

**National College of Ireland**

**Project Submission Sheet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name:** | Ankit Mudgil | | |
| **Student ID:** | 23392801 | | |
| **Programme:** | MSc Cybersecurity | **Year:** | 2025-26 |
| **Module:** | Forensics & eDiscovery | | |
| **Lecturer:** | Prof. Eugene Mclaughlin | | |
| **Submission Due Date:** | 28/02/2025 | | |
| **Project Title:** | CA1 | | |
| **Word Count:** | 2461 | | |

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

|  |  |
| --- | --- |
| **Signature:** | Ankit Mudgil |
| **Date:** | 28/02/2025 |

**PLEASE READ THE FOLLOWING INSTRUCTIONS:**

1. Please attach a completed copy of this sheet to each project (including multiple copies).

2. Projects should be submitted to your Programme Coordinator.

3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.

4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**

5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

|  |  |
| --- | --- |
| **Office Use Only** | |
| Signature: |  |
| Date: |  |
| Penalty Applied (if applicable): |  |

AI Acknowledgement Supplement

# [Insert Module Name]

# [Insert Title of your assignment]

|  |  |  |
| --- | --- | --- |
| **Your Name/Student Number** | **Course** | **Date** |
|  |  |  |

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click [here](https://libguides.ncirl.ie/useofaiinteachingandlearning/studentguide).

# AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

|  |  |  |
| --- | --- | --- |
| **Tool Name** | **Brief Description** | **Link to tool** |
|  |  |  |
|  |  |  |

# Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

|  |  |
| --- | --- |
| **[Insert Tool Name]** | |
| [Insert Description of use] | |
| [Insert Sample prompt] | [Insert Sample response] |

# Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

# Additional Evidence:

[Place evidence here]

# Additional Evidence:

[Place evidence here]

**CA1**

**Ankit Mudgil**

**23392801**

**Forensics Analysis Report on Facebook**

**Executive Summary**

**Introduction**

Facebook, as we all know is a big social media platform that is being used by over 3.07 billion uses. It also serve us as a messaging application that helps us to get in touch with our family and friends and lets us share content like photos, videos, memories and updates about our day to day life. In this report, there is an investigation being performed to for forensic analysis to find data stored by facebook application in android enviornment. in i am sharing the findings, methodology and refernces that were used during this forensics investigation.

**Objectives**

Analyizing FACEBOOK application to capture data, app behavior and finding locations of confidential databases related to user.

**Key Findings**

While conducting this forensic investigation I found the important data like SQL databases that stores data related to user activity and can be pulled out from directory named ‘com.facebook.katana’ and such as log information, media files, contact information (Friends list) etc. Facebook also has different types of user permissions such as access to storage, geolocation, biometric, contacts, calls, microphone, etc, that can lead to multiple privacy threats. There was also a dynamic analysis of facebook that was conducted by using android studio and while using logcat feature that gave us logs related to the app behaviour and how the facebook application communicates with its API and servers. That can expose the user activity while using facebook.

**Methodology**

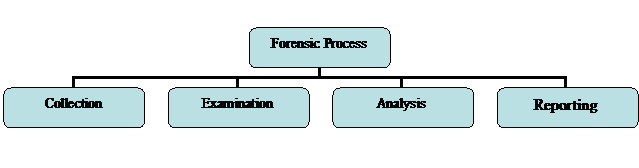
Forensics methodology used in this report has its roots in NIST research that followed some steps for data collection. This forensic investigation is executed following the process of collection, examination, analysis and reporting the findings (Fig.1). I will also use a similar methodology during the following this investigation process. This methodology was used for the reliability and integrity of the evidence and data. This methodology contains basic steps given by NIST, that were designed for forensic analysis and to make sure results that were collected during investigation were in safe custody (*FORENSIC TECHNIQUES*, no date). The key phases as outlined by NIST are as follows :

Figure 1 Forensic Analysis Steps

1. **Collection**: Data collection started from the virtual device running in Android studio by following the steps according the NIST guidelines using Android Debug Bridge (ADB) commands, but ADB will only work after downloading SDK components (*How to Install APK Files in Android Studio Emulator (3 Methods)*, 2022). And after installing facebook on a virtual device Pixel 6 with x86 architecture in android studio, ADB pull command was used to retrieve the databases (.db), Cache media files and messages.
2. **Examination**: Forensic tools like Autopsy, DB browser SQL and Android SDK were used to examine the extracted data including the stories, contact list, chats and user activity logs. Main part of this investigation was focused on SQLite Cipher tool as it helped in understanding the database files such as mib\_msys\_echo that store messages and can be located in the com.facebook.katana/files that were essentials in understanding the entire data collected in the local directories of Facebook application.
3. **Analysis**: During this phase, analysis of the the extracted data took place to determine the forensic artifacts, such as user interactions, cached media files and Friends lists, etc. All the NIST guidelines were followed to make sure that this analysis was reproducible and also double-checked all of the findings using different tools, including Autopsy and manual reviews of database files.
4. **Reporting**: In this last phase, a report was created to document the findings, all the used methods and forensic evidence from Facebook application.

These data files were extracted from the root directory named com.facebook.katana using Android Debug Bridge (ADB) commands as shown in the below screenshot.

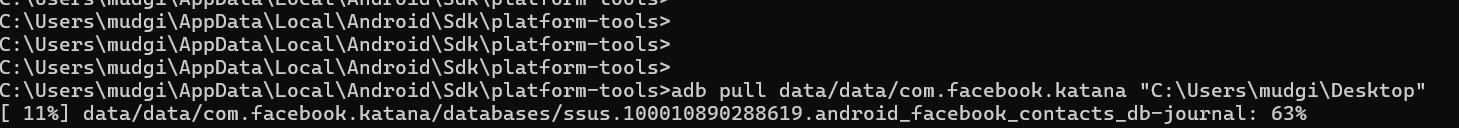


Figure 2 ADB Pull Command

The collected data was stored in the local directory with the decompiled facebook.apk (using APK tool and Android studio’s Profile or debug apk option) and analyzed using forensic tools such as Autopsy, DB Browser (SQL Cipher) and Logcat. As the main motive to create this report was to understand the process of how facebook application store data locally.

**Literature Review**

In recent years investigation related to forensics analysis of social media are increasing and one of the biggest reasons is the rapid increase in cyber crimes related these applications such as Instagram, Facebook, Snapchat, WhatsApp, etc. There are many studies that have explored different types of forensic methodologies and tools that are used to extract, analyse and extract digital evidence from these social media platforms. Even law enforcement agencies and researchers are now focusing on digital forensics due rise of cyberstalking, harassment and especially identity theft as these types of crime can cause financial loss to people and sometimes companies like happened in **477 Million** hack of FTX Trading case ((*Hunting the $477,000,000 FTX Hacker*, 2025)).

There are several studies that have explained forensic methodologies for social media applications. Daniel Walnycky et al. (2015) also examined evidence traces that these platforms leave, revealing data such as pictures, audios and messages that were sent and told how we can reconstruct these as well for later evidences. And not only him AL Mutawa et al. (2016) also used different operating systems for investigating user activity on these social media applications like Twitter, Facebook and mySpace, and found that android and ios devices are in rich sources for these kinds of evidences (Agrawal, Sharma and Khatri, 2019).

Agarwall et al. (2019) also did a deep analysis of Facebook app using a Genymotion virtual environment. Their study also reached to the same conclusions like the others, that Facebook’s valuable data like timestamps, newsfeeds, user details, contacts and messages can be extracted really easily. Tools that they used while conducting this investigation were simple and accessible such as FTK Imager, WxHexEditor and Fiddler as this also a very cost effective approach (Agrawal, Sharma and Khatri, 2019).

Eris and Akbal (2021) also did same kind of research and had more expanded findings while investigation they didn’t just investigate Facebook, but also included WhatsApp, Instagram and Twitter. And they used more extensive commercial tools such as Oxygen Forensic, Paraben E3:DS and Magnet Axiom. There research was more about manual data extraction with automated forensic tools, while doing they want to prove that software tools are good but these software tools fail to detect all of the data. They proved that taking a hybrid approach in data detection is much better for forensic analysis (Eriş and Akbal, 2021).

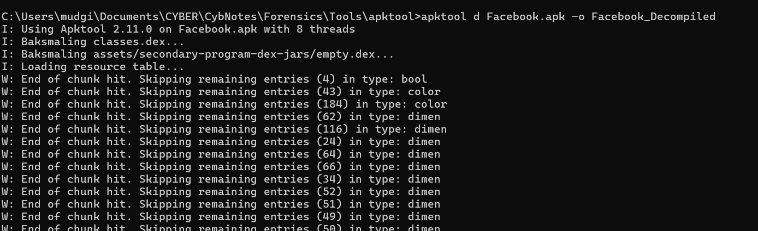
I included these research papers in my assignment because of there easy but smart approach and learned new things from both research papers. And mostly used open source tools and forensic environment (Eriş and Akbal, 2021).

**Description of the Tools & Test Environment Setup**

Tools that are in following table were used in this forensic analysis.

|  |  |
| --- | --- |
| **Configuration & Tools** | **Description** |
| APK Tool | APK Tool is used to decompile apk files to get application data |
| Google Pixel 6 | Architecture of the devices was x86, Running on Android 10.0 “Q” and API level 29 |
| SDK Component | Software development kit is a collection of tools that is for android environment and development |
| DB Browser (SQL Cipher) | It helped in viewing the database files (SQL) extracted during the analysis |
| Epoch Converter | Epoch is an web based time converter used for timestamps (*Epoch Converter*). |
| Autopsy | Autopsy is an open source digital forensic tool used to analyze different types of files |
| Android Studio | Android studio is an emulator tool used to create android environment and android development |

**APK Tool**: APK tool was used to decompile Facebook application, to find the details of regarding apk file such as AndroidManifest.xml, resources and smali codes were discovered which helped in understanding facebook application architecture along with that it also revealed the AndroidManifest.xml file which contained app permissions this application had or did not had (Fig. 3).

**Autopsy**: Autopsy is forensic tool that helped us in the analysis of extracted data from

com.facebook.katana. All investigation of data including databases, videos, timelines, images and other type of data was conducted on autopsy in one way or another.

Figure 3 APK Tool Decompling Facebook

**DB Browser (SQL Cipher):** DB browser is an open source software that has been a great software in examining all sql databases contained in Facebook app. It is also used to decrypt sql databases that will help in examining database (*DB Browser for SQLite*).

**Android Studio:** Understanding how the app functioned became possible through working with the android studio emulator and analysing logs using logcat feature of android studio. Even after the turning of the application we spotted that the application was still running in the background and communicating waith api int real time and updating data for better user experience.

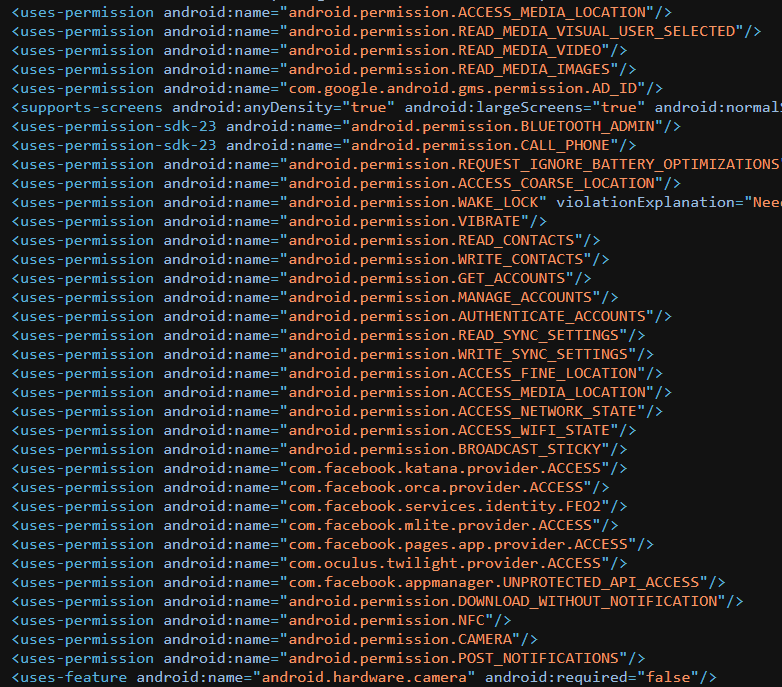
**App Investigation and Findings**

These details were found while investigating the Facebook.apk. The Facebook application contains a code signing certificate.

|  |  |
| --- | --- |
| **Content** | **Description** |
| Facebook\_501.0.0.61.70.apk | Facebook .apk file |
| MD5 | 769812f8780e317b643c62262c749441 |
| PublicKey Algorithm | 1024-bit RSA |
| SHA1 | 4a4ee4b47390e953660a7ac68b739508d5b2c6af |
| SHA256 | 565f9f13e45f8055e6596df600b02f9cced5c7bae08bbc3ca4571630731a1afa |

**AndroidManifest.xml:**  AndroidManifest.xml is file that stores multiple types of permissions that were given like **android.permission.READ\_MEDIA\_VIDEO**, **android.permission.READ\_MEDIA\_IMAGES**, **android.permission.CAMERA,** these permissions allow facebook to take photos or videos using device camera and microphone . More permissions are also contained like **android.permission.INTERNET,**

**android.permission.CREDENTIAL\_MANAGER\_SET\_ALLOWED\_PROVIDERS, android.permissions.READ\_PROFILE**, etc (Shown in Fig. 4). Hash file of this file is **MD5: 79a6cd5cfe40615b09308a8754f840c3 and**

**SHA1: 178582a846df397f4a52a4776d69540b6608688b.**

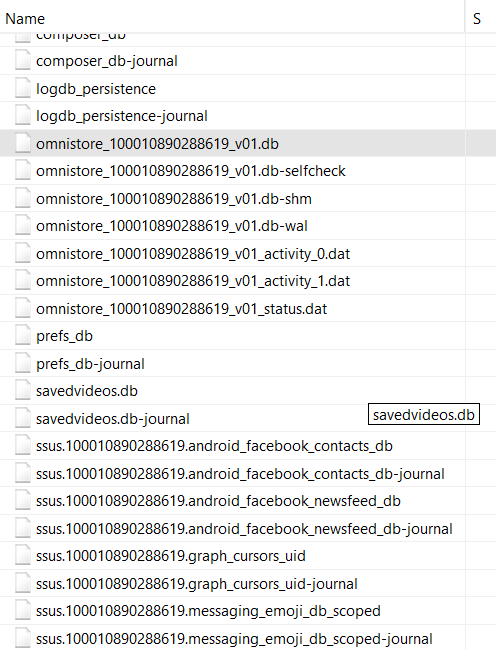
**SQL Databases**: In com.facebook.katana there is directory named databases which contained most sql databases related to user activity, friends list and log\_persistence database containing username and other information. SQL Cipher was used to examine this data with ease. Using this software also revealed a vulnerability in facebook application, such as anyone with rooted device can access this data with ease if they extract and this data is not even encrypted. These sql databases such as **omnistore\_100010890288619\_v01.db** contain sensitive data. They also contain timestamps that are useful to check conversations between users (Fig.5).

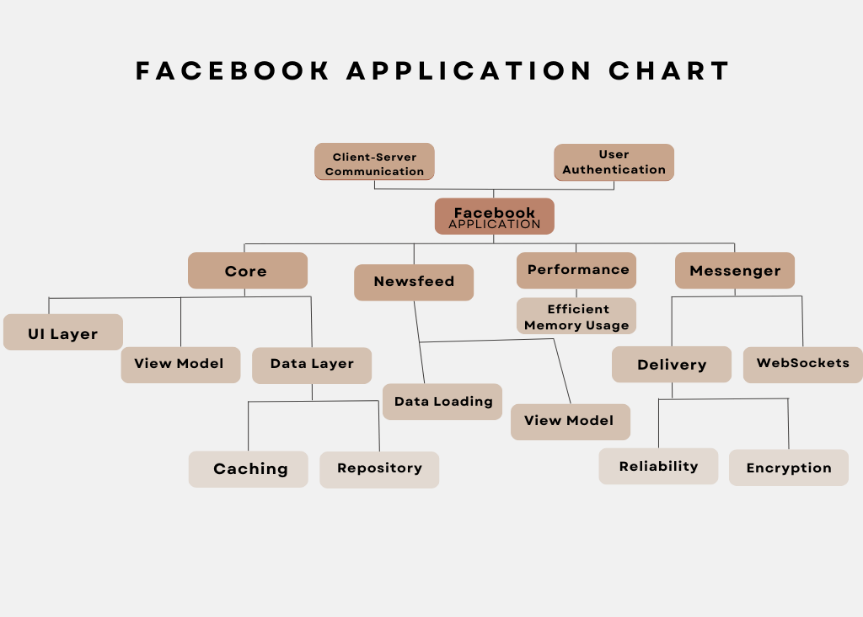
Figure 4 AndroidManifest.xml

**Found Files:** While investigating there were a lot of files founds such as .db (SQL database), .thd (Audio), .smali, .msg (Chats), .txt (text), video, etc.

Figure 5 SQL Databases

|  |  |
| --- | --- |
| **File Type** | **LOCATION** |
| Photos | com.facebook.katana/cache/image\_scoped/100010890288619 |
| Messages (Internal Facebook) | com.facebook.katana/files/mib\_msys\_echo/100010890288619/echo/AdvancedCrypto/ |
| Stickers | |  | | --- | | com.facebook.katana/cache/image\_scoped/100010890288619 | |
| Videos | com.facebook.katana/databases/ssus.100010890288619android\_facebook\_newsfeed\_db.db |
| Databases | com.facebook.katana/databases |
| Friends List | com.facebook.katana/databases/ssus.100010890288619android\_facebook\_contacts\_db.db |
| GIF | com.facebook.katana/cache/image\_scoped/100010890288619 |
| Stickers | |  | | --- | | com.facebook.katana/cache/image\_scoped/100010890288619 | |
| Facebook story | |  | | --- | | com.facebook.katana/files/fb\_temp/com.facebook.katana/fb\_temp\_7\_days/ | |
| AndroidManifest.xml | Stored beside smali code directory in decompiled apk file |

**Smali Code:** Smali codes was also extracted from .apk file that helped in analysis of all types of features in facebook like Authentication, permissions, UI, etc.

**Application Architecture** (Explained in Fig. 7)

**App Behavior**

The behavior of the application was examined using android studio application on a virtual Pixel 6 API 29 device with x86 architecture. Using logcat feature in android studio as shown in Fig. 8 we can see how it interacts as we start the application **W** stands for warning, **D** stands for debug, **I** for Info, **E** for Eror, but except there are **F** that means fatal and **V** stands for Verbose (Android Developers). All of these interactions were going to com.facebook.katana, root folder of application. For example, in the image given below in second line you can see there is a D (Debug) log, it means there is a scheduled task for updating Facebook preferences for the user. Even when the user is not using the application, logcat showed us new logs which means the application was still active and was interacting with API and server to update every 60 seconds for newer content to show on screen to the user.

Figure 6 FaceBook Architecture (Canva, 2020) (Komilov, Y. (2024))

**Recommendations**

Based on the forensic analysis of the Facebook application, the recommendations that can be made for future forensic investigators:

**Implementing Data Extraction Techniques:** Investigators can use basic and open source tools such as Autopsy, APK tool and DB Browser to extract data from the application database.

**Monitoring Application Permissions:** Users should regularly review Facebook’s permissions, such as access to storage, location, contacts, and microphones.

**Encrypt and Secure User Data:** After doing a forensic analysis on facebook it is really obvious that some databases such as omnistore\_100010890288619\_v01.db were accessible in plaintext using a any rooted device. Facebook should encrypt all types of local storage data, ensuring that sensitive user data cannot be extracted so easily.

**Conclusion**

In conclusion, this forensic investigation revealed the app behavior and found locally stored data that was stored by the Facebook application. Using tools such as APK Tool, Autopsy, DB Browser and logcat, this forensic analysis revealed key findings, including SQLite databases, cached media, log files and user interaction logs. Facebook application stores most its data in the com.facebook.katana directory, including user activity logs, friend lists, chat data and cached images. Various types of sensitive data such as contact information and API logs, can be extracted really easily that pose a big privacy risk if accessed by unauthorized individuals. The facebook application should implement a stronger data encryption method for more security and permission control to minimize security risks.

This study was performed in a virtual Android environment, but if I had more time then I would use a physical device as that might reveal more forensic evidence. Will also review the network traffic related to Facebook’s API calls and encrypted data streams could offer valuable insights into the security of data transmission.

**Bibliography**

Agrawal, A.K., Sharma, A. and Khatri, P. (2019) ‘Digital Forensic Analysis of Facebook App in Virtual Environment’, in 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom). 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 660–664. Available at: <https://ieeexplore.ieee.org/abstract/document/8991287/authors#authors> (Accessed: 22 February 2025).

Android Developers. (2019) Processes and threads overview | Android Developers. Available at: <https://developer.android.com/guide/components/processes-and-threads>.

Android Developers. (n.d.) View logs with Logcat. Available at: <https://developer.android.com/studio/debug/logcat>.

Canva. (2020) Canva. Available at: <https://www.canva.com/design/DAGgU6qMPck/nuyeJsNBZ0RCmbGk3tPYSA/edit>.

DB Browser for SQLite (no date). Available at: <https://sqlitebrowser.org/>.

Epoch Converter (no date). Available at: <https://www.epochconverter.com> (Accessed: 26 February 2025).

Eriş, F.G. and Akbal, E. (2021) ‘Forensic Analysis of Popular Social Media Applications on Android Smartphones’, Balkan Journal of Electrical and Computer Engineering, 9(4), pp. 386–397. Available at: <https://doi.org/10.17694/bajece.761271>.

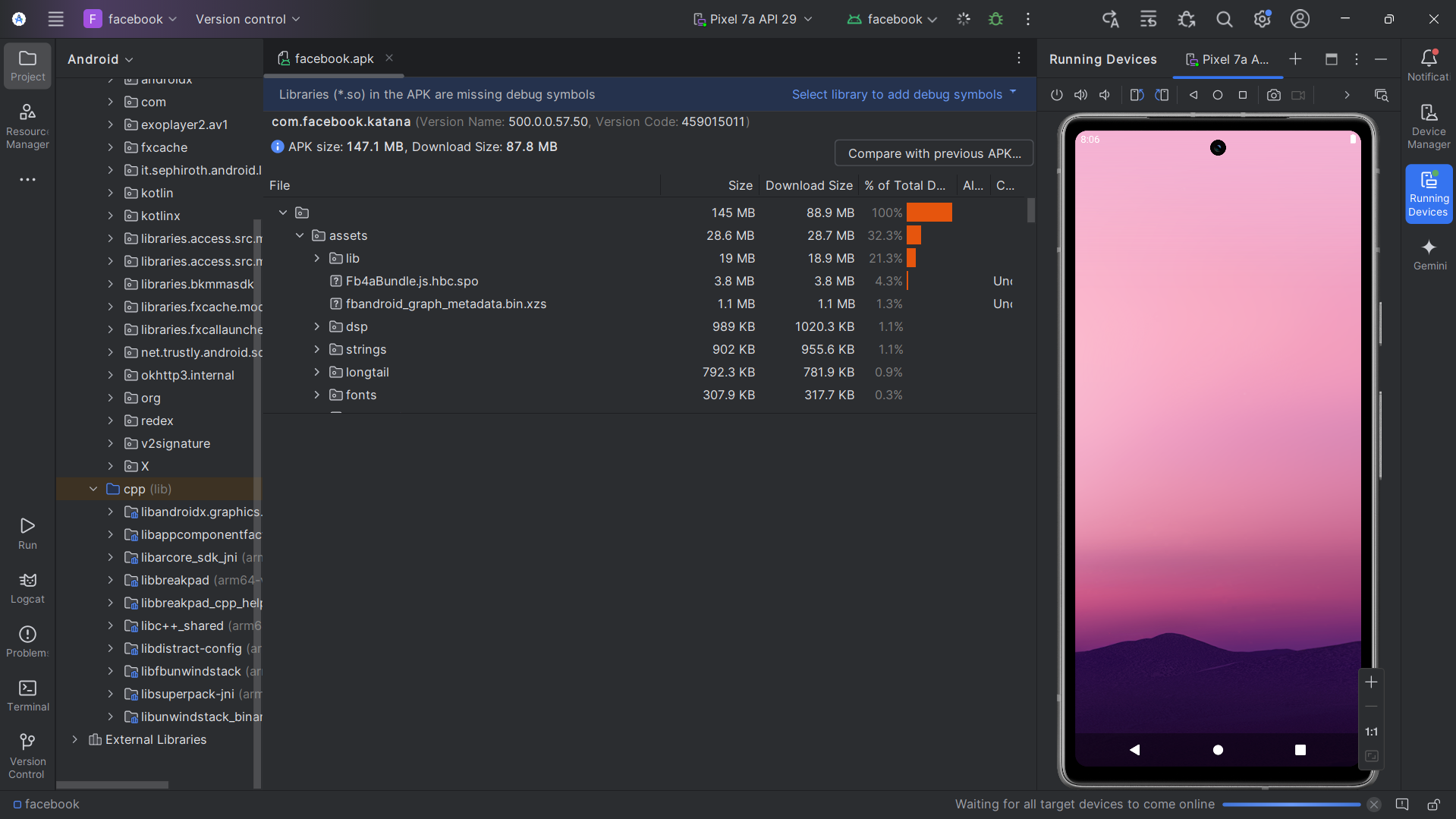
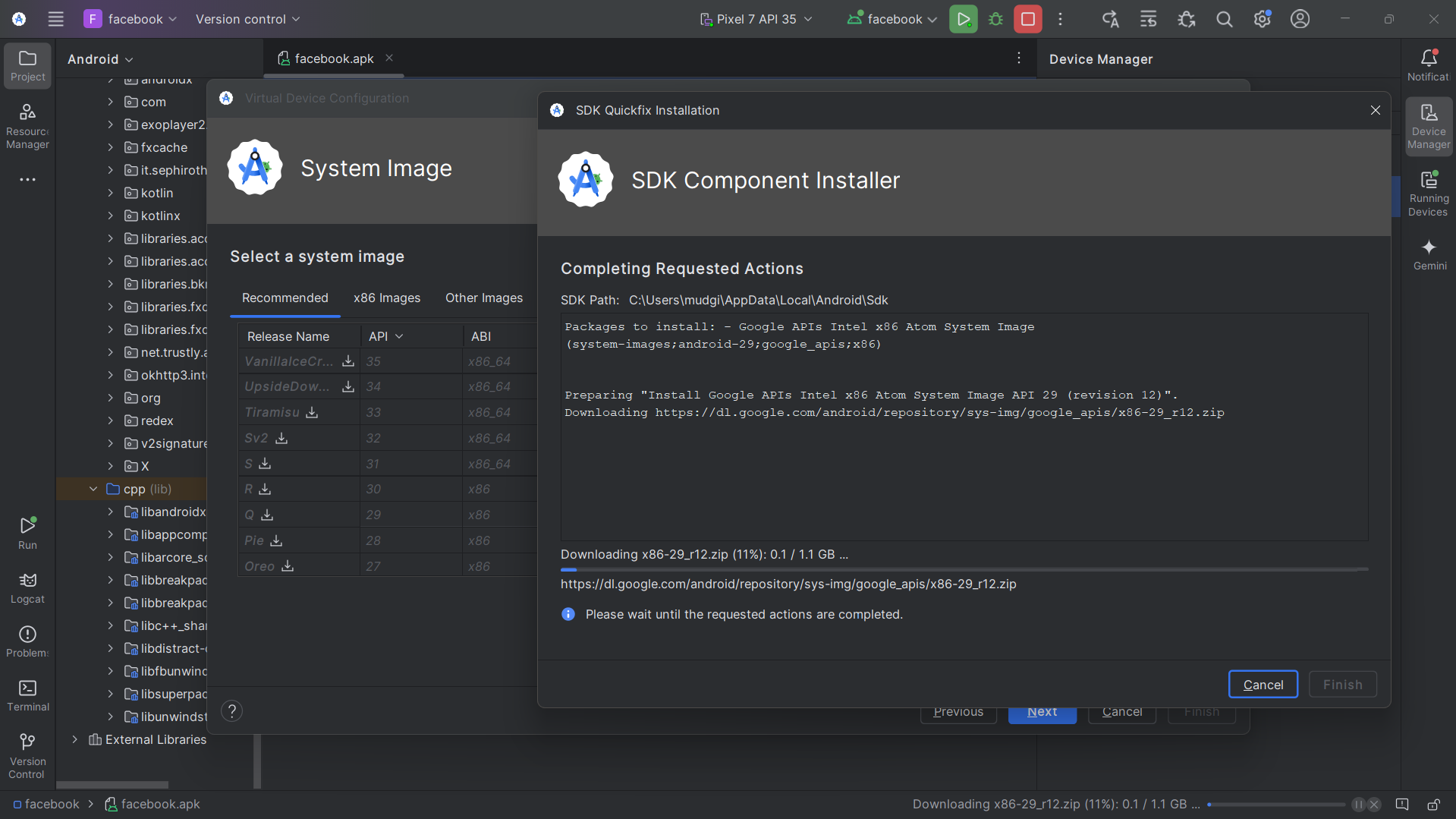
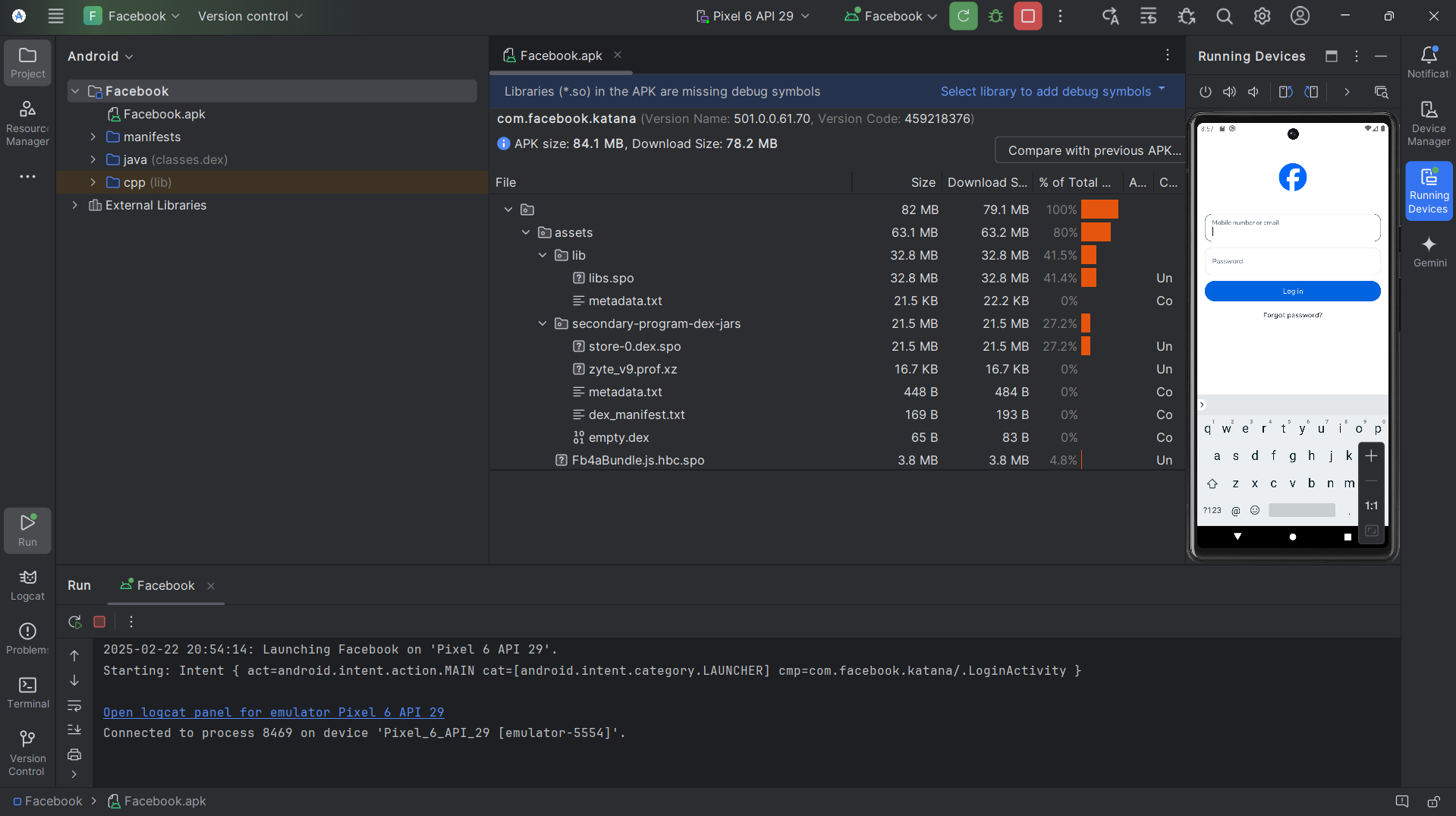
FORENSIC TECHNIQUES: HELPING ORGANIZATIONS IMPROVE THEIR RESPONSES TO INFORMATION SECURITY INCIDENTS (no date). Available at: <https://uh.edu/~pkoya/6322/assignments6322/NIST%20800-86.htm>.

Hunting the $477,000,000 FTX Hacker (2025). Available at: <https://www.youtube.com/watch?v=ima8O-DFQis> (Accessed: 26 February 2025).

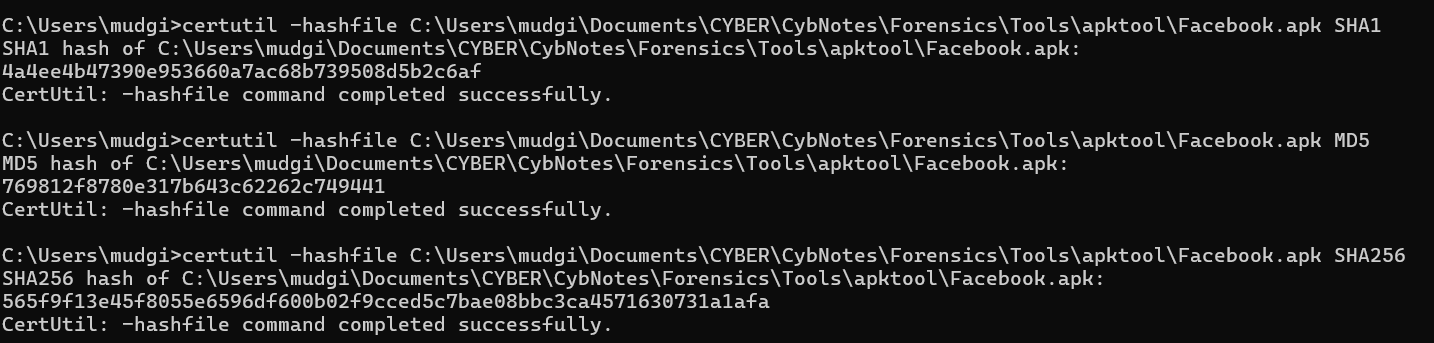
How to Install APK Files in Android Studio Emulator (3 Methods) (2022). Available at: <https://www.youtube.com/watch?v=X4bdoD8eKV8> (Accessed: 21 February 2025).

Komilov, Y. (2024) ‘System Design of Facebook’s Android App: An In-Depth Look’, Medium, 22 September. Available at: <https://medium.com/@YodgorbekKomilo/system-design-of-facebooks-android-app-an-in-depth-look-00add9b180c9>.

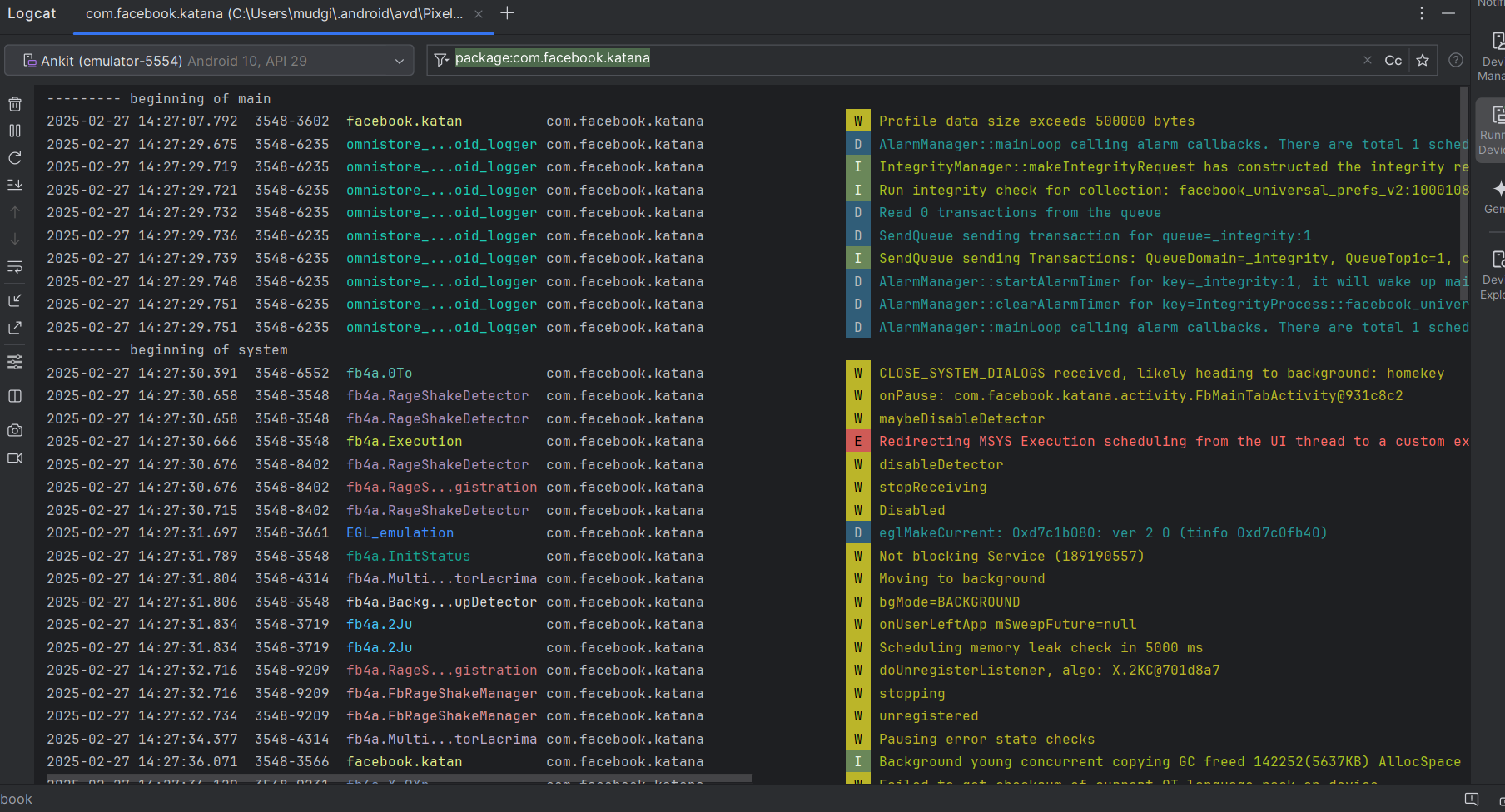
**Appendix**

1. 
2.  Installation of SDK component
3. 

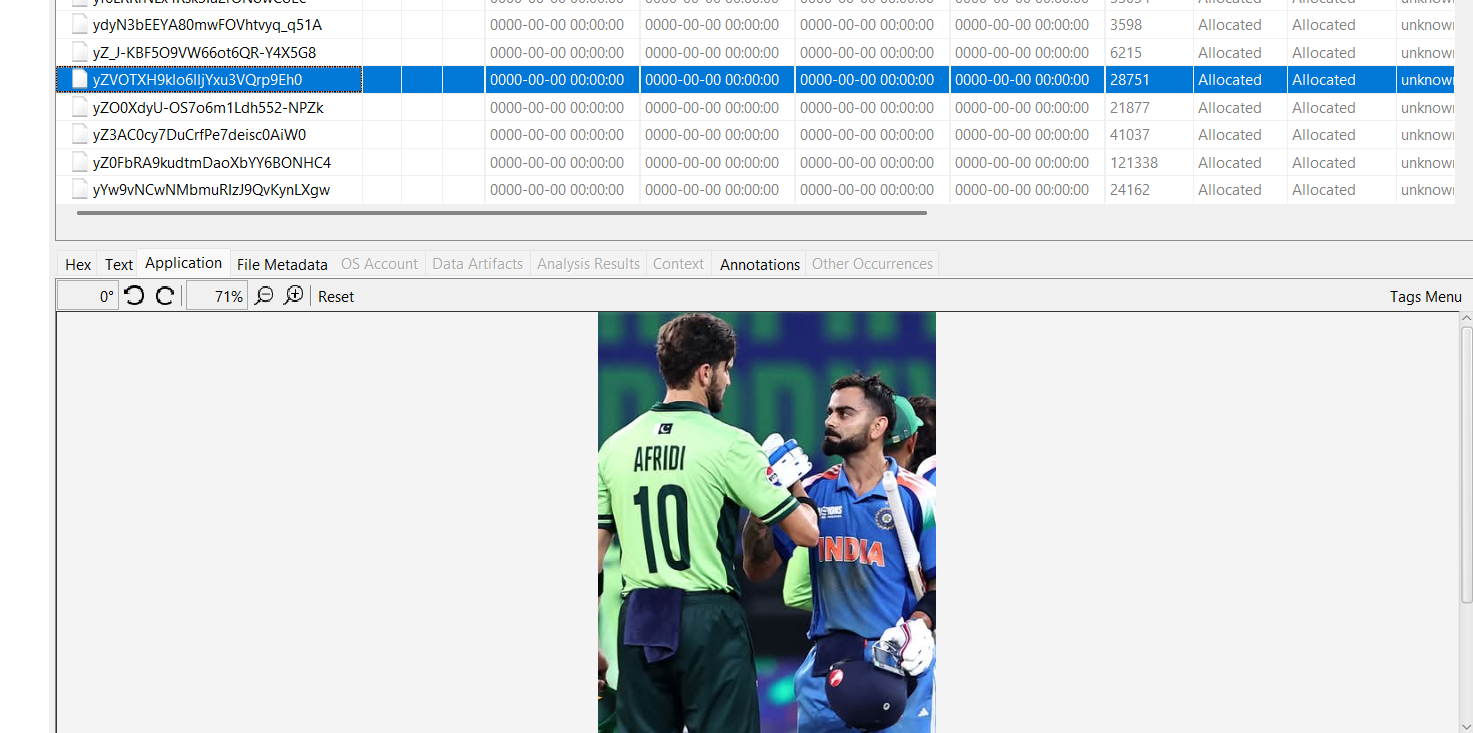
Running Facebook on Emulator

1. 

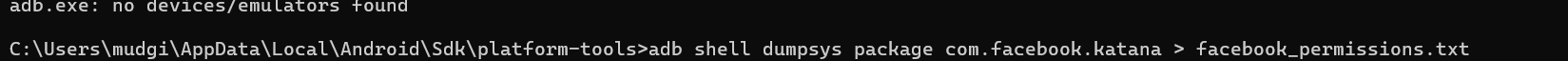
Getting Hash values of facebook .apk file

1. 

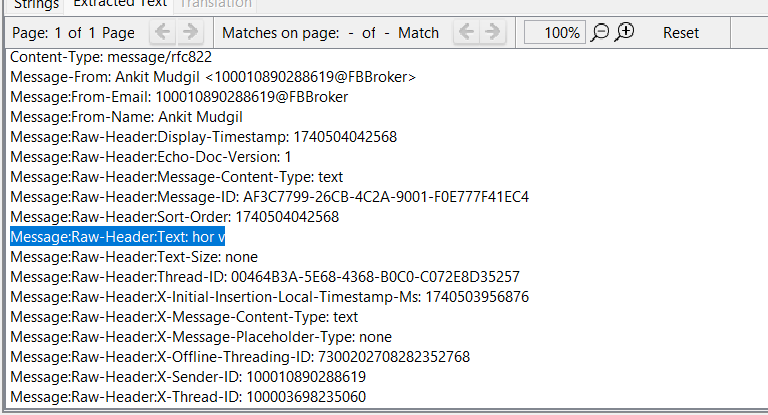
Logcat capturing logs while starting the Application

1. 

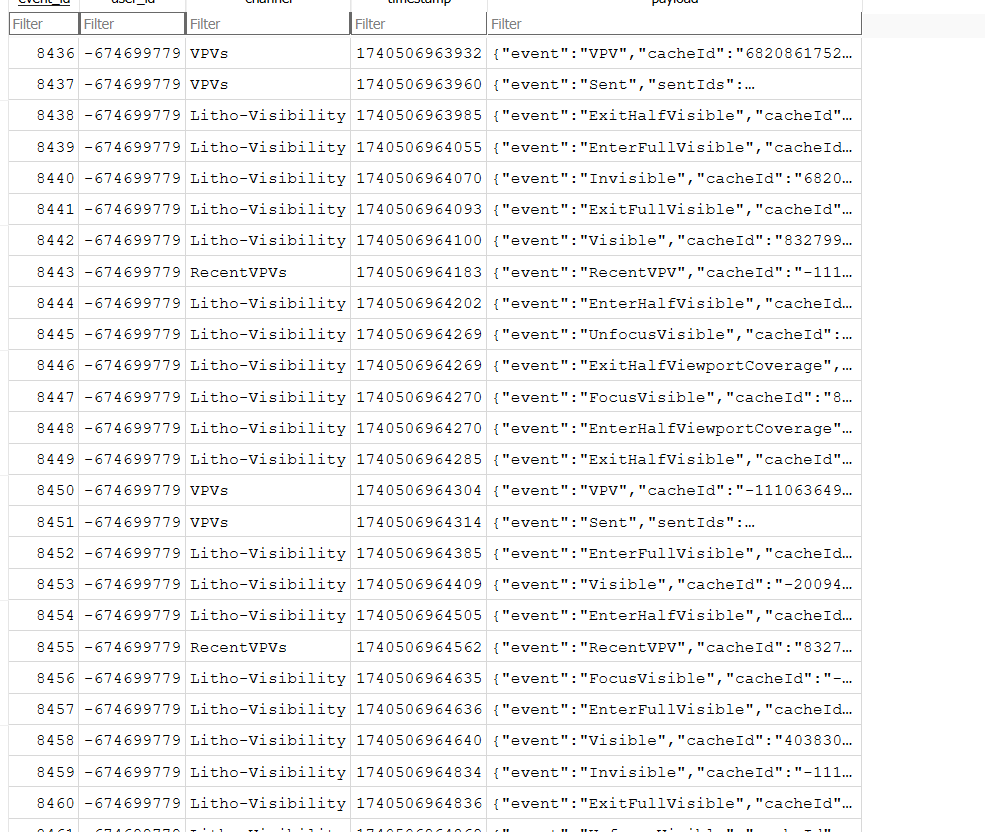
Found posts I liked

1. 

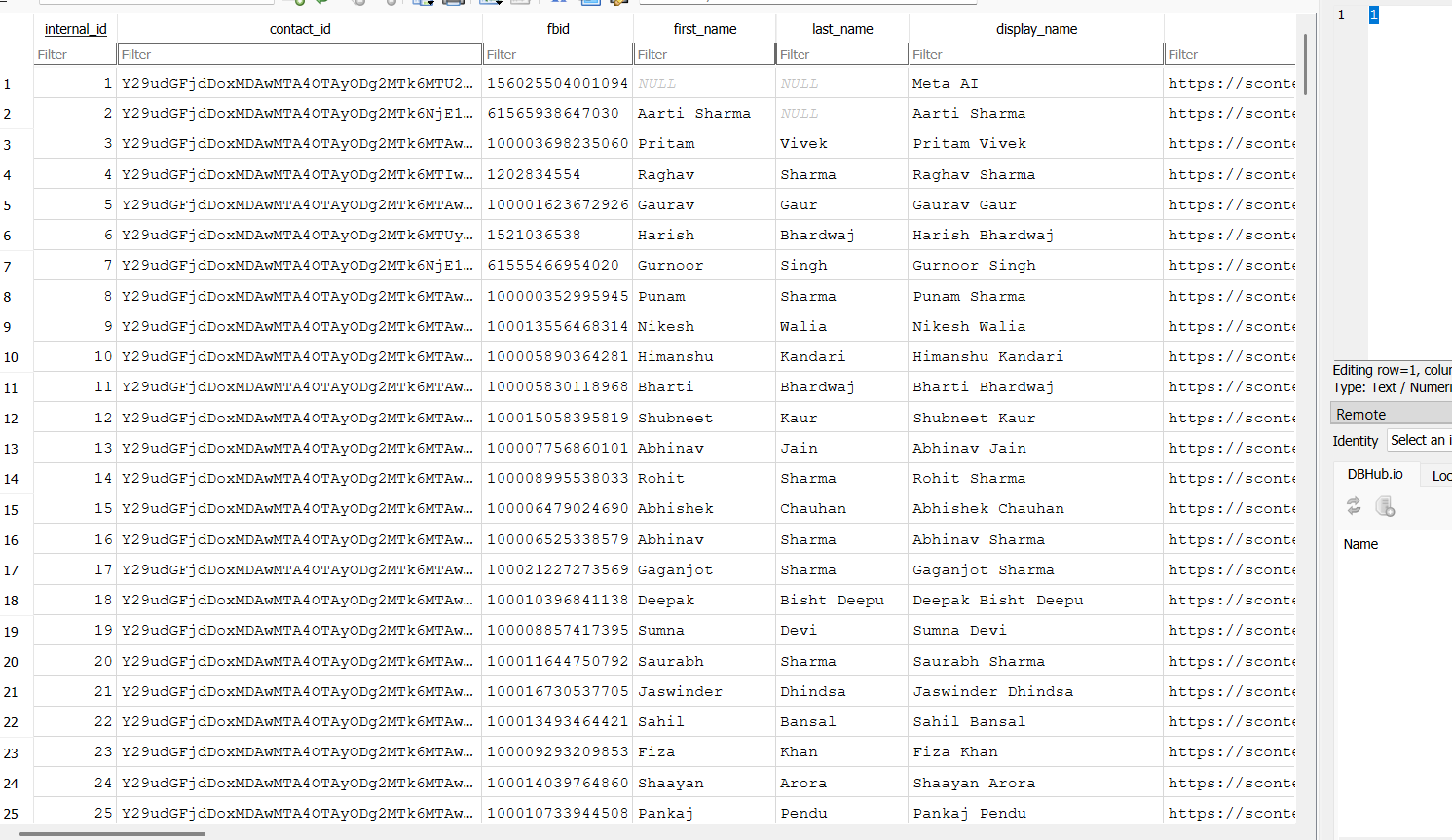
Using cmd to get permissions given to facebook application

1.  Permissions given to facebook
2. 

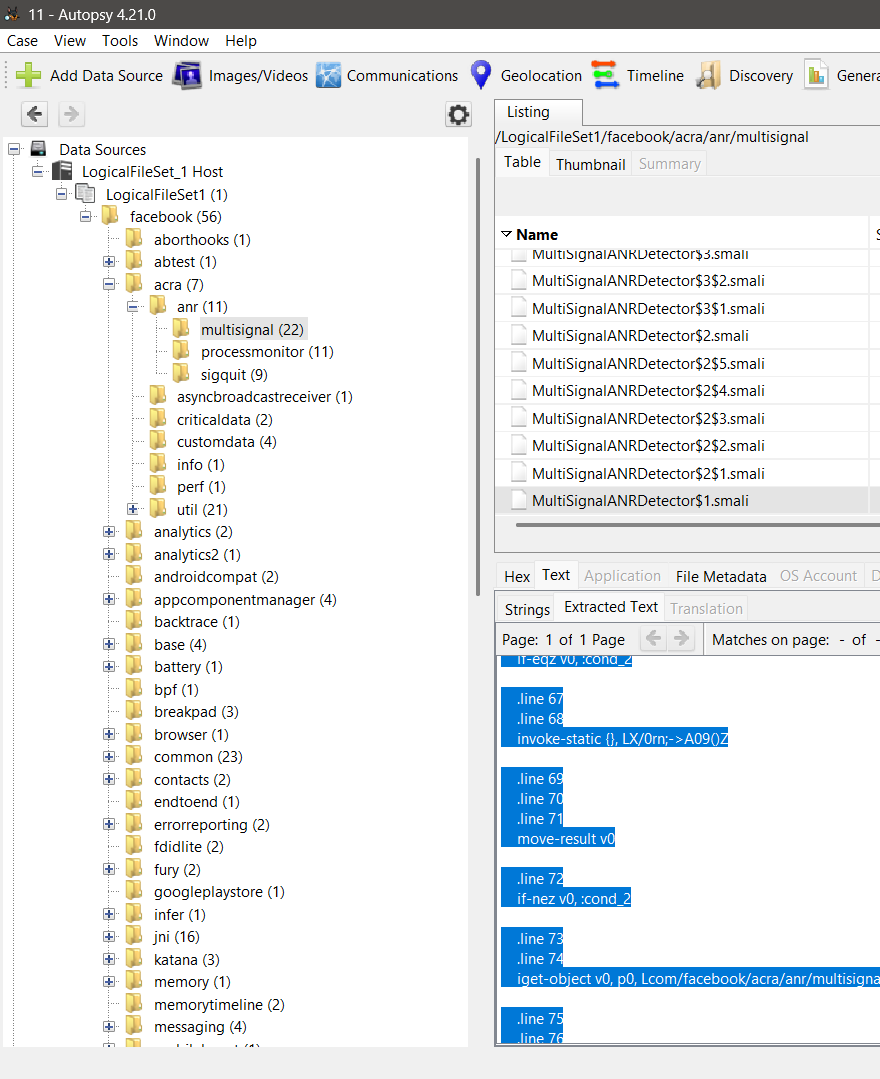
Found Messages

1. 

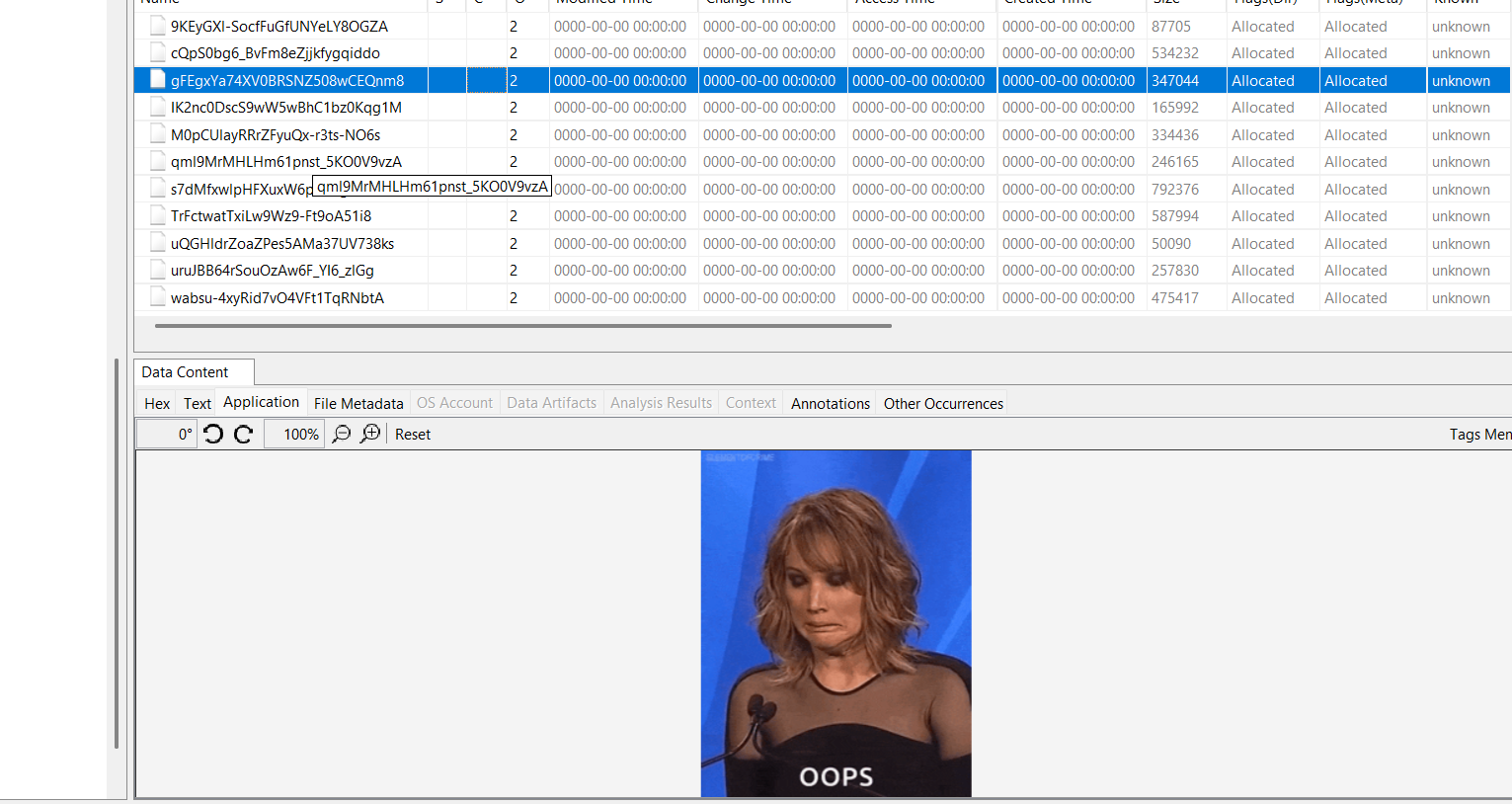
User Activity logs

1. 

Friends list

1. 

Found smali code files While Working in autopsy

1. 

Found a GIF in

1. 

Code Signature certificate