

Table of Contents

1. Executive Summary.....	2
1.1. Introduction.....	2
1.2. Objectives	2
1.3. Key findings.....	3
2. Methodology	3
2.1. NIST Digital Forensics Process	3
2.2. Forensic Methodology Applied.....	4
2.3. Platform, App and Tools Selection	5
2.3.1. Platform.....	5
2.3.2. Mobile Application	6
2.3.3. Sandbox Environment.....	6
2.3.4. Forensic Tools.....	6
3. App Investigation, Analysis and Findings.....	7
3.1. Acquisition	7
3.2. Analysis.....	7
3.2.1. DB Browser for SQLite	7
3.2.2. Autopsy	7
3.2.3. App Permissions	7
3.2.4. Key Instagram Artifacts	8
4. Conclusion.....	9
5. References	9
6. Appendix	10
6.1. Setup screenshots	10
6.2. Acquisition screenshots.....	11
6.3. Analysis screenshots	12
6.4. App permissions.....	15
6.5. Table of artifacts	15

1. Executive Summary

1.1. Introduction

Instagram is a popular social media app with over 2 billion active users worldwide. It allows users to share photos and videos, connect with friends and followers, and explore content from other users. Here I used Android Studio to analyze Instagram APK file with the help of Pixel 6 Pro (API 34) Virtual mobile device. This may include identifying the user account associated with the APK file, recovering details of photos and videos, and examining direct messages.

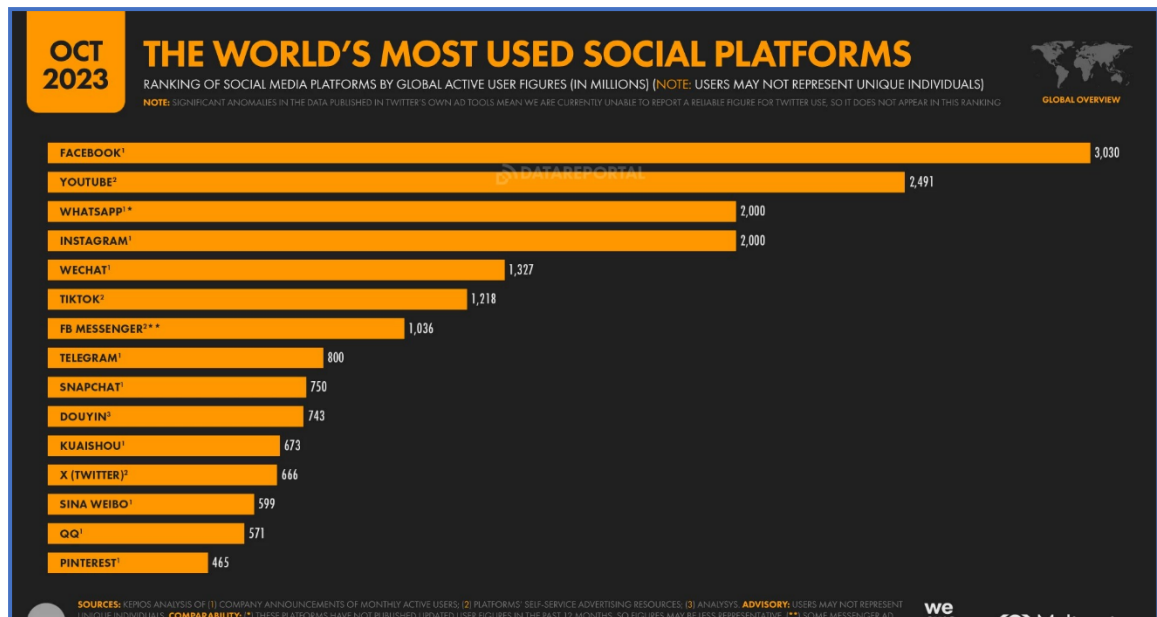


Fig 1: The most popular messaging apps in the world [1]

1.2. Objectives

The objective of this forensic investigation of an Instagram APK file is to collect and analyze evidence from Instagram to identify the user account associated with the APK file, gather information's of photos and videos, examine direct messages, and investigate other aspects of Instagram. The evidence collected from the APK file can also be used to support a criminal investigation or to identify and prosecute individuals who are using Instagram for illegal purposes.

Specifically, the objectives of a forensic investigation of an Instagram APK file may include:

- Identifying the user account associated with the APK file.
- Recovering details of photos and videos received & sent.
- Examining direct messages
- Reviewing the app's permissions
- Monitoring the user's geolocation
- Details of Devices logged in.
- Identifying how the app is collecting and using user data.

The specific objectives of a forensic investigation of an Instagram APK file will vary depending on the specific circumstances of the case. However, the overall goal is to collect and analyze evidence from the APK file to identify and prosecute individuals who are using Instagram for illegal purposes.

1.3. Key findings

The key findings of this forensic investigation are,

- Username account info
- User Profile picture
- User's friend list
- Logs
- Direct messages
- Login details of devices where the user account is logged in.
- GPS location
- IP Address

2. Methodology

ISO and NIST are two biggest organizations that have developed digital forensic frameworks to provide guidelines for the proper investigation and handling of digital evidence. Both frameworks aim to ensure the integrity, authenticity, and usability of digital evidence in legal and investigative proceedings.

ISO/IEC 27037:2012

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly developed ISO/IEC 27037:2012, titled "Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence." This framework provides a comprehensive set of guidelines for the handling of digital evidence throughout the investigative process, from identification and collection to preservation and analysis.

NIST SP 800-86

The National Institute of Standards and Technology (NIST) developed NIST SP 800-86, titled "Guideline on Digital Forensic Investigations," to provide a more detailed and prescriptive set of guidelines for conducting digital forensic investigations. This framework focuses on the technical aspects of digital forensics, including evidence acquisition, analysis, and reporting [2].

2.1. NIST Digital Forensics Process

According to the National Institute of Standards and Technology (NIST), Data collection, examination, analysis, and reporting are the four key phases of the digital forensics process. These phases are essential for conducting a thorough and accurate digital forensic investigation [2].



- **Data Collection** – The first phase of the digital forensics process is data collection, involves identifying, preserving, and collecting potential digital

evidence. The goal of data collection is to collect all relevant evidence in a way that minimizes the risk of contamination or alteration. There are several methods for collecting digital evidence, including:

- Imaging: This involves creating a bit-for-bit copy of a digital storage device.
- File carving: This involves recovering deleted files from a digital storage device.
- Live acquisition: This involves capturing data from a live computer system.
- **Data Examination** – The second phase of the digital forensics process is data examination. This involves examining the collected data to identify and extract relevant information. The goal of data examination is to identify all relevant information and to extract it in a way that preserves its integrity. There are several methods for examining digital evidence, including:
 - Hashing: This involves creating a unique fingerprint of a digital file.
 - Carving: This involves searching for specific types of data, such as images or documents.
 - Parsing: This involves breaking down a file into its constituent parts.
- **Data Analysis** – The third phase of the digital forensics process is data analysis. This involves analyzing the extracted information to identify and interpret findings. The goal of data analysis is to draw conclusions about the events that occurred on the digital device. There are several methods for analyzing digital evidence, including:
 - Timeline analysis: This involves creating a timeline of events that occurred on a digital device.
 - Link analysis: This involves identifying relationships between different pieces of data.
 - Content analysis: This involves examining the content of files to identify patterns or anomalies.
- **Data Reporting** – The fourth phase of the digital forensics process is data reporting. This involves documenting the findings of the investigation. The goal of data reporting is to communicate the findings of the investigation in a clear, concise, and legally defensible manner. A data report should include the following information:
 - Scope of the investigation: This should include the purpose of the investigation, the dates of the investigation, and the resources used.
 - Findings: This should include a summary of the findings, including the evidence that was collected, the methods that were used, and the conclusions that were drawn.
 - Recommendations: This should include recommendations for further investigation or mitigation.

2.2. Forensic Methodology Applied

I have chosen three papers which are based on NIST Forensic Analysis methodology, which is similar to my analysis in the case of tools, data extraction & analysis process. Below are the three papers:

Paper title	Authors	Description	Link
Forensic analysis of Instagram and path on	Reema Al Mushcab & Pavel Gladyshev	In this paper, they hope to sort some challenges of social network apps by performing a forensic analysis on Instagram and Path in a iPhone 5s device.	[3]

an iPhone 5s Mobile device		The process was installing the app, exploring functionalities of app, taking a logical image of mobile and start analysis. The real objective of the analysis was to check any data is stored in the internal memory of the device. Then in the result few data are stored in the device memory and they showed those data's with their location.	
Forensic Analysis of Social Networks Based on Instagram	Ming Sang Chang & Chih Ping Yen	In this paper, Instagram was taken as the subject and Windows 10 machine & an Android smartphone from Bluestacks were used as testing devices. They analysed the traces left in different browsers in Windows 10 machine and in the device storage of Android smartphone. An Android VM from Bluestacks, ES File Explorer, CCleaner, Recuva, are the tools used in the analysis. The Forensic analysis was done by using WinHex, DB Browser for SQLite.	[4]
Forensic Analysis of Popular Social Media Applications on Android Smartphones	Fatma Güneş Eriş and Erhan Akbal	In this paper, the procedures for Data extraction and Forensic Investigation are explained. Here WhatsApp, Facebook, Messenger, Instagram and Twitter are installed in an android device [Sony Xperia Z2 LTE-A(D6503) 16 Gb Android 10.0)] and accessed normal functionalities of those apps. Then the Forensic Analysis has been done by using Oxygen Forensic, Paraben E3:DS and Magnet Axion, DB Browser for SQLite & Android SDK.	[5]

Table 2.1

2.3. Platform, App and Tools Selection

2.3.1. Platform

S. No	Device	Details	Usage
1.	Acer Nitro 5 AN515-55	Intel (R) Core (TM) i7-10750H CPU @ 2.60GHz 2.59 GHz 8GB RAM Windows 11 22H2	Workstation
2.	Android Studio Giraffe 2022.3.1 Patch 2	Build #AI-223.8836.35.2231.10811636, built on September 14, 2023 Runtime version: 17.0.6+0-b2043.56-10027231 amd64 VM: OpenJDK 64-Bit Server VM by JetBrains s.r.o.	Android Emulator

3.	Pixel 6 Pro	Disk Space used – 10 GB. API Level - 34 Resolution – 1440 x 3120 (Can be Rooted)	Virtual Android Mobile Device
----	-------------	---	-------------------------------------

Table 2.2

Refer Appendix for screenshot.

2.3.2. Mobile Application

S. No	Application	Details	Usage
1.	Instagram	307.0.0.34.111- 370711653 minAPI28(x86_64) (nodpi)	Application used for Analysis

Table 2.3

Refer Appendix for screenshot.

2.3.3. Sandbox Environment

S. No	Device	Details	Usage
1.	Oracle Virtual Box	VirtualBox Graphical User Interface Version 7.0.12 r159484 (Qt5.15.2)	Virtualization provider
2.	Windows 11	WinDev2310Eval VM in Oracle Virtual Box	Used as a Sandbox Environment.

Table 2.4

Refer Appendix for screenshot.

2.3.4. Forensic Tools

S. No	Application	Details	Usage
1.	Autopsy	Product Version: Autopsy 4.21.0 (RELEASE) Sleuth Kit Version: 4.12.1 Netbeans RCP Build: 15- 387759c96ce1b891ec45ffaf524a53499455fe1a Java: 17.0.8; Java HotSpot (TM) 64-Bit Server VM 17.0.8+9-LTS-211 System: Windows 11 version 10.0 running on amd64; Cp1252; en_US (autopsy) User Dir: C:\Users\yog26\AppData\Roaming\autopsy	Automated tool for Digital Forensic Analysis
2.	DB Browser for SQLite	Version 3.12.2 Built for x86_64-little_endian-llp64, running on x86_64. Qt Version 5.12.8 SQLite Version 3.35.5.	Database File Viewer

Table 2.5

Refer Appendix for screenshot.

3. App Investigation, Analysis and Findings

3.1. Acquisition

The first phase of the digital forensics process is data collection or acquisition, involves identifying, preserving, and collecting potential digital evidence. The goal of data collection is to collect all relevant evidence in a way that minimizes the risk of contamination or alteration.

Initially Oracle Virtual Box has been installed in the workstation and Windows 11 VM in the Virtual Box. Then the Android Studio was installed in the Sandbox Windows 11 VM with all needed dependencies. Then a Virtual device has been created with the latest Android version which is suitable for the Instagram Application. Then created an account and logged in, accessing all functionalities in the application, like messaging, saving reels, posting story and posts, etc. Once the application is accessed completely, there is a functionality in Instagram, where we can get a copy of our account's complete activity. Then a request was sent and got my complete activity in my account. Then I downloaded the activity as .html in my virtual device. Finally, the virtual device has been rooted by using SDK tool. The command to root the virtual device in the terminal of Android Studio was, "**C:\Users\yog26\AppData\Local\Android\Sdk\platform-tools>. /adb root**". Once the device is rooted, the data in the mobile device is pulled to the Sandbox Windows 11 VM using the command, "**./adb pull -a <remote folder> <destination folder>**". Now the pulled data from the android device can be used for analysis. This is the process of logical data acquisition. The next process is the Analysis phase.

3.2. Analysis

The second phase of the digital forensics process is data examination. This involves examining the collected data to identify and extract relevant information. The goal of data examination is to identify all relevant information and to extract it in a way that preserves its integrity [6].

3.2.1. DB Browser for SQLite

DB Browser for SQLite is a free and open-source database management tool designed to handle SQLite databases. It is available for Windows, macOS, and Linux operating systems. The tool provides a user-friendly graphical interface for managing SQLite databases, including creating, modifying, and deleting tables and data, executing SQL queries, and exporting data to various formats [7].

3.2.2. Autopsy

Autopsy is an open-source digital forensics platform and graphical interface (GUI) to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card [8].

3.2.3. App Permissions

The App Permissions of Instagram in the virtual device can be seen in the below screenshot.

Permissions	Access
Calendar	Allowed
Camera	Allowed
Contacts	Allowed
Location	Allowed
Microphone	Allowed
Nearby Devices	Allowed
Notifications	Allowed
Phone	Allowed
Photos and Videos	Allowed

Table 3.1

Refer Appendix for screenshot.

The Pulled data from the Virtual device are analyzed by using DB Browser for SQLite and Autopsy. DB Browser for SQLite was used to view the databases extracted from the Virtual device. Autopsy is an automated forensic tool, where a case must be created and the base files like ISO image or logical files must be supplied to get the results. Here the extracted data was supplied into the Autopsy for analysis. Once it is done, the results can be seen as a tree structure on the left side of the Autopsy tool screen. Then we must check each and every file in the tree structure result, where we can get much crispy evidence. Here we got much evidence like friends list, direct messages, etc., The Autopsy report and those evidence are listed as screenshots in the Appendix.

3.2.4. Key Instagram Artifacts

Few of the data artifacts are listed below,

Location	Artifacts recovered
data/com.instagram.android/databases/ig_msys_database_17843299797097473	Information of the logged-in devices of this Instagram account
data/com.instagram.android/app_analytics/micro_batch/com.instagram.android/null/19669/472067/batch-77228-d322dea8-7bfd-432d-973f-30d63de39b47-5.json	Account Logs
data/com.instagram.android/databases/ranked_user_62931729472	Friends List
instagram-yog.anand.26-2023-11-08-DtZknv2a.zip/media	Profile photo, Posts, Stories,
data/com.instagram.android/databases/direct.db/messages	Direct Messages

Table 3.2

Refer Appendix for screenshot.

4. Conclusion

In this study, we conducted a forensic analysis of the Instagram mobile app installed on a virtual Android device in Android Studio. The analysis focused on identifying and extracting artifacts related to user activities, including posted images, comments, likes, and private messages. We also examined the app's data storage mechanisms and the impact of different privacy settings on the retention of user data. The findings of the study revealed that Instagram generates a significant amount of data that can be used to reconstruct user activities. This data includes location information, device identifiers, and timestamps, in addition to the content of user posts, comments, and messages. We also found that the app's data storage mechanisms are designed to minimize the amount of data that is retained on the device, making it more challenging to conduct forensic analysis. The study also demonstrated that different privacy settings can have a significant impact on the retention of user data. For example, users who have enabled the "Location Tracking" setting will have their location data stored on the app's servers, while users who have disabled this setting will not. This data can be useful for investigators who are trying to track the movements of a suspect or to identify potential witnesses. This forensic analysis of the Instagram mobile app in a virtual Android device has revealed that the app is a rich source of digital evidence that can be used to reconstruct user activities. Investigators should be aware of the app's data storage mechanisms and privacy settings when conducting forensic analysis.

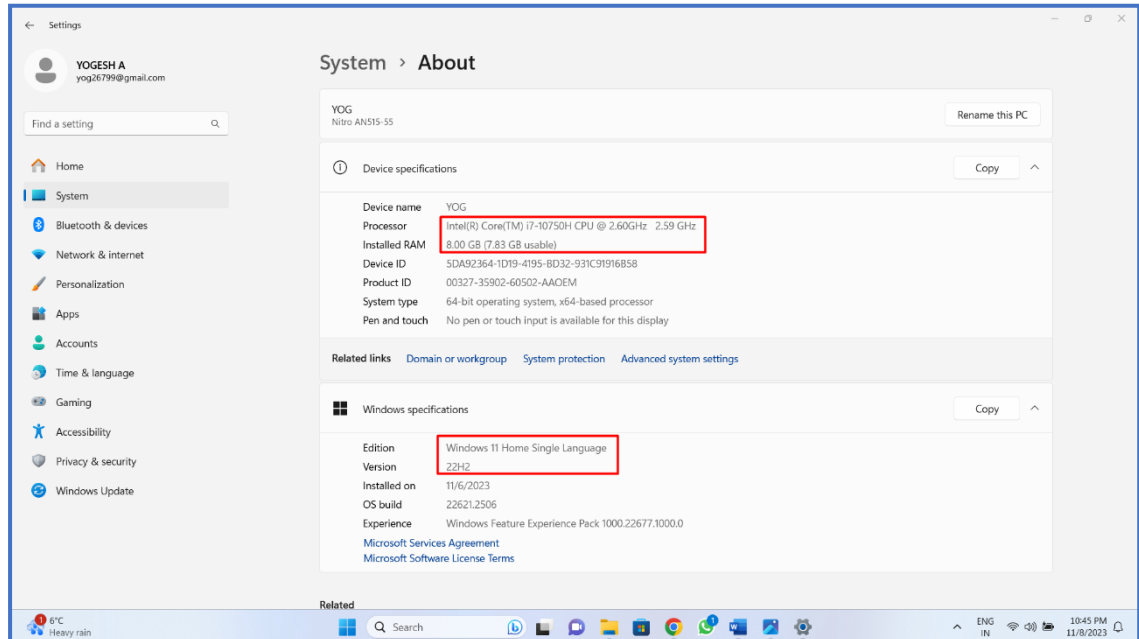
5. References

- [1] Marinela Potor, 'The most popular messaging apps worldwide by country', Sinch engage. Accessed: Nov. 10, 2023. [Online]. Available: <https://engage.sinch.com/blog/most-popular-messaging-apps-in-the-world/>
- [2] K. Kent, S. Chevalier, T. Grance, and H. Dang, 'Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology', *NIST*.
- [3] R. Al Mushcab and P. Gladyshev, 'Forensic analysis of instagram and path on an iPhone 5s mobile device', *Proc IEEE Symp Comput Commun*, vol. 2016-February, pp. 146–151, Feb. 2016, doi: 10.1109/ISCC.2015.7405508.
- [4] M. S. Chang and C. P. Yen, 'Forensic Analysis of Social Networks Based on Instagram', *International Journal of Network Security*, vol. 21, no. 5, p. 850, 2019, doi: 10.6633/IJNS.201909.
- [5] Fatma Güneş, Eriş, and Erhan Akbal, 'Forensic Analysis of Popular Social Media Applications on Android Smartphones', *Dergibark*, 2021, doi: 10.17694/bajece.761271.
- [6] Alyssa, 'Mobile Devices Forensics — Forensic Acquisition of an Android Studio Emulator | by Alyssa I. | Medium', Medium. Accessed: Nov. 10, 2023. [Online]. Available: <https://medium.com/@ailaria/mobile-devices-forensics-forensic-acquisition-of-an-android-studio-emulator-1c272ee8a5b3>
- [7] DB Browser, 'DB Browser for SQLite', *sqlitebrowser*. Accessed: Nov. 10, 2023. [Online]. Available: <https://sqlitebrowser.org/>
- [8] Autopsy, 'Autopsy - Digital Forensics', Autopsy. Accessed: Nov. 10, 2023. [Online]. Available: <https://www.autopsy.com/>

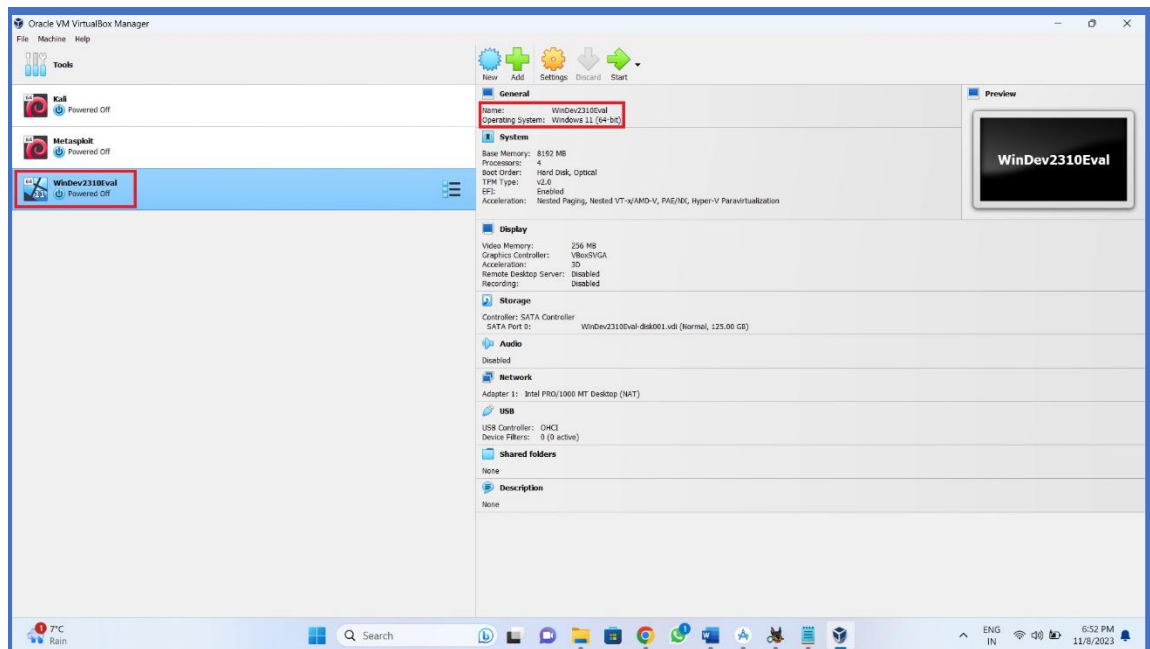
6. Appendix

6.1. Setup screenshots

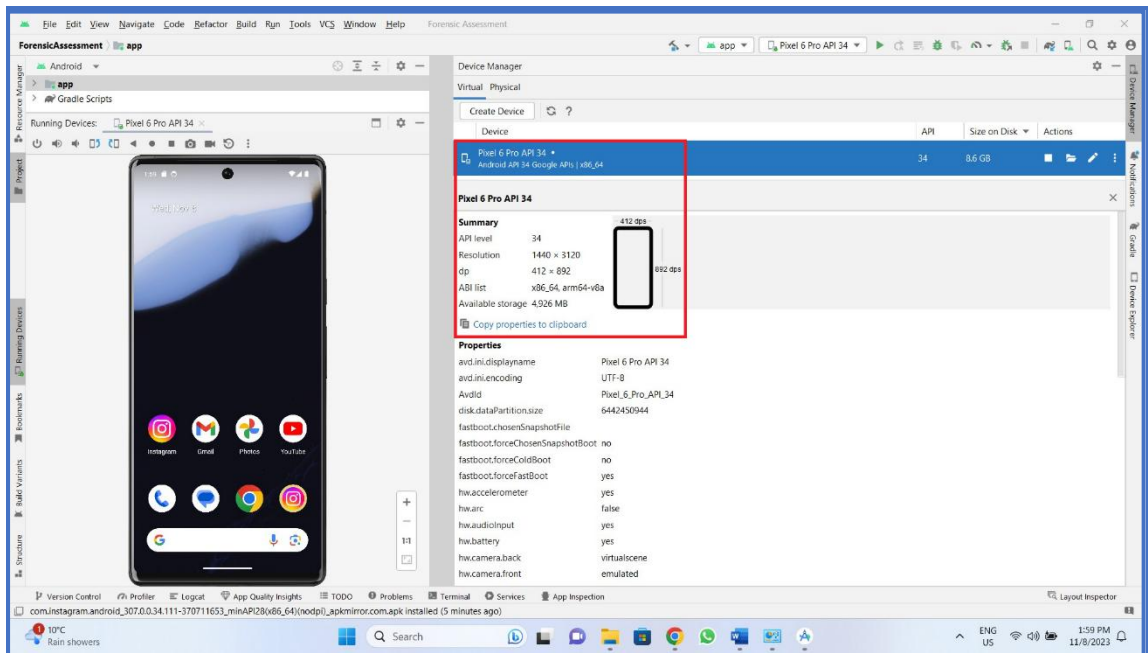
1. Workstation (Acer Nitro 5)



2. Sandbox Environment (Windows 11 VM in Virtual Box)

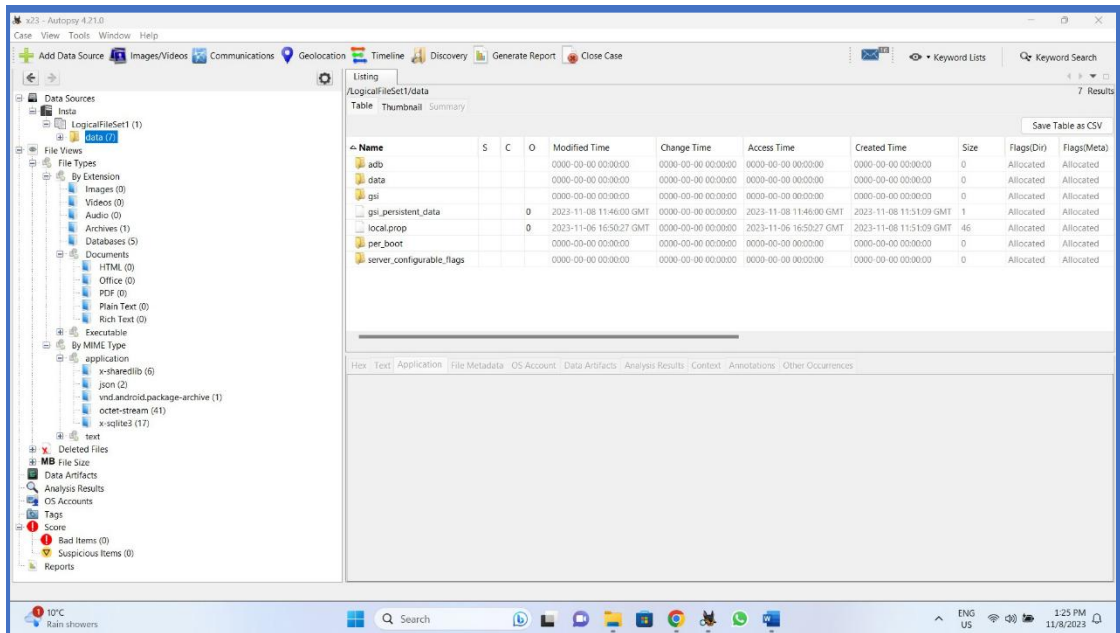


3. Android Studio & Pixel 6 Pro (Virtual Mobile Device)

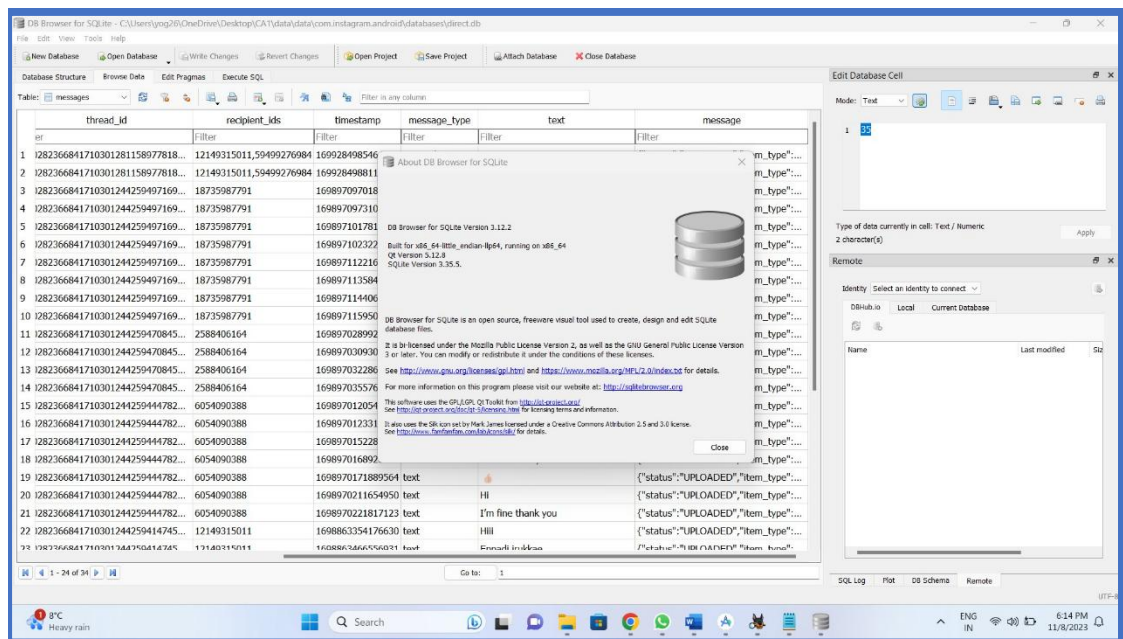


6.2. Acquisition screenshots

1. Autopsy

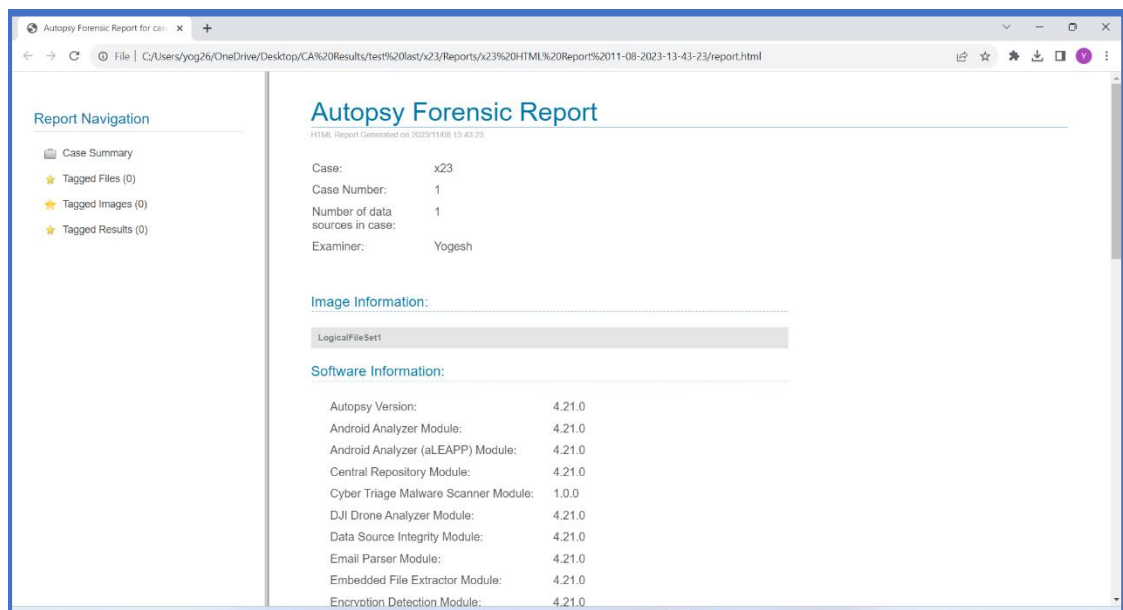


2. DB Browser for SQLite



6.3. Analysis screenshots

1. Autopsy Final Report



2. Logged in Devices Information

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the file system tree with 'Data Sources' and 'File Views' expanded. The main pane shows the 'Listing' tab with a table of 'application/x-sqlite3' files. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), and Known. The table lists several SQLite databases, including 'user_reel_medias_room_db_62931729472', 'transactions.db', 'time_in_app_62931729472.db', 'sponsored_pool_db_62931729472', 'safety_interventions_db_62931729472', 'recent_searches.db', 'ranked_user_62931729472', and 'ig_mys_database_17843299797097473'. The 'ig_mys_database_17843299797097473' file is selected, and its contents are displayed in the 'Table' view. The table has columns: crypto_mail, device_id, platform, manufact., model, last_seen_ts, registration., latitude, longitude, location, and ip. The table lists 9 entries, with the last entry highlighted in red.

crypto_mail	device_id	platform	manufact.	model	last_seen_ts	registration.	latitude	longitude	location	ip
3	1	Instagram	Apple	iPhone 14 Pro	1699403046	1698788951	53.3476	-6.2591	Dublin, Dublin, Ireland	2a01b34083c:
3	2	Instagram	Google	sdg_gphone4_x86_64	1698871624	1698863063	53.3476	-6.2591	Dublin, Dublin, Ireland	2a01b34084c:
3	3	Instagram	Google	sdg_gphone4_x86_64	1698940426	1698874872	53.3476	-6.2591	Dublin, Dublin, Ireland	212.129.740
3	4	Instagram	Google	sdg_gphone4_x86_64	1699043260	1698949321	53.3476	-6.2591	Dublin, Dublin, Ireland	2a01b34083c:
3	5	Instagram	Google	sdg_gphone4_x86_64	1699290649	1699279019	53.3475	-8.21944	Bellinacree, Galway, Ireland	193.1245.0
3	6	Instagram	Google	sdg_gphone4_x86_64	1699349072	1699291181	53.3476	-6.2591	Dublin, Dublin, Ireland	2a01b34083c:
3	7	Instagram	Google	sdg_gphone4_x86_64	1699441760	1699349552	53.3476	-6.2591	Dublin, Dublin, Ireland	2a01b34083c:
3	8	Instagram	Windows	Chrome	1699400752	1699400114	53.3476	-6.2591	Dublin, Dublin, Ireland	2a01b34083c:
3	9	Instagram	Google	sdg_gphone4_x86_64	1699443564	1699443555	53.3476	-6.2591	Dublin, Dublin, Ireland	2a01b34080c7c3a1ebee1f5a235a

3. Direct Messages

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the file system tree with 'Data Sources' and 'File Views' expanded. The main pane shows the 'Listing' tab with a table of 'Databases' files. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), and Known. The table lists three SQLite databases: 'direct.db', 'direct.db', and 'fieregistry.db'. The 'direct.db' file is selected, and its contents are displayed in the 'Table' view. The table has columns: _id, user_id, server_id, client_id, thread_id, recipient, timestamp, message, and text. The table lists 34 entries, with the last entry highlighted in red.

_id	user_id	server_id	client_id	thread_id	recipient	timestamp	message	text
35	629317294	313462752	712731780	340282366	121493150	1699284908	action_log	BL08 Det...
36	629317294	313462752	712731780	340282366	121493150	1699284908	text	Hello buddy
37	629317294	313462752	712731780	340282366	187359877	169897097	text	Hi
38	629317294	313462752	712731780	340282366	187359877	169897097	text	Ana madire
39	629317294	313462752	712731780	340282366	187359877	169897101	text	Olangae idhiya
40	629317294	313462752	712731780	340282366	187359877	169897102	text	Thandheya
41	629317294	313462752	712731780	340282366	187359877	169897112	text	Hooy
42	629317294	313462752	712731780	340282366	187359877	169897113	text	Nandu aaythu
43	629317294	313462752	712731780	340282366	187359877	169897114	text	Neeru oota madidra?
44	629317294	313462752	712731780	340282366	187359877	169897115	text	Chennagidhni, neeru?
45	629317294	313462752	712731780	340282366	25840616	169897028	text	Namaste
46	629317294	313462752	712731780	340282366	25840616	169897030	text	Mera naam Yogesh
47	629317294	313462752	712731780	340282366	25840616	169897032	text	Tumara naam kya hai???
48	629317294	313462752	712731780	340282366	25840616	169897035	text	Dekh ni rha profile me
49	629317294	313462752	712731780	340282366	605409038	169897012	text	Hi!!!
50	629317294	313462752	712731780	340282366	605409038	169897012	text	How are you
51	629317294	313462752	712731780	340282366	605409038	169897015	text	8878541310

4. Instagram Account Friends list

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the file tree with 'Data Sources' expanded, showing 'Initial' and 'data (7)'. The main pane shows a table of files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags. The table lists various files related to the Instagram account, including 'user_reel_medias_room_db_6293172942', 'transactions.db', 'time_in_app_6293172942.db', 'sponsored_pool_db_6293172942', 'safety_interventions_db_6293172942', 'recent_searches.db', 'ranked_user_6293172942', 'ig_msys_database_17642299797097473', 'flash_media_6293172942', 'fileregistry.db', and 'feed_items_room_db_6293172942'. Below the table, the 'Table local_recipients_ranked' is selected, showing 6 entries. The table has columns: igid, entity_type, score, username, and profile_picture_url. The entries are:

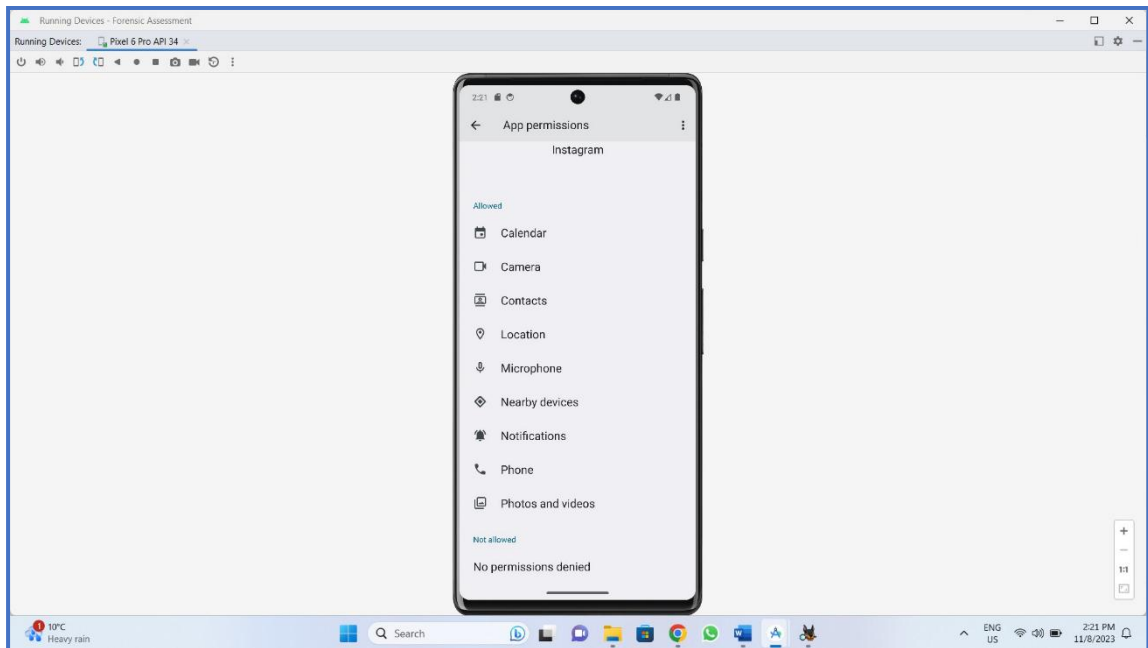
igid	entity_type	score	username	profile_picture_url
26996180594	IG_USER	0.0181312468	ranjithkumar_saravanan	https://scontent.cdninstagram.com/v/t51.2885-19/296808258_1396086654208390_3256700654
59499276984	IG_USER	0.0181312468	y26.pvot	https://scontent.cdninstagram.com/v/t51.2885-19/35625542_10065016309571_444143850
12149315011	IG_USER	0.0181312468	yogesh.26	https://scontent.cdninstagram.com/v/t51.2885-19/385492945_274785132091361_3662641583
18735987791	IG_USER	0.0181312468	the_musicophile	https://scontent.cdninstagram.com/v/t51.2885-19/293824224_3198173787165832_471854474
6054090388	IG_USER	0.0181312468	miss_chassy	https://scontent.cdninstagram.com/v/t51.2885-19/392904231_668817635221349_361117578
2580406164	IG_USER	0.0181312468	chandananandran97	https://scontent.cdninstagram.com/v/t51.2885-19/270056916_315201867136440_4697561700

5. Instagram Account Logs

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the file tree with 'Data Sources' expanded, showing 'Initial' and 'data (7)'. The main pane shows a table of files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags. The table lists various files related to the Instagram account, including 'batch-537139-37419c5-1475-46bc-9c21-5b0e0f013', 'batch-548187-37419c5-1475-46bc-9c21-5b0e0f013', 'batch-562980-0383c5-333b-42d4-bef9-0e5f0a7f', 'batch-76083-eb83ecf-bf8c-485f-8dc1-74493b2c', and 'batch-77228-d322eaa0-7bf5-432d-973f-30d63de1'. Below the table, the 'Strings' tab is selected, showing a list of strings extracted from the files. The strings include:

- batch-537139-37419c5-1475-46bc-9c21-5b0e0f013
- batch-548187-37419c5-1475-46bc-9c21-5b0e0f013
- batch-562980-0383c5-333b-42d4-bef9-0e5f0a7f
- batch-76083-eb83ecf-bf8c-485f-8dc1-74493b2c
- batch-77228-d322eaa0-7bf5-432d-973f-30d63de1

6.4. App permissions



6.5. Table of artifacts

Retrieved by Autopsy:

SHA 256 Hash	Artifacts recovered
11ADD983BFF92F25141F9CEB04 228887E934C9B871858E92E37750 19AB4DE306	Information of the logged-in devices of this Instagram account
E3B0C44298FC1C149AFBF4C899 6FB92427AE41E4649B934CA4959 91B7852B855	Account Logs
F8046FB6523B685349E4CEAA5B6 3D5653F3D4D9BC0291DD9546056 BFABD76205	Friends List
AA1ABFE43F1E08A416333685AD ABCE22CCB70842DE0EEF99935 AD847C6046A89	Profile photo, Posts, Stories, Eg : Post in Instagram page.
D2B81A6846A82A2F5DF69A60DB 9CC4DEF70BA14B0F5B5D550E8 A8E897FB0E1C3	Direct Messages