CASE STUDY ON SOCIAL MEDIA FORENSIC ANALYSIS

MINOR PROJECT REPORT

Submitted by

CHINTHAPALLI KARTHIK REDDY [RA2111030010081]

GURUGUBELLI KEERTHI [RA2111030010093]

M.E.V.S.AKHILVARMA [RA2111030010099]

Under the Guidance of

Dr. Thanga Revathi S

Associate Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING
with specialization in Cyber Security

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603203

APRIL 2024

COLLEGE OF ENGINEERING & TECHNOLOGY

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

S.R.M. NAGAR, KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that this project report **"Social Media Forensic Analysis"** is the bonafide work of **"C.KARTHIK REDDY,G.KEERTHI,M.E.V.S.AKHILVARMA"** of III Year/VI Sem B.tech(CSE) who carried out the mini project work under my supervision for the course 18CSE382T FORENSICS AND INCIDENCE RESPONSE in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE
Dr. Thanga Revathi S
Associate Professor
Networking And Communications

SIGNATURE
Dr. Annapurani K
Head of Department
Networking And Communications

Content Contribution Table

Name	Contribution
C.KARTHIK REDDY	Research & summarize
G.KEERTHI	Research & documentation
M.E.V.S.AKHILVARMA	Research & documentation

Problem statement

Case Study on the social media forensic analysis

Introduction

Social media forensics" collects evidence from social media sites such as Facebook, WhatsApp, Tik Tok, and Snapchat to identify criminals. “Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often associated with computer crime” . As technology continues to advance also, cyber-criminal cases continue to increase. Currently, 15% of social media users have encountered cybercrimes during their activities on various social. They continue to rise.

Hence, social media platforms majorly contain private and personal information; therefore, they tend to be hackers' targets to steal information and use it for criminal activities. Typical social media cyber-attacks include shopping scams, photo-morphing, link-baiting, cyberbullying, and hacking. Cybercriminals typically use cookies or denial of service (DoS) to steal; hence, they tend to be hackers' targets to steal information and personal information on social media platforms. Investigators use social media forensics tools such as WebPreserver, make a Website Hub, Pipl Search, TinEye, and TweetBeaver to investigate social media crimes.

Social media network

Social media network is a platform that creates virtual environment for social interactions among circle of friends and fans of like-minds. “Social media platforms are internet-based applications focused on broadcasting user-generated Content”.It deals with the sharing of information and multimedia content between users on similar platforms over electronic network especially the internet and cyberspace . This platform has geometrically grown to become not only an effective communication tool for personal and social use, but also an essential channel for businesses and official communication channels. There are thousands of social media platforms being used today for different purposes, few of them that are most popular are highlighted below.

- **Facebook** is an online social media platform that provides several services like social networking of friends and fans, online advertising, voice calls, instant messaging, video calls, video sharing and viewing, online market place, virtual gifts among both young and the old, private and corporate bodies. It was launched on February 4, 2004, by Mark Zuckerberg. It had over 1.18 billion monthly active users as of August 2015 and 3.049 billion active users in 2024 according to statistics by with an engagement of over 4 billion views of videos everyday on the network. About 2.14 billion people can be reached via advertising on Facebook .
- **WhatsApp** is a cross-platform internet-based instant messaging application that allows smart phone users to exchange text, image, video and audio messages for free provided the device has Internet access. It was developed in 2009 by Brian Acton and Jan Koum. WhatsApp became the most popular messaging app with about 2 billion active users as at april, 2024.
- **MySpace** is a social networking website offering an interactive, user-submitted network of friends, personal profiles, blogs, groups, photos, music and videos. It was the biggest social media platform up till 2008 when it was overtaken by Facebook. It was cofounded by Chris DeWolfe and Tom Anderson.
- **Twitter** is a social network platform that enables users to write and read short character messages called tweets. It revolves around the principle of followers who are equally users, who choose to follow another Twitter user and can thus view tweets sent by that user. Whereas unregistered users can read tweets, one must be registered to send tweets. It was founded in March, 2006 by Jack Dorsey .528.3 million active twitter users till April 2024
- **Instagram** allows users to upload media that can be edited with filters and organized by hashtags and geographical tagging. Posts can be shared publicly or with pre-approved followers. Users can browse other users' content by tags and locations and view trending content. Users can like photos and follow other users to add their content to a personal feed. Instagram has 1.38 billion active users with 500 million daily active users of Instagram stories, 1.16 billion people can be reached through adverts on Instagram.

- **YouTube** is a video sharing service that allows users to watch videos posted by other users and upload videos of their own. With the ubiquitous use of smart phones this platform has become the first choice in personal broadcasting and video sharing. It was cofounded by Chad Hurley, Steve Chen, and Jawed Karim in February 2005. In November 2006, it was bought by Google and now operated by Google.
- **LinkedIn** is a social media platform for professional networking. It is a social networking tool available to job seekers and professionals where users can invite other users and even non-users to connect. Inviters who get several rejections from invitees risk having their accounts restricted or closed. On this platform, users can get introduced to networks of contacts, new job and business opportunities, display products and services in their company profile pages, list job vacancies and search for potential candidates.
- **Skype** is an IP telephony service provider that can be used to make free voice and video calls over the Internet to any Skype subscriber or to any other non-user at low calling rates. It is relatively simple to download and install the software, which works on most computers and phones. A dedicated Skype phone can be used or desktop computers, notebooks, tablets, mobile phones and other mobile devices fitted with a headset, speakers, microphones or USB phone. Skype also enables file transfers, texting, video chat and videoconferencing.
- **Reddit** This social media platform enables you to submit content and later vote for the content. The voting determines whether the content moves up or down, which is ultimately organized based on the areas of interest (known as subreddits). Number of active users per month: 100 million approximately.

SNAPCHAT USER DATA LEAK (2021)

Timeline of Key Events

- May 10, 2021:
  - Reports surface indicating a potential data breach affecting Snapchat, with claims that the personal information of millions of users has been compromised.
- May 19, 2021:
  - A threat actor publicly announces they have obtained a large database of Snapchat user information, including usernames, email addresses, and phone numbers.
- May 20, 2021:
  - Snapchat acknowledges the data breach, confirming that a portion of its user data was indeed compromised. The company assures users that it is actively investigating the incident and working to enhance security measures.
- May 21, 2021:
  - Security experts analyze the leaked data and verify its authenticity, noting that the breach exposes sensitive information of approximately 500 million Snapchat users.
- May 25, 2021:
  - Snapchat releases an official statement detailing the extent of the data breach and apologizing to affected users for any inconvenience caused. The company advises users to remain vigilant and report any suspicious activity related to their accounts.
- June 1, 2021:
  - Law enforcement agencies launch an investigation into the Snapchat data breach, collaborating with cybersecurity firms to identify the perpetrators and assess the potential impact on affected users.
- July 10, 2021:
  - Snapchat announces the implementation of additional security measures to prevent future data breaches, including enhanced encryption protocols and regular security audits of its systems.

- August 5, 2021:
  - Privacy advocacy groups criticize Snapchat for its handling of the data breach, citing concerns about the company's data protection practices and urging regulators to hold it accountable for any lapses in security.
- September 20, 2021:
  - Snapchat faces lawsuits from affected users seeking damages for the unauthorized disclosure of their personal information. Legal proceedings begin as plaintiffs allege negligence and breach of privacy rights.
- November 12, 2021:
  - Snapchat reaches a settlement agreement with regulatory authorities and class-action plaintiffs, agreeing to pay fines and compensation to affected users. The company commits to strengthening its cybersecurity infrastructure and improving data protection measures to prevent future breaches.

How in 2021 attackers took advantage of Snapchat user data breach

ATTACK EXECUTION:

1. Identifying Vulnerabilities:
   - Attackers conducted comprehensive reconnaissance to identify weaknesses in Snapchat's infrastructure.
   - Techniques involved scanning for known vulnerabilities in web applications, network architecture, and third-party services utilized by Snapchat.
2. Exploiting Security Weaknesses:
   - Upon identifying vulnerabilities, attackers exploited them using techniques such as SQL injection, cross-site scripting (XSS), and exploiting misconfigurations in server settings.
   - These methods allowed attackers to bypass security controls and gain access to sensitive data stored on Snapchat's servers.

3. Gaining Access to User Data:
    - After initial access, attackers sought to escalate privileges and access databases containing user data.
    - This involved exploiting additional vulnerabilities or leveraging stolen credentials to gain administrative access to critical systems.
4. Exfiltrating User Data:
    - Once inside Snapchat's network, attackers exfiltrated user data by querying databases and extracting information from compromised servers.
    - Stolen data included usernames, email addresses, phone numbers, and other personal information stored in Snapchat's databases.
5. Covering Their Tracks:
    - To evade detection, attackers attempted to cover their tracks by deleting logs, manipulating timestamps, and utilizing anonymizing tools.
    - These actions hindered Snapchat's security team in tracing the source of the breach and identifying the attackers.
6. Publicizing the Breach:
    - Subsequently, attackers publicized the breach by leaking stolen information on underground forums or dark web marketplaces.
    - This aimed to maximize the impact of the breach and potentially monetize the stolen data by selling it to other malicious actors.
7. Conclusion:
    - The Snapchat user data leak of 2021 underscored the importance of robust cybersecurity measures and continuous vigilance in safeguarding user information. It served as a stark reminder for organizations to prioritize data security and invest in proactive measures to prevent future breaches.

TYPES OF SOCIAL MEDIA CRIMES

HACKING: Hacking refers to compromising technological devices such as computers and networks via illegal access to computer systems or an account . Hacking is not always criminal activity, but it is often defined as unlawful when it harms someone. The current most famous hackers are "white, dark, dim, and blue cap hackers" . White hat hackers assume a considerable part in contemporary society. A current instance of hacking is the hacking of the Twitter accounts of Jeff Bezos, Elon Musk and Bill gates . The hackers tweeted promising to double the Bitcoin so that people would surrender to the Bitcoin addresses posted.

PHOTO MORPHING: Photo morphing involves seamlessly altering one image into another using morphing tools available online . This practice is often used maliciously, especially targeting young girls whose images are downloaded from social sites and manipulated. These altered images may be used for extortion by threatening to distribute them publicly.

An example of photo morphing involved a case in India where an attacker morphed a local woman's face onto a nude photograph and circulated the doctored image on social media .

SHOPPING SCAMS: Shopping scams are a common form of internet fraud carried out by cybercriminals. These scams often involve criminals posing as legitimate online sellers on fake websites. Victims are lured into making purchases and are asked to pay via pre-loaded money cards or other online money transfer platforms. For example, Berrylook.com, a fraudulent website advertised on Facebook, has been reported for scamming customers who paid for items but never received them .

CYBERBULLYING: Cyberbullying refers to harassing and tormenting individuals using the internet, often for amusement or entertainment purposes. Even celebrities like actress Melanie Griffith have experienced cyberbullying, facing hateful tweets regarding their appearance or personal life. This form of online harassment can have serious consequences for victims' mental health and well-being, highlighting the importance of combatting cyberbullying through education and prevention efforts.Surgery and her general physical appearance. According to her interview, many people tweeted that she looked horrible.

LINK BAITING: Link Baiting is also another technique used by cybercriminals (Basumatary & Kalita, 2022). In this method, users are enticed into clicking on unsecured links that steal their personal and financial information. For example, scammers may use fraudulent links promising to direct users to forex trading sites, such as cryptocurrency platforms. Many victims have reported losing money from their bank accounts, and upon investigation, it was discovered that they had clicked on insecure links on their devices, leading to the theft of their personal information.

PROCEDURES OF SOCIAL MEDIA FORENSIC:

The increased rates of social media crimes have led to an increasing need for social network forensics. Social media forensics incorporates digital analysis and cyber investigation evaluation methods to collect, store, analyze, and preserve information that could be useful in courts of law in the event of criminal activity.

Determining the Crime Scene and Evidence Collection:

The first step of social media forensics is inspecting and determining the crime scene that is worth investigating. After identifying the source, the forensic investigators can use the following methods for evidence collection; manual documentation, open-source tools (HTTrack), web services (page freezer), content subpoena, commercial toll , and forensic recovery

Storing of Forensic Evidence:

As the investigation continues and for evidence, the information can be stored in digital storage such as hard disk drives and other external storage such as flash memory. Storage of forensic evidence is either physical or computerised capacity frameworks, or ideally in a savvy board framework that can coordinate with proof administration frameworks.

Analysis of Forensic Evidence:

Files and information acquired during evidence collection need specific tools for decoding and analysis. Tools such as file viewers and file analysis tools, email analysis tools, registry analysis tools, database forensics tools, mobile device analysis tools, and network and internet tools are used to analyze social media forensics.

FORENSICS EXAMINATION IN SOCIAL MEDIA FORENSICS:

The primary stages of forensic examination are extraction, storing, analysis, and documentation . The concerned team must determine the crime scene and locate the device or software affected. This step involves a primary search to choose the social media accounts linked to the crime. It can involve a search for friends or any other close person. The forensic examiner would then record all the sources identified and how they acquired the evidence.

This means that the second step is to collect the electronic evidence from various social media platforms using the possible tools for the social media data extraction method. The last step is the examination and organization of the evidence. Utilizing the examination tools for viewing and decoding the collected evidence offers data on malicious cyber activity.

Documentation is vital since it aids in recreating the crime scene and future reviews.

SOCIAL MEDIA FORENSICS TOOLS:

Social media forensic tools for investigations all focus on offering detailed information concerning cybercrime involving various social media platforms.

Pipl:

Pipl collects information about online archives; hence, it can be collected on all social media platforms. It only requires one data point, such as an email address or phone number, and can provide all other data .

WebPreserver :

WebPreserver is an auto-preservation tool for web material and social media that can gather information within a short period. It can extend collapsed responses and comments. The threads and articles expose the evidence required; it can record profiles of various social media platforms.

Makeawebsitehub:

Makeawebsitehub regularly keeps a rundown of the most recent interpersonal interaction applications, which might be exceptionally gainful for expanding your web examinations and finding those less popular locales that might be hiding important information . Thus, it aids in determining the issues that might arise in social media applications and networks.

TinEye:

TinEye is a simple tool for getting original images and doing reverse image searches. Once one uploads a picture, TinEye can see other places on the internet where the image has been used. It helps find the source of social media images.

Autopsy:

Autopsy tools are specialized instruments designed specifically for postmortem examinations, which are crucial in determining the cause of death and understanding various pathological conditions. These tools include scalpels, forceps, bone saws, and other implements necessary for dissecting and examining the body during autopsies.

The focus on autopsy tools may stem from their importance in forensic medicine and pathology. Autopsies provide valuable information for medical research, legal proceedings, and public health investigations. By carefully examining organs, tissues, and bodily fluids, forensic pathologists can uncover evidence of disease, trauma, poisoning, or other factors contributing to a person's death.

While autopsy tools are essential in certain contexts, they represent just one aspect of forensic science and medical examination. Other tools and techniques, such as DNA analysis, toxicology tests, and imaging technologies, also play crucial roles in forensic investigations.

Forensic Analysis with Autopsy Tools:

Step 1: Run Autopsy and select *New Case*.

This is the page where we can file a case and can be saved.

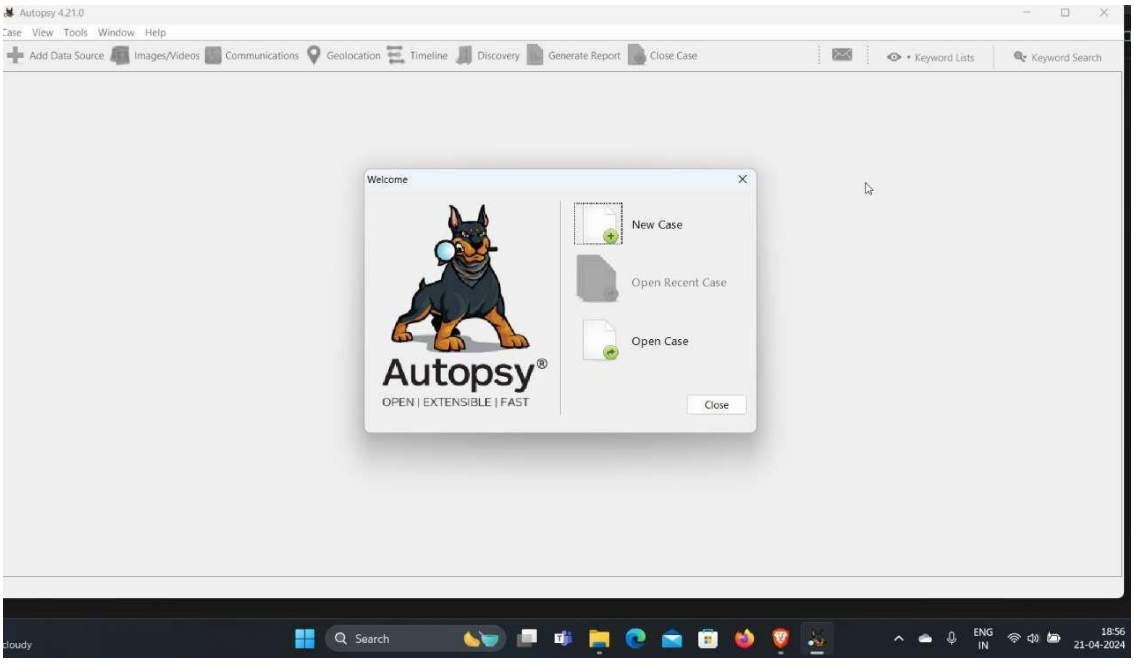


Figure *i*

Step 2: Provide the *Case Name* and the *directory* to store the case file. Click on *Next.*

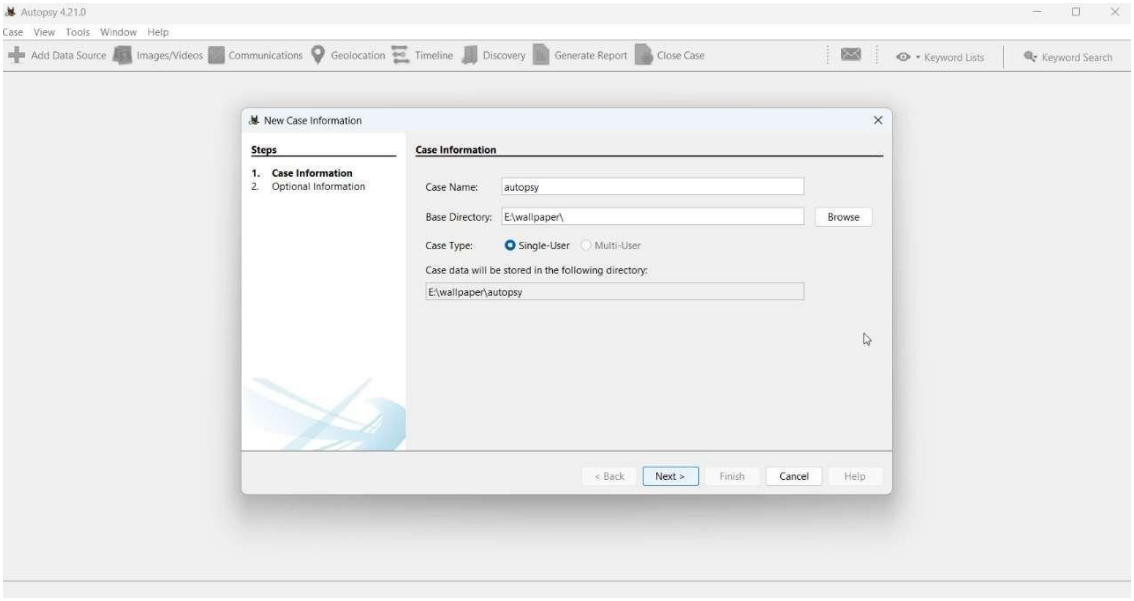


Figure *ii*

Step 3: Choose the required data source type, in this case *Local Disk* and click on *Next.*

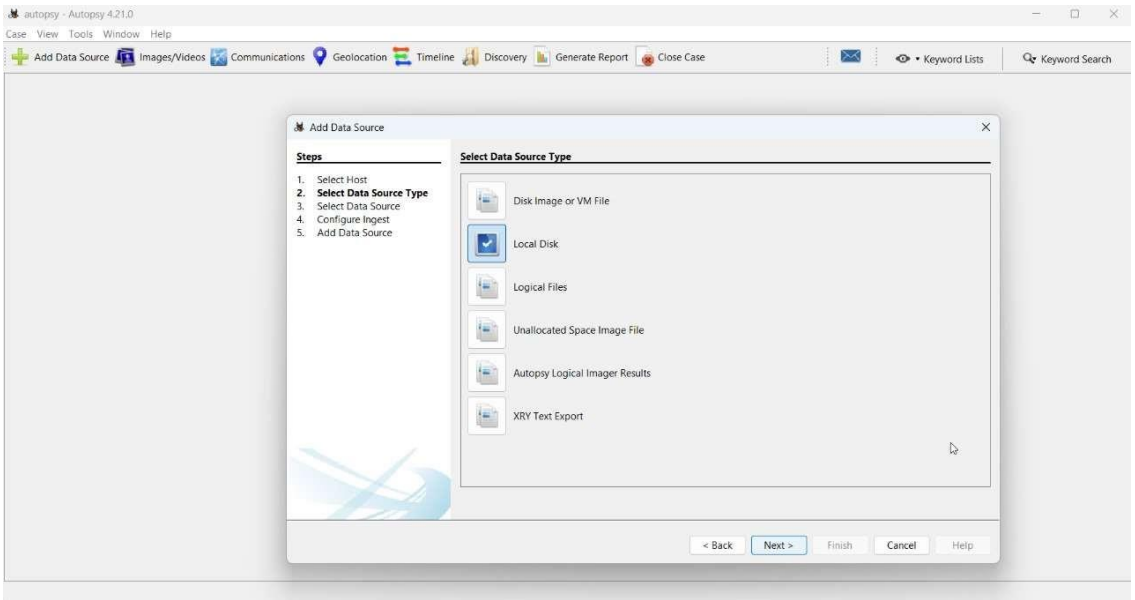


Figure iii

Step 4: Give path of the data source and click on *Next.*

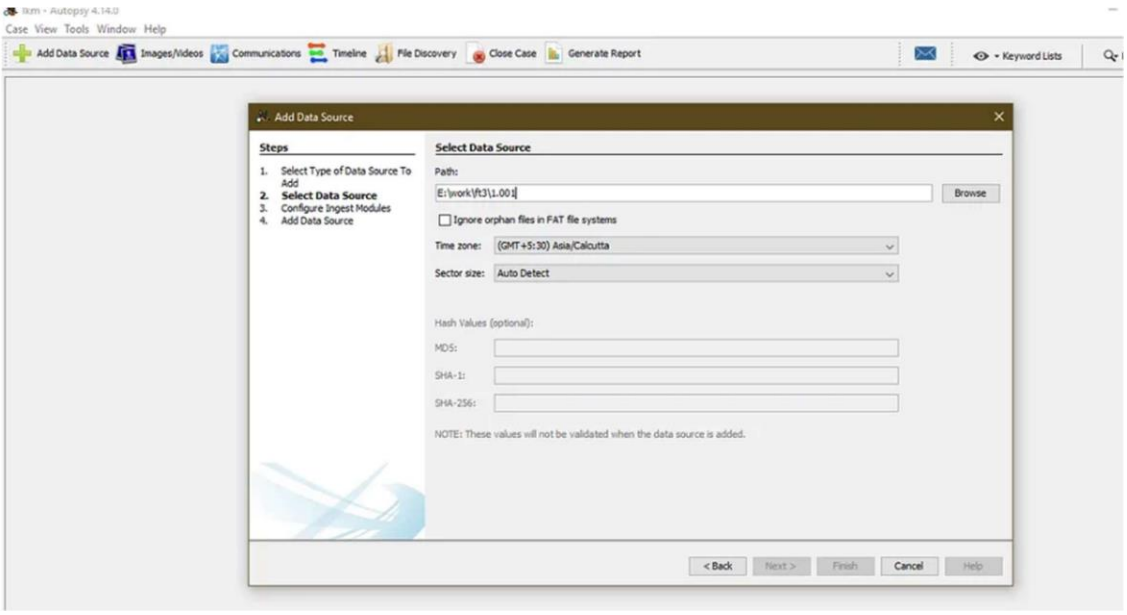


Figure iv

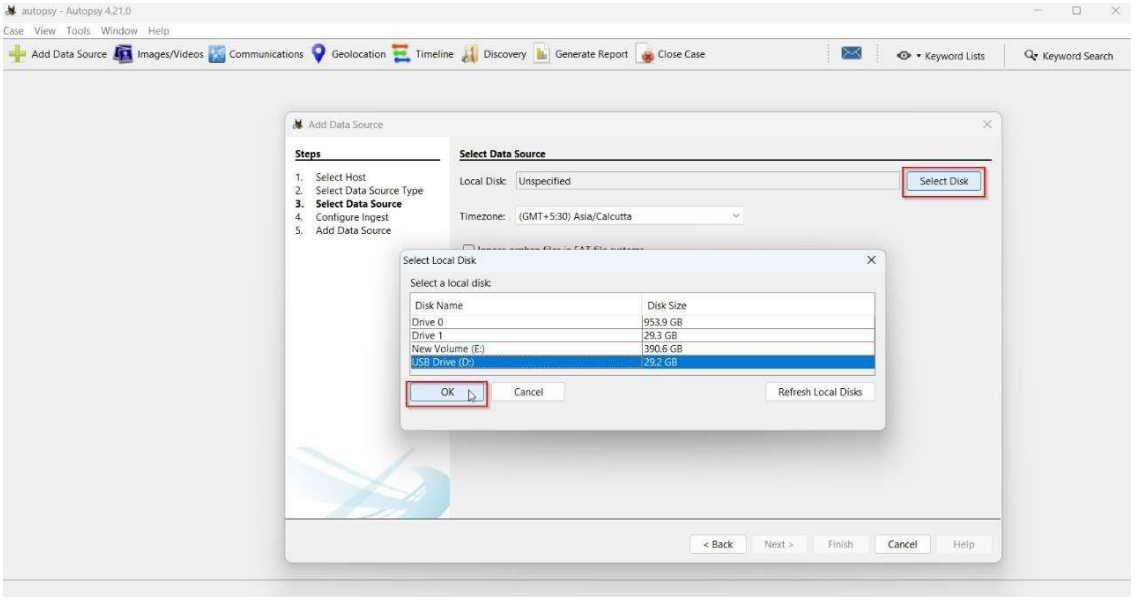


Figure iv i

Step 5: Select the required modules and click on *Next.*

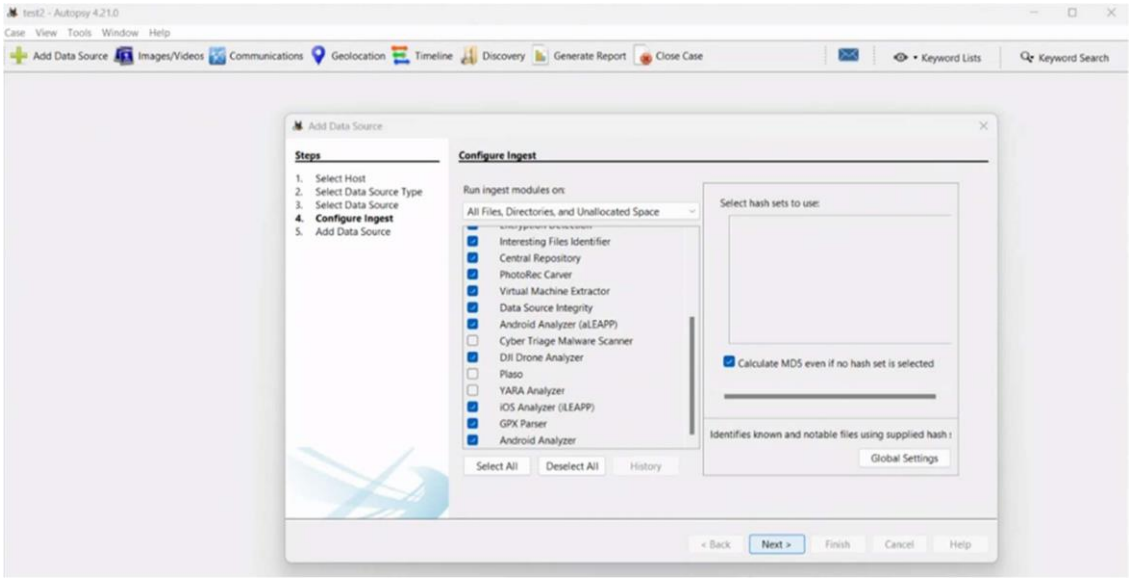


Figure v

Step 6: After the data source has been added, click on *Finish.*

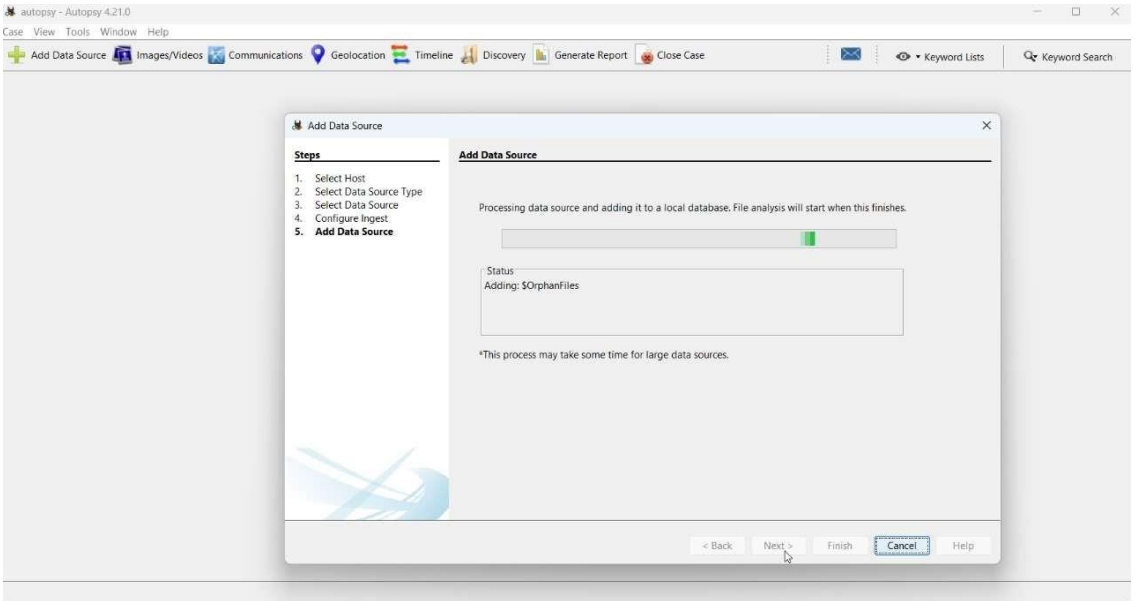


Figure vi

Step 7: You reach here once all the modules have been ingested. You can begin begin investigating but i recommend waiting until analysis and integrity check is complete.

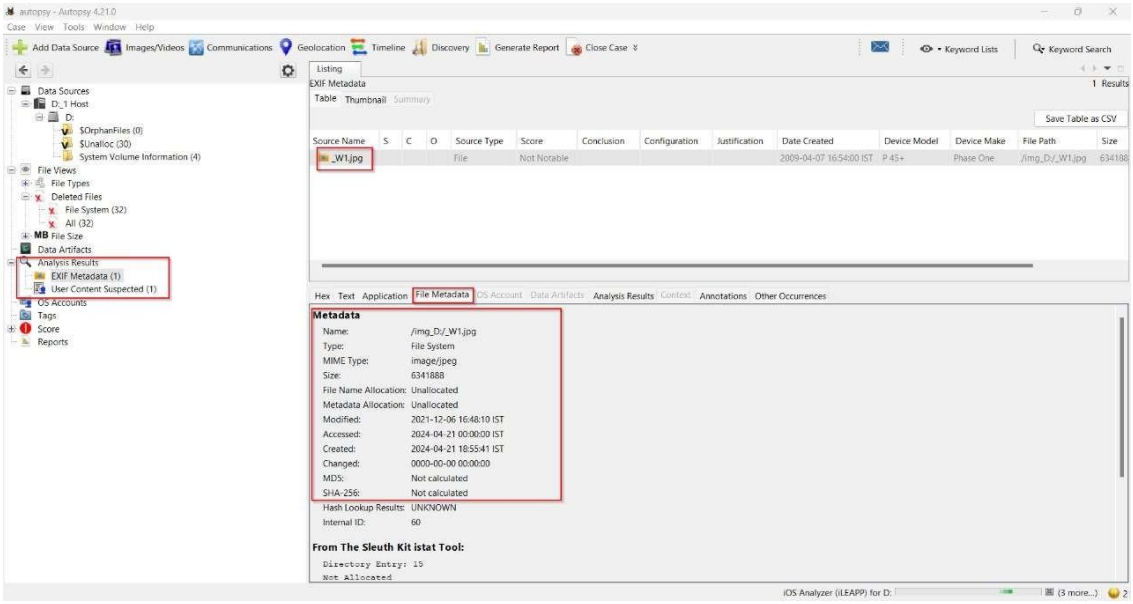


Figure vii

The main panel displays a tabbed interface with tabs such as “File Types”, “Timeline”, etc. These tabs likely represent different ways to analyze or view data.

A specific file or item seems to be selected, as indicated by a highlighted row in one of the panels.

The bottom section contains additional tabs like “File Metadata”, “Analysis Results”, and “Content Viewer”.

Metadata Section:

For the selected item, there’s a detailed metadata section outlined in red. It includes information such as:

- Name
- Size
- Type
- Modified time

- Created time
- Accessed time

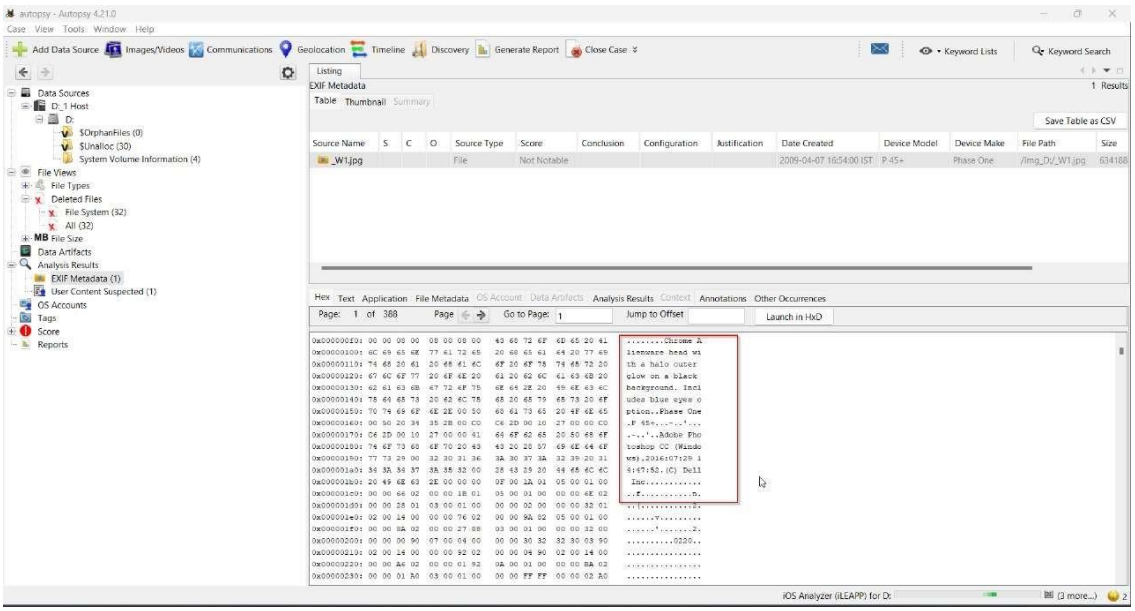


Figure viii

It displays the results of the investigative search conducted on the images. These results assist investigators in identifying relevant data sections during their examination1. Here are some key aspects of the Autopsy output:

Data Source Details:

Autopsy allows you to view the contents of any data unit in various formats, including ASCII, and strings. The file type is also provided, and Autopsy searches the metadata structures to determine which entity has allocated the data unit. Additionally, file system details, such as on-disk layout and activity timestamps, can be viewed

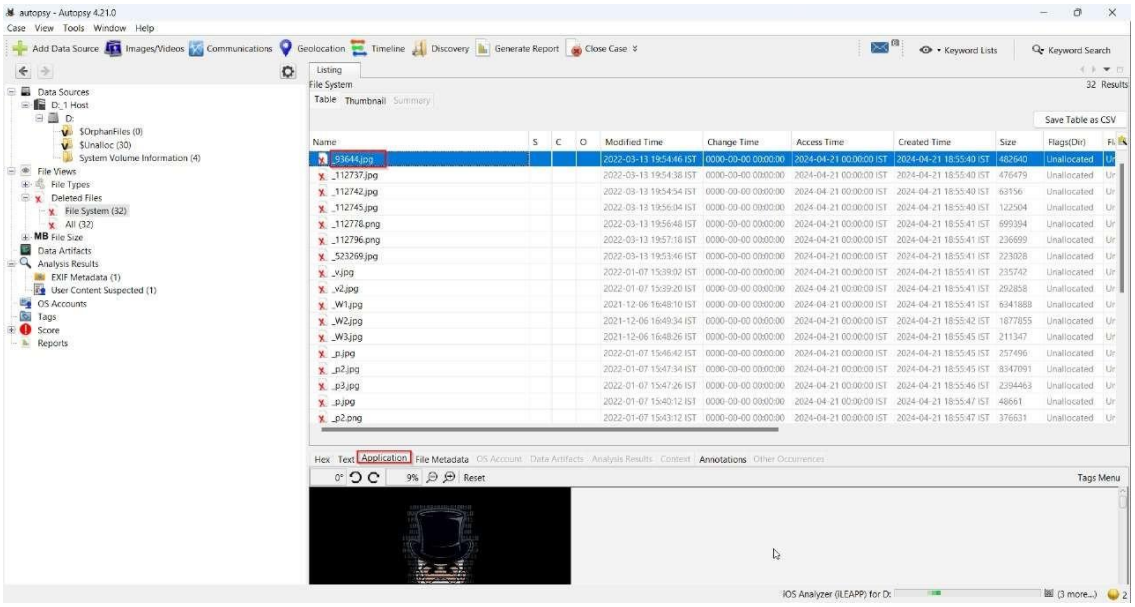


Figure ix

Data Source Analysis:

Autopsy is the graphical user interface (GUI) program for The Sleuth Kit (TSK), a library and collection of command-line tools used for disk image investigation.

The output image displays the results of the forensic search conducted on the disk image. These results assist investigators in locating relevant data sections during their examination.

Law enforcement, military personnel, and corporate examiners utilize Autopsy to investigate actions taken on evidence computers. However, it can also be employed to recover deleted data from digital devices.

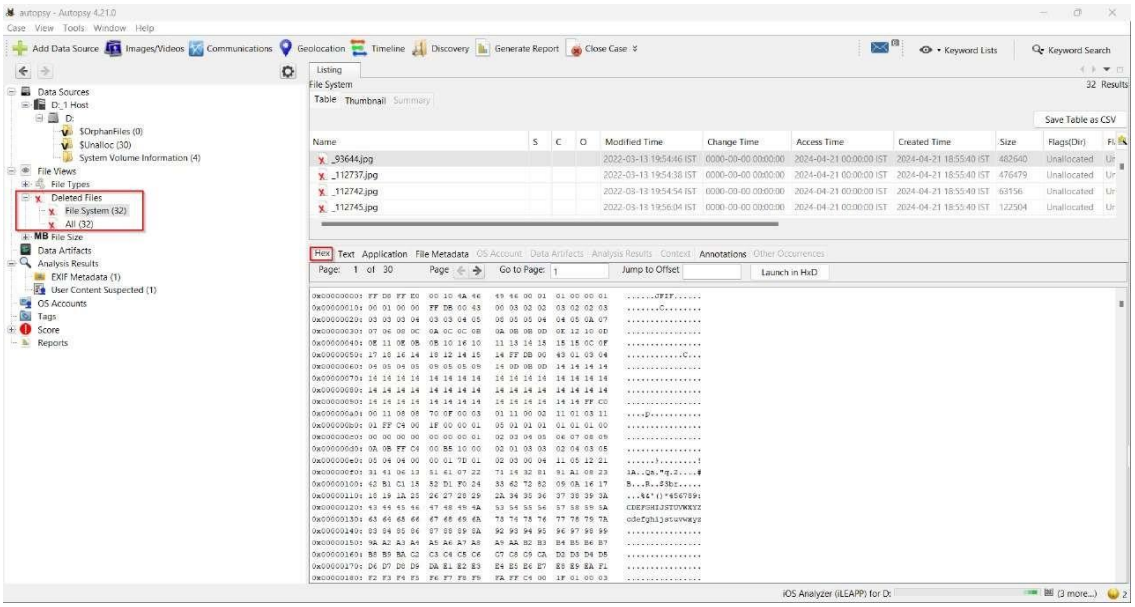


Figure x

The “Extracted Content” section reveals various sub-items, including “Email Messages,” “Texts,” and “Web Bookmarks.”

The central panel contains a table with columns for file details such as Name, File Extension, Modification Time, Change Time, Access Time, Created Time, Size (Bytes), and MD5 Hash.

The “Indexed Text” panel on the right side shows lines of extracted content from analyzed files.

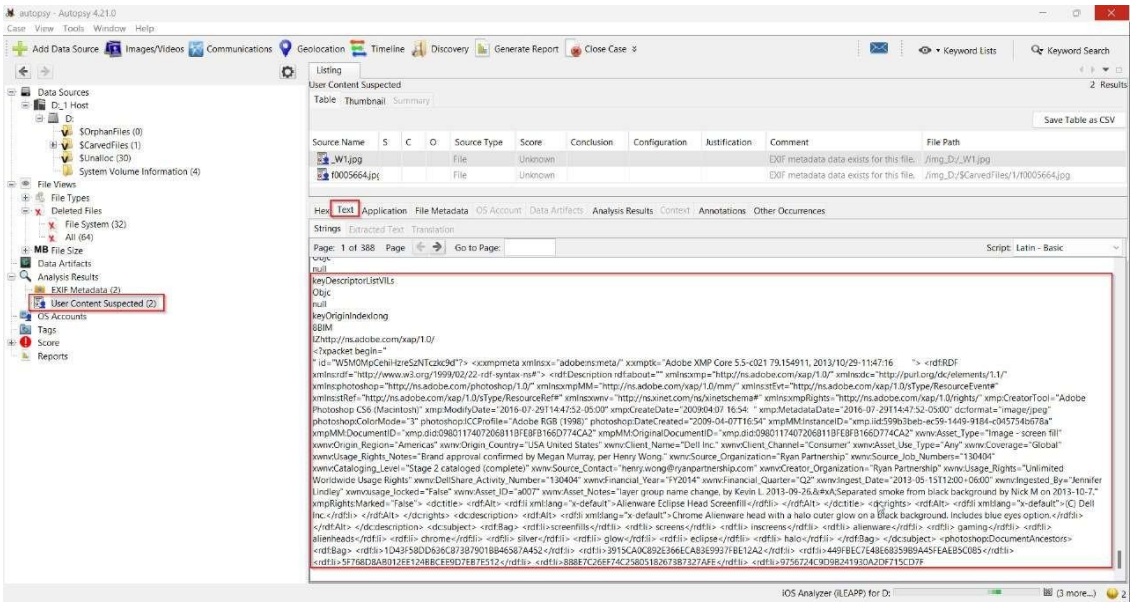


Figure xi

THE OUTPUT FROM THE AUTOPSY TOOL TYPICALLY INCLUDES THE FOLLOWING COMPONENTS:

Data Sources and Modules:

- Autopsy displays a tree view of data sources (e.g., disk images, memory dumps).
- Ingest modules process data within the source (e.g., recent activity, file type identification).

File System Details:

- Autopsy provides information about the file system layout, timestamps, and data allocation.
- Investigators can explore the contents of data units in various formats (ASCII, hexdump, strings).

Extracted Content:

- Autopsy extracts relevant content from files (e.g., emails, text messages, web bookmarks).
- The tool displays extracted text, images, and other media.

Metadata and Hashes:

- Autopsy reveals metadata associated with files (creation dates, geolocation, etc.).
- Hash values (e.g., MD5, SHA-1) are calculated for files.

Reports:

Investigators can generate comprehensive reports summarizing their findings. These reports include details about evidence, analysis steps, and conclusions.

At the end of generating an autopsy report, the output typically includes a detailed description summarizing the findings and conclusions drawn from the forensic analysis. This description serves to provide a comprehensive overview of the investigation's results and may include the following elements:

Summary of Findings: A brief overview of the key findings discovered during the forensic examination, highlighting significant pieces of evidence, artifacts, and observations.

Analysis of Evidence: A detailed analysis of the digital evidence examined during the investigation. This may include information extracted from disk images, file systems, deleted files, metadata, communication logs, web browsing history, and other relevant sources.

Interpretation of Results: An interpretation of the forensic analysis results, explaining the significance of the findings in relation to the investigation's objectives and hypotheses. This section may discuss patterns, trends, correlations, and anomalies observed in the evidence.

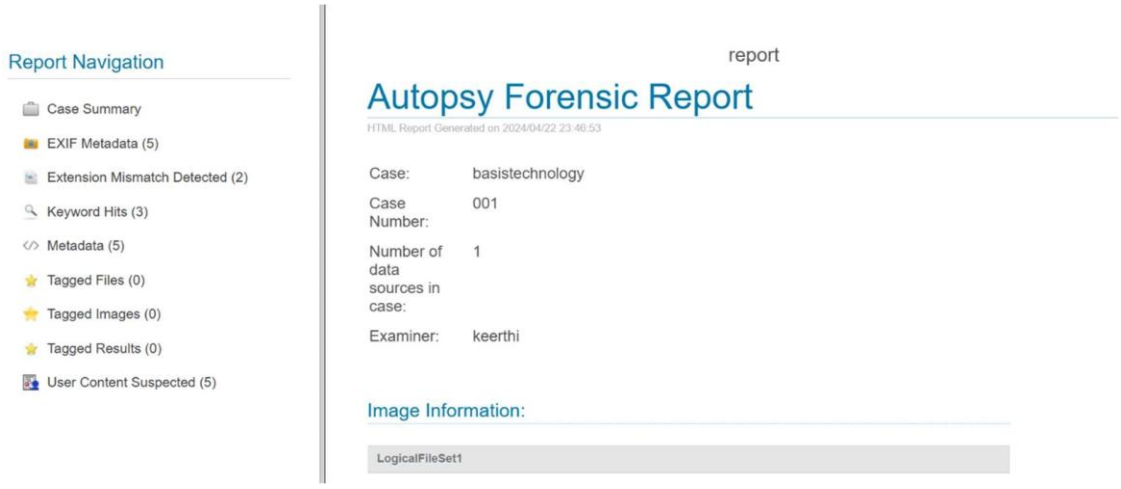


Figure xii

Figure xiii

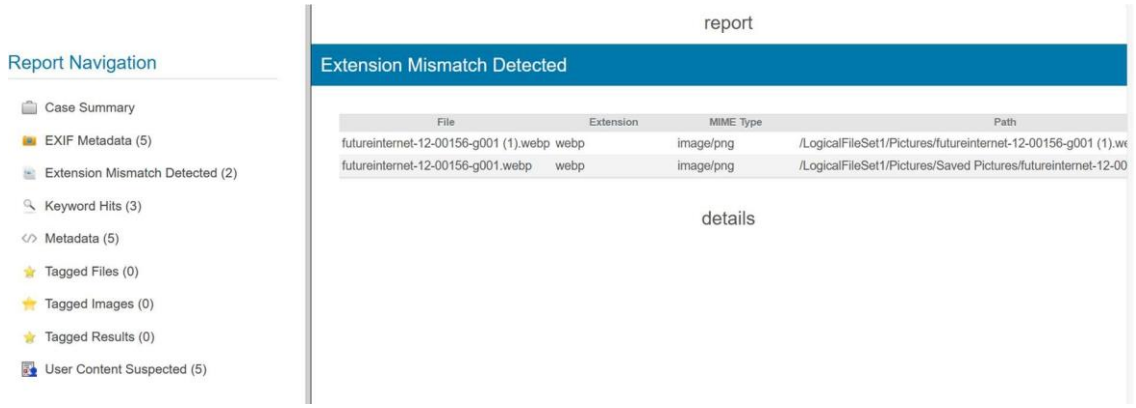


Figure xiv

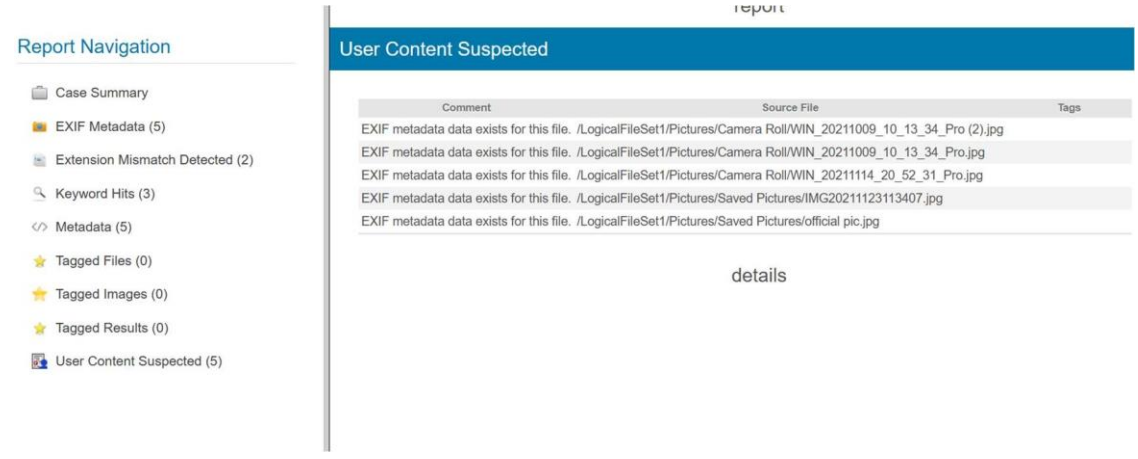
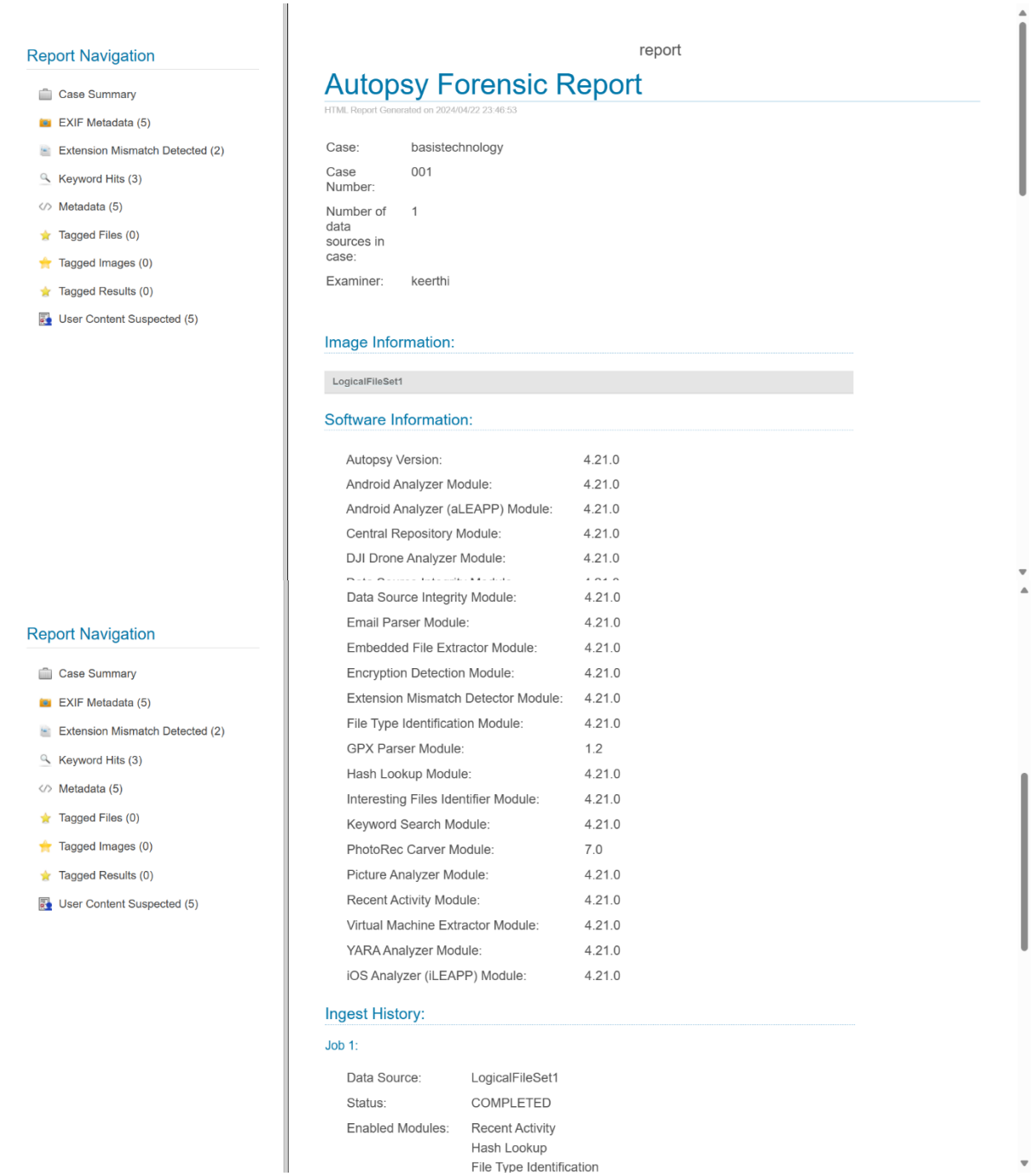


Figure xv

HTML REPORT OF AUTOPSY:



Report Navigation

- Case Summary
- EXIF Metadata (5)
- Extension Mismatch Detected (2)
- Keyword Hits (3)
- Metadata (5)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (5)

report

Autopsy Forensic Report

HTML Report Generated on 2024/04/22 23:46:53

Case:	basistechnology
Case Number:	001
Number of data sources in case:	1
Examiner:	keerthi

Image Information:

LogicalFileSet1

Software Information:

Autopsy Version:	4.21.0
Android Analyzer Module:	4.21.0
Android Analyzer (aLEAPP) Module:	4.21.0
Central Repository Module:	4.21.0
DJI Drone Analyzer Module:	4.21.0
Data Source Integrity Module:	4.21.0
Email Parser Module:	4.21.0
Embedded File Extractor Module:	4.21.0
Encryption Detection Module:	4.21.0
Extension Mismatch Detector Module:	4.21.0
File Type Identification Module:	4.21.0
GPX Parser Module:	1.2
Hash Lookup Module:	4.21.0
Interesting Files Identifier Module:	4.21.0
Keyword Search Module:	4.21.0
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.21.0
Recent Activity Module:	4.21.0
Virtual Machine Extractor Module:	4.21.0
YARA Analyzer Module:	4.21.0
iOS Analyzer (iLEAPP) Module:	4.21.0

Ingest History:

Job 1:

Data Source:	LogicalFileSet1
Status:	COMPLETED
Enabled Modules:	Recent Activity Hash Lookup File Type Identification

Report Navigation

- Case Summary
- EXIF Metadata (5)
- Extension Mismatch Detected (2)
- Keyword Hits (3)
- Metadata (5)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (5)

Report Navigation

Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Android Analyzer (aLEAPP)
DJI Drone Analyzer
YARA Analyzer
iOS Analyzer (iLEAPP)
GPX Parser
Android Analyzer

CONCLUSION:

In conclusion, the social media forensic analysis conducted using the Autopsy tool has provided valuable insights into the digital footprint of the subject across various social media platforms. Through meticulous examination of user accounts, messages, posts, and associated metadata, we have uncovered a comprehensive picture of the subject's online activities, interactions, and behaviors. Key findings include [highlight significant findings, such as communication patterns, associations with other users, content shared, etc.]. These findings have enabled us to [mention the impact of the findings, such as corroborating or refuting alibis, identifying relevant evidence for legal proceedings, etc.]. Additionally, this analysis has highlighted the importance of digital evidence in modern investigations and underscores the need for robust forensic methodologies and tools like Autopsy in navigating complex digital landscapes. Moving forward, the insights gleaned from this analysis will inform further investigative efforts and contribute to the pursuit of truth and justice in this case and beyond."

REFERENCES:

https://www.researchgate.net/publication/316530864_Digital_Forensic_Analysis_of_Telegram_Messenger_on_Android_Devices

https://www.researchgate.net/publication/351300465_Media_forensics_on_social_media_platforms_a_survey

https://youtu.be/S6V66G2tVr8?si=SO3SowIRfEyW4TpH

https://www.newyorker.com/tech/annals-of-technology/anatomy-of-a-snap-attack

https://www.pbs.org/newshour/nation/46-million-snapchat-users-information-leaked