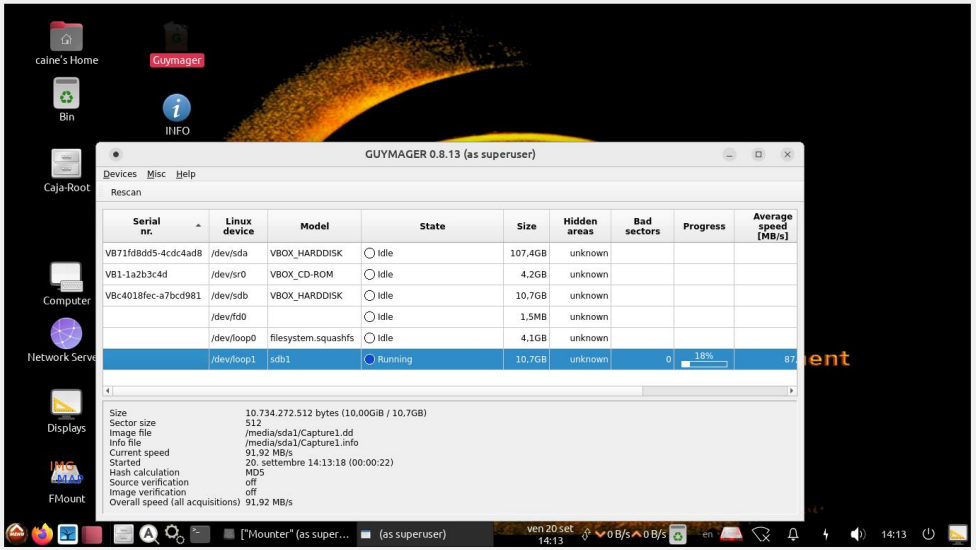
photograph and videography as taken action and takes a notes. The acquisition use a specific forensic tools such as CAIN, Autopsy to created image of the data. This image an exact copy of the original data.

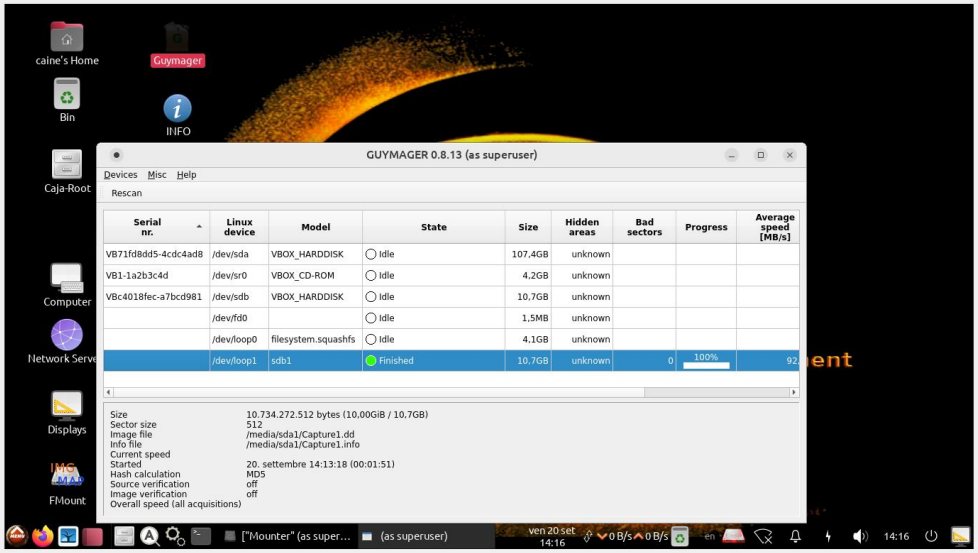


Erya Anom

Digital Forensic







Erya Anom

Digital Forensic

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Keyword Lists | Keyword Search

- Data Sources
  - piratesWHDD.dd_1 Host
- File Views
  - File Types
    - By Extension
      - Images (18552)
      - Videos (66)
      - Audio (253)
      - Archives (179)
      - Databases (76)
      - Documents
        - HTML (597)
        - Office (12)
        - PDF (24)
        - Plain Text (261)
        - Rich Text (43)
      - Executable
    - By MIME Type
  - Deleted Files
    - File System (5462)
    - All (5462)
  - MB File Size
    - MB 50 - 200MB (29)
    - MB 200MB - 1GB (5)
    - MB 1GB+ (3)
- Data Artifacts
- Analysis Results
- OS Accounts
- Tags
- Score
  - Bad Items (0)
  - Suspicious Items (123)
- Reports

Listing

Office — 12 Results

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time
MsolrmProtector.xls				2015-07-10 12:00:01 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:01 BST
MsolrmProtector.doc				2015-07-10 12:00:27 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:27 BST
MsolrmProtector.ppt				2015-07-10 12:00:27 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:27 BST
MsolrmProtector.xls				2015-07-10 12:00:27 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:27 BST
MsolrmProtector.doc				2015-07-10 12:00:01 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:01 BST
MsolrmProtector.ppt				2015-07-10 12:00:01 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:01 BST
MsolrmProtector.xls				2015-07-10 12:00:01 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:01 BST
MsolrmProtector.doc				2015-07-10 12:00:27 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:27 BST
MsolrmProtector.ppt				2015-07-10 12:00:27 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:27 BST
MsolrmProtector.xls				2015-07-10 12:00:27 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:27 BST
MsolrmProtector.doc			0	2015-07-10 12:00:01 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:01 BST
MsolrmProtector.ppt			0	2015-07-10 12:00:01 BST	2024-09-09 18:28:38 BST	2015-07-10 12:00:01 BST

OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Hex | Text | Application | File Metadata

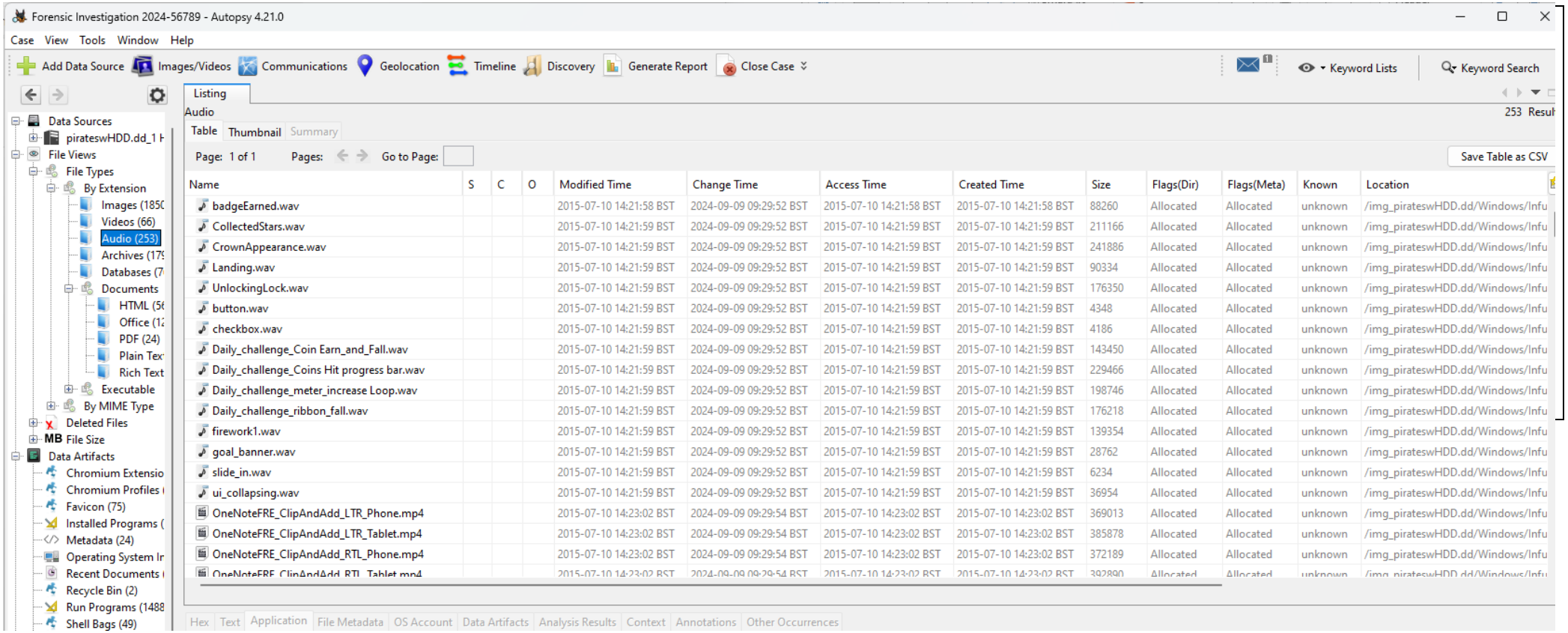
Strings | Extracted Text | Translation

Page: 1 of - Page | Matches on page: - of - Match | 100% | Reset

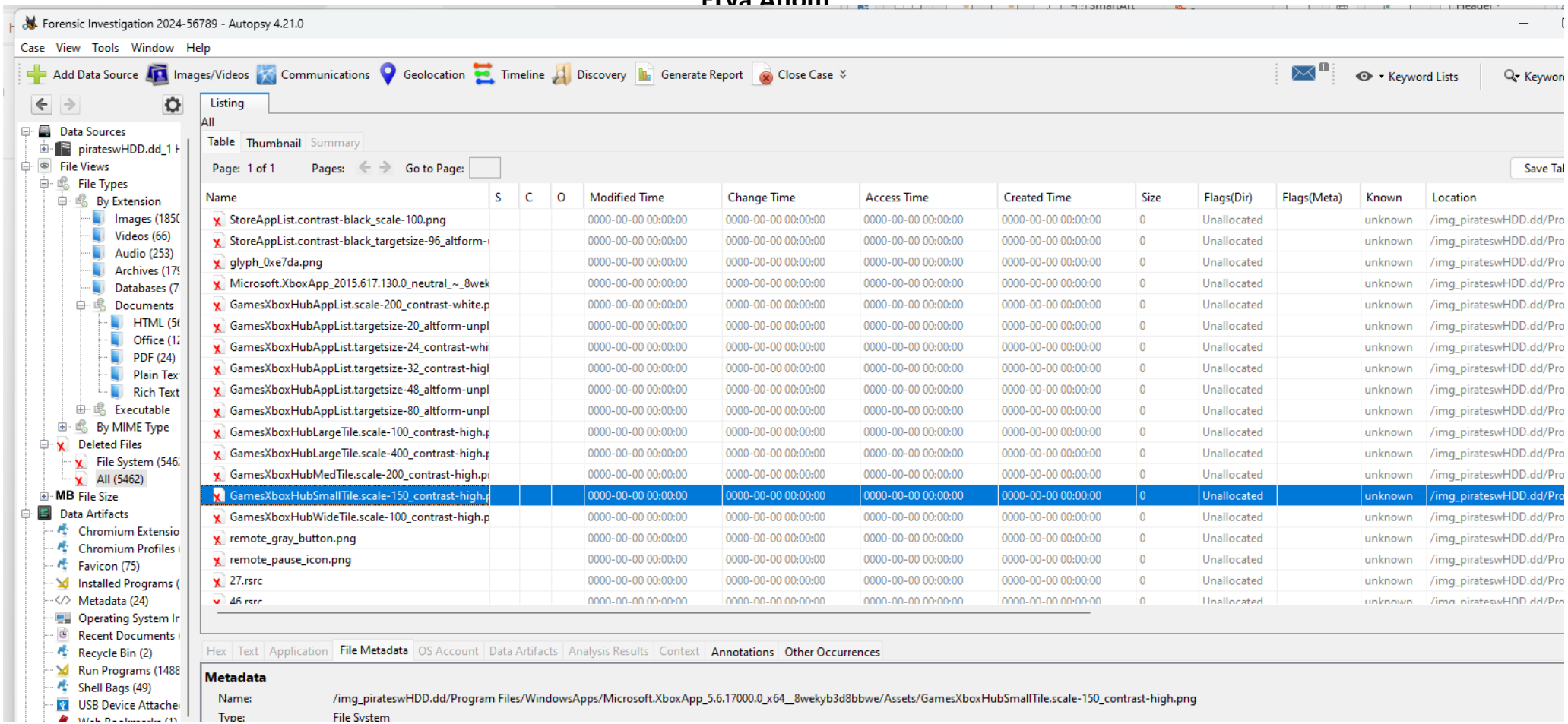
Text Source: File Text

Erya Anom

Digital Forensic



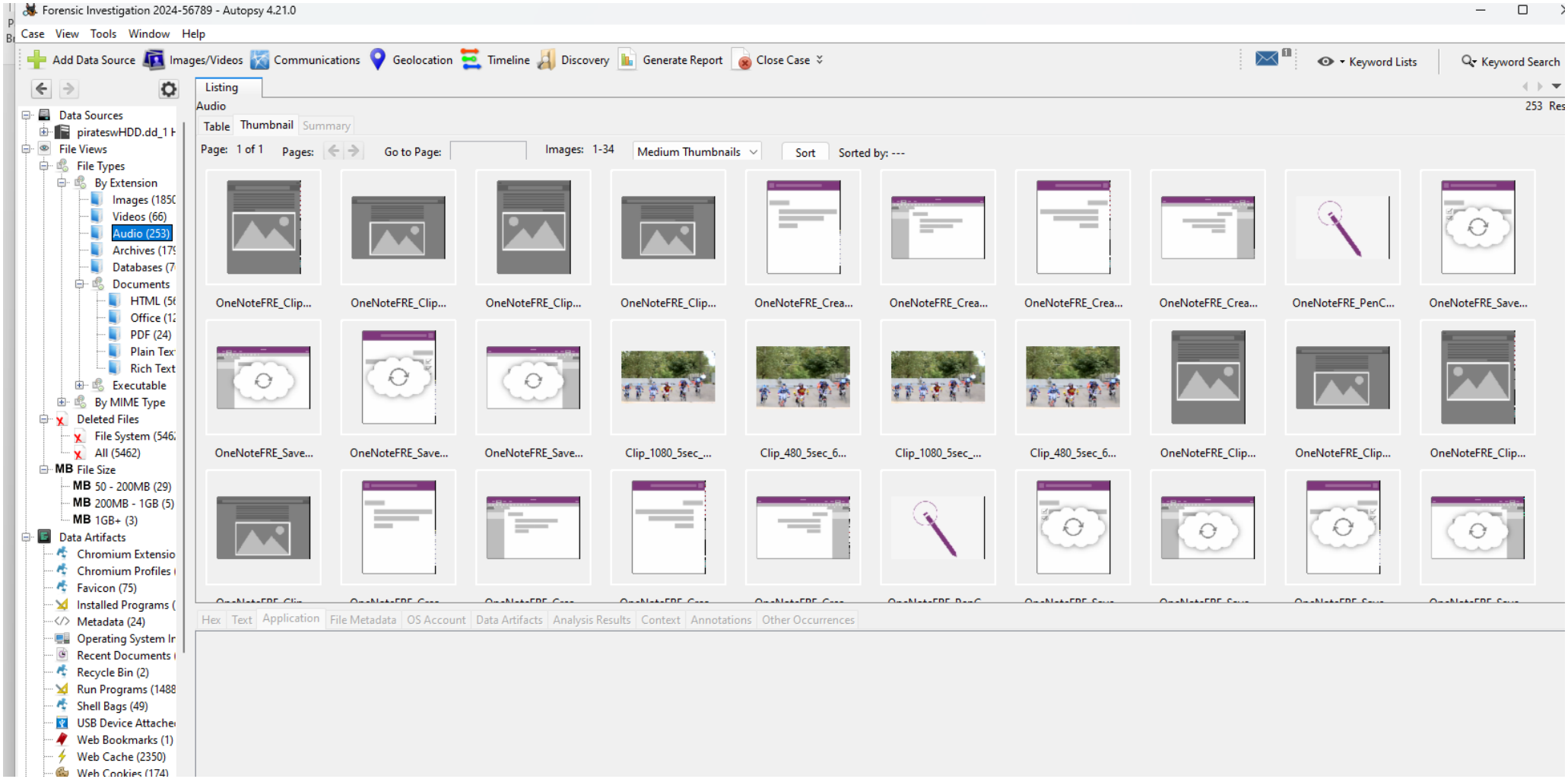
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
badgeEarned.wav				2015-07-10 14:21:58 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:58 BST	2015-07-10 14:21:58 BST	88260	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
CollectedStars.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	211166	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
CrownAppearance.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	241886	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
Landing.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	90334	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
UnlockingLock.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	176350	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
button.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	4348	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
checkbox.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	4186	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
Daily_challenge_Coin Earn_and_Fall.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	143450	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
Daily_challenge_Coins Hit progress bar.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	229466	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
Daily_challenge_meter_increase Loop.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	198746	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
Daily_challenge_ribbon_fall.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	176218	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
firework1.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	139354	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
goal_banner.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	28762	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
slide_in.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	6234	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
ui_collapsing.wav				2015-07-10 14:21:59 BST	2024-09-09 09:29:52 BST	2015-07-10 14:21:59 BST	2015-07-10 14:21:59 BST	36954	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
OneNoteFRE_ClipAndAdd_LTR_Phone.mp4				2015-07-10 14:23:02 BST	2024-09-09 09:29:54 BST	2015-07-10 14:23:02 BST	2015-07-10 14:23:02 BST	369013	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
OneNoteFRE_ClipAndAdd_LTR_Tablet.mp4				2015-07-10 14:23:02 BST	2024-09-09 09:29:54 BST	2015-07-10 14:23:02 BST	2015-07-10 14:23:02 BST	385878	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
OneNoteFRE_ClipAndAdd_RTL_Phone.mp4				2015-07-10 14:23:02 BST	2024-09-09 09:29:54 BST	2015-07-10 14:23:02 BST	2015-07-10 14:23:02 BST	372189	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu
OneNoteFRE_ClipAndAdd_RTL_Tablet.mp4				2015-07-10 14:23:02 BST	2024-09-09 09:29:54 BST	2015-07-10 14:23:02 BST	2015-07-10 14:23:02 BST	392890	Allocated	Allocated	unknown	/img_pirateswHDD.dd/Windows/Infu



Output and Findings
Finding a suspicious illegally downloading and sharing of software using autopsy and found suspicious items 123 files, and 5462 files had been deleted, internet history. In conclusion, these findings provide a comprehensive view of the suspects' illegally downloading and sharing activities.

Erya Anom

Digital Forensic



va Ar

al Fo

Forensic Investigation 2024-56789 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Keyword Lists | Keyword Search

Listing

Audio

253 Results

Table | Thumbnail | Summary

Page: 1 of 1 | Pages: | Go to Page: | Images: 1-34 | Medium Thumbnails

Sort | Sorted by: ---

OneNoteFRE_Clip... | OneNoteFRE_Clip... | OneNoteFRE_Clip... | OneNoteFRE_Clip...

OneNoteFRE_Crea... | OneNoteFRE_Crea... | OneNoteFRE_Crea... | OneNoteFRE_Crea...

OneNoteFRE_PenC... | OneNoteFRE_Save... | OneNoteFRE_Save... | OneNoteFRE_Save...

OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Hex | Text | Application | File Metadata

- Data Sources
  - piratesWHDD.dd_1 Host
- File Views
  - File Types
    - By Extension
      - Images (18552)
      - Videos (66)
      - Audio (253)
      - Archives (179)
      - Databases (76)
      - Documents
        - HTML (597)
        - Office (12)
        - PDF (24)
        - Plain Text (261)
        - Rich Text (43)
      - Executable
    - By MIME Type
  - Deleted Files
    - File System (5462)
    - All (5462)
  - MB File Size
    - MB 50 - 200MB (29)
    - MB 200MB - 1GB (5)
    - MB 1GB+ (3)
- Data Artifacts
  - Chromium Extensions (26)
  - Chromium Profiles (1)
  - Favicon (75)
  - Installed Programs (31)
  - Metadata (25)
  - Operating System Information (1)
  - Recent Documents (22)
  - Recycle Bin (2)
  - Run Programs (1488)
  - Shell Bags (49)
  - USB Device Attached (2)
  - Web Bookmarks (1)
  - Web Cache (2350)
  - Web Cookies (174)
  - Web Downloads (9)
  - Web Form Autofill (1)
  - Web History (81)
  - Web Search (26)
- Analysis Results
  - Encryption Suspected (3)
  - EXIF Metadata (25)
  - Extension Mismatch Detected (114)
  - User Content Suspected (25)

Forensic Investigation 2024-56789 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Keyword Lists | Keyword Search

Listing

Databases

76 Results

Table | Thumbnail | Summary

Page: 1 of 1 | Pages: | Go to Page: | Save Table as CSV

Name	S	C	O	Modified Time	Change Time
resource.db				2015-07-10 12:00:07 BST	2024-09-09 09:39:37 E
AgAppLaunch.db				2024-09-09 09:30:22 BST	2024-09-20 15:25:02 E
AgCx_SC4.db				2024-09-20 13:32:14 BST	2024-09-20 15:25:02 E
AgGlFaultHistory.db				2024-09-20 15:26:46 BST	2024-09-20 15:25:02 E
AgGlFgAppHistory.db				2024-09-20 15:26:46 BST	2024-09-20 15:25:02 E
AgGlGlobalHistory.db				2024-09-20 15:26:46 BST	2024-09-20 15:25:02 E
AgGlUAD_P_S-1-5-21-737214921-86318431-401185E				2024-09-20 15:19:52 BST	2024-09-20 15:25:02 E
AgGlUAD_S-1-5-21-737214921-86318431-40118584E				2024-09-20 15:19:52 BST	2024-09-20 15:25:02 E
AgRobust.db				2024-09-20 15:26:46 BST	2024-09-20 15:25:02 E
cversions.3.db				2024-09-09 09:36:06 BST	2024-09-09 09:36:06 E
{17A6A947-B905-4D30-88C9-B63C603DA134}.3.ver0				2024-09-09 09:36:06 BST	2024-09-09 09:36:06 E
resource.db				2015-07-10 12:00:07 BST	2024-09-09 09:39:37 E
resource.db				2015-07-10 12:00:07 BST	2024-09-09 09:39:37 E
cversions.2.db			0	2015-07-10 13:21:43 BST	2024-09-09 18:27:59 E
{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x			0	2015-07-10 13:21:43 BST	2024-09-09 18:27:59 E
{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0			0	2015-07-10 13:21:43 BST	2024-09-09 18:28:00 E
mpcache-26CA6CB0C0ECC266FCA0630EBB42E5DF			0	2024-09-20 14:31:56 BST	2024-09-20 14:31:56 E
mpenginedb.db			0	2024-09-20 15:25:21 BST	2024-09-20 15:25:21 E
IconCache.db			0	2024-09-20 15:26:45 BST	2024-09-20 15:26:45 E
cversions.1.db			0	2024-09-09 09:35:16 BST	2024-09-09 09:35:16 E
cversions.3.db			0	2024-09-09 09:36:03 BST	2024-09-09 09:36:03 E
{384756BA-B905-4D30-88C9-B63C603DA134}.3.ver0			0	2024-09-09 09:36:07 BST	2024-09-09 09:36:07 E
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.1.ver0			0	2024-09-20 12:49:51 BST	2024-09-20 12:49:51 E
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.1.ver0			0	2024-09-20 14:35:43 BST	2024-09-20 14:35:43 E

OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Hex | Text | Application | File Metadata

Page: 1 of 17 | Page | Go to Page: 1 | Jump to Offset | Launch in H

```
0x00000000: 47 52 45 53  1D D2 62 14   66 01 00 00   00 00 00 00   GRES..b.f.......
0x00000010: 01 00 00 00  01 00 01 00   02 00 01 00   03 00 01 00   ................
0x00000020: 04 00 01 00  05 00 01 00   06 00 01 00   07 00 01 00   ................
0x00000030: 08 00 01 00  09 00 01 00   0A 00 01 00   0B 00 01 00   ................
0x00000040: 0C 00 01 00  0D 00 01 00   0E 00 01 00   0F 00 01 00   ................
0x00000050: 10 00 01 00  11 00 01 00   12 00 01 00   13 00 01 00   ................
0x00000060: 14 00 01 00  15 00 01 00   16 00 01 00   17 00 01 00   ................
0x00000070: 19 00 01 00  1A 00 01 00   1B 00 01 00   1C 00 01 00   ................
0x00000080: 1D 00 01 00  1E 00 01 00   1F 00 01 00   20 00 01 00   ............ ...
0x00000090: 21 00 01 00  22 00 01 00   23 00 01 00   24 00 01 00   !..."...#...$...
```

Forensic Investigation 2024-56789 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Keyword Lists | Keyword Search

- Data Sources
  - piratesWHDD.dd_1 Host
- File Views
  - File Types
    - By Extension
      - Images (18552)
      - Videos (66)
      - Audio (253)
      - Archives (179)
      - Databases (76)
      - Documents
        - HTML (597)
        - Office (12)
        - PDF (24)
        - Plain Text (261)
        - Rich Text (43)
      - Executable
    - By MIME Type
  - Deleted Files
    - File System (5462)
    - All (5462)
  - MB File Size
    - MB 50 - 200MB (29)
    - MB 200MB - 1GB (5)
    - MB 1GB+ (3)
- Data Artifacts
- Analysis Results
- OS Accounts
- Tags
- Score
  - Bad Items (0)
  - Suspicious Items (117)
- Reports

Listing

Suspicious Items — 115 Results

Table | Thumbnail | Summary

Page: 1 of 1 | Pages: | Go to Page: | Images: 1-19 | Medium Thumbnails

Sort | Sorted by: ---

Logo.png.DATA | LogoBeta.png.DATA | LogoCanary.png.... | LogoDev.png.DATA

SmallLogo.png.DATA | SmallLogoBeta.p... | SmallLogoCanary... | SmallLogoDev.pn...

RecoveryStore.{... | {98DBF9BD-7743-... | {98DBF9BE-7743-... | Logo.png.DATA

Hex | Text | Application | File Metadata

OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Forensic Investigation 2024-56789 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Keyword Lists | Keyword Search

- Data Sources
  - piratesw HDD.dd_1 Host
- File Views
  - File Types
    - By Extension
      - Images (18552)
      - Videos (66)
      - Audio (253)
      - Archives (179)
      - Databases (76)
      - Documents
        - HTML (597)
        - Office (12)
        - PDF (24)
        - Plain Text (261)
        - Rich Text (43)
      - Executable
    - By MIME Type
  - Deleted Files
    - File System (5462)
    - All (5462)
  - MB File Size
    - MB 50 - 200MB (29)
    - MB 200MB - 1GB (5)
    - MB 1GB+ (3)
- Data Artifacts
- Analysis Results
- OS Accounts
- Tags
- Score
  - Bad Items (0)
  - Suspicious Items (117)
- Reports

Listing

13 Results

Table | Thumbnail | Summary

Page: Pages: Go to Page: Save Table as CSV

Source Module Name	Report Name	Created Time	Report File Path
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:37 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:37 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Users/Default/NTUS...	2024-10-04 13:22:38 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Users/User/NTUSER....	2024-10-04 13:22:39 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/ServicePr...	2024-10-04 13:22:40 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/ServicePr...	2024-10-04 13:22:40 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Users/User/AppData...	2024-10-04 13:22:40 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:41 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:43 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:43 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:52 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:52 BST	Y:\30122856\Des
RecentActivity	RegRipper /img_piratesw HDD.dd/Windows/System32...	2024-10-04 13:22:53 BST	Y:\30122856\Des

Hex | Text | Application | File Metadata

OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Forensic Investigation 2024-56789 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Keyword Lists | Keyword Search

Discovery
Generate Report
Close Case

- Data Sources
  - piratesWHDD.dd_1 Host
- File Views
  - File Types
    - By Extension
      - Images (18552)
      - Videos (66)
      - Audio (253)
      - Archives (179)
      - Databases (76)
      - Documents
        - HTML (597)
        - Office (12)
        - PDF (24)
        - Plain Text (261)
        - Rich Text (43)
      - Executable
    - By MIME Type
  - Deleted Files
    - File System (5462)
    - All (5462)
  - MB File Size
    - MB 50 - 200MB (29)
    - MB 200MB - 1GB (5)
    - MB 1GB+ (3)
- Data Artifacts
- Analysis Results
- OS Accounts
- Tags
- Score
  - Bad Items (0)
  - Suspicious Items (117)
- Reports

Listing

Data Artifacts

Table | Thumbnail | Summary

Page: Pages: Go to Page:

Artifact Type	Child C
Chromium Extensions (26)	26
Chromium Profiles (1)	1
Favicon (75)	75
Installed Programs (31)	31
Metadata (25)	24
Operating System Information (1)	1
Recent Documents (22)	22
Recycle Bin (2)	2
Run Programs (1488)	1488
Shell Bags (49)	49
USB Device Attached (2)	2
Web Bookmarks (1)	1
Web Cache (2350)	2350
Web Cookies (174)	174
Web Downloads (9)	9
Web Form Autofill (1)	1
Web History (81)	81
Web Search (26)	26

Hex | Text | Application | File Metadata

OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Forensic Investigation 2024-56789 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Keyword Lists | Keyword Search

- Data Sources
  - piratesWHDD.dd_1 Host
- File Views
  - File Types
    - By Extension
      - Images (18552)
      - Videos (66)
      - Audio (253)
      - Archives (179)
      - Databases (76)
      - Documents
        - HTML (597)
        - Office (12)
        - PDF (24)
        - Plain Text (261)
        - Rich Text (43)
      - Executable
        - .exe (2515)
        - .dll (16848)
        - .bat (13)
        - .cmd (12)
        - .com (23)
    - By MIME Type
  - Deleted Files
    - File System (5462)
    - All (5462)
  - MB File Size
    - MB 50 - 200MB (29)
    - MB 200MB - 1GB (5)
    - MB 1GB+ (3)
- Data Artifacts
- Analysis Results
  - Encryption Suspected (8)
  - EXIF Metadata (25)
  - Extension Mismatch Detected (115)
  - User Content Suspected (25)
  - Web Categories (4)
- OS Accounts
- Tags
- Score
  - Bad Items (0)
  - Suspicious Items (123)
- Reports

Listing

Encryption Suspected — 8 Results

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

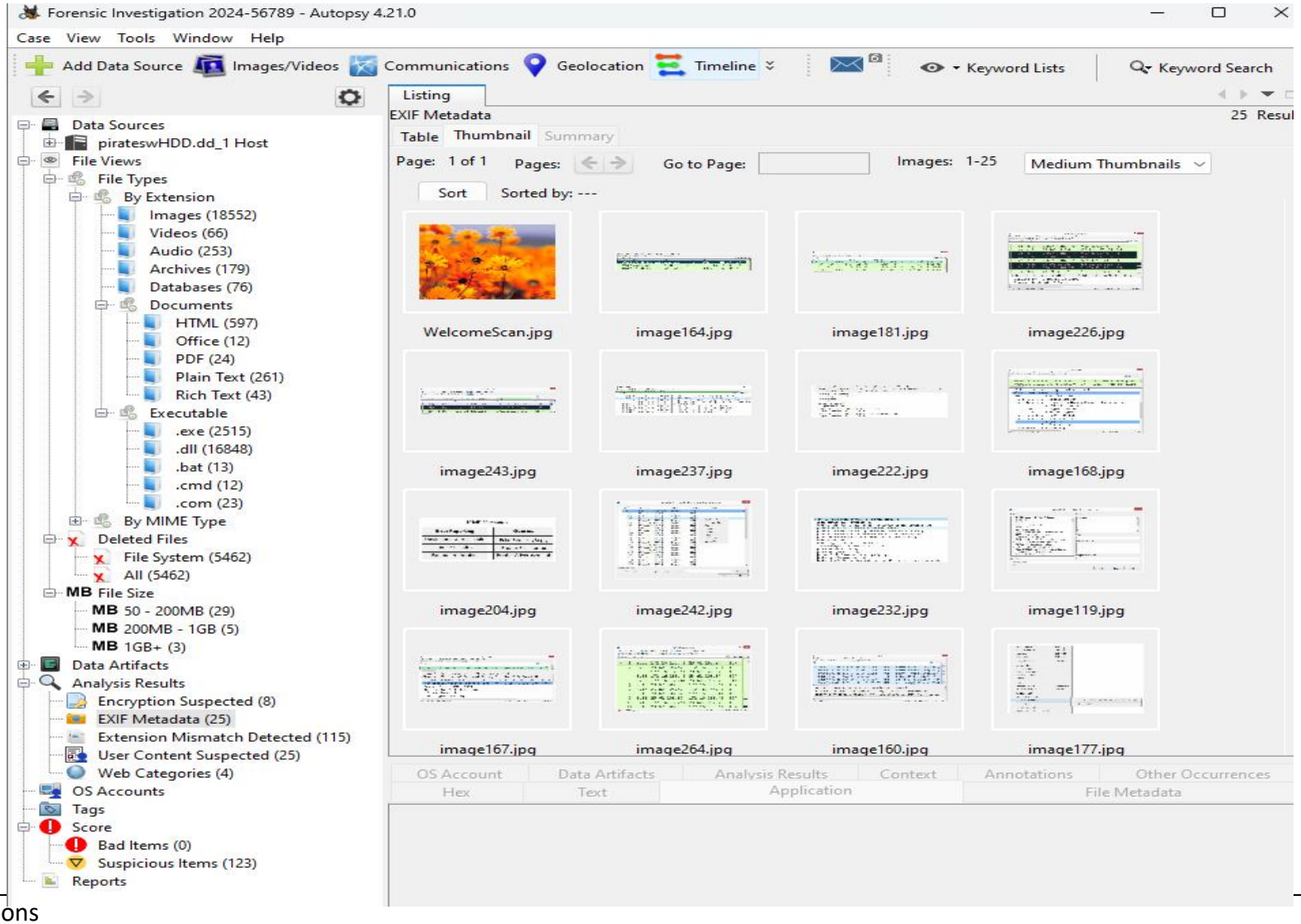
Source Name	S	C	O	Source Type	Score	Conclusion
events01.rbs-slack				File	Likely Notable	
mpenginedb.db			0	File	Likely Notable	
appdb.dat-slack				File	Likely Notable	
resource.db			0	File	Likely Notable	
AgGIFaultHistory.db			0	File	Likely Notable	
AgGIFgAppHistory.db			0	File	Likely Notable	
AgGIUAD_S-1-5-21-737214921-86318431-40118584			0	File	Likely Notable	
AgGIGlobalHistory.db			0	File	Likely Notable	

OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Hex | Text | Application | File Metadata

Strings | Extracted Text | Translation

Page: 1 of Page Go to Page: Script: Latin - Basic



Recommendations
Further investigation in these area will help to uncover unconditional evidence, and verify more the authenticity of current finding and provides more evidence to understanding more of the case. Areas further investigation such as deep analysis, network traffic, mobile phone and storage. And this is crucial maintain documentation and follow up for proper chain of custody procedures.

Erya Anom

Digital Forensic

Appendices (you should put images of the evidence found)

Phillips, N. and Enfinger, S. (2009). Guide to computer forensics and investigations. Clifton Park, N.Y.: Delmar ; Andover.
Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.