Unlock & Extract: Android Forensics

Farrukh - 24109124

Digital Forensics

Submitted to Mr. Muhammad Waqar

Project Description: Android Phone Forensics and Data Extraction

The primary objective of my project is to unlock an Android phone and extract the maximum amount of data from it for forensic analysis. The device in question belongs to an individual who has been apprehended for allegedly misappropriating funds from the office accounts. As part of the investigation, it is crucial to retrieve and analyze data from the suspect's phone to determine how the theft was carried out.

This project involves several key steps:

1. **Device Unlocking**: Gaining authorized access to the locked Android device using forensic techniques, ensuring that the integrity of the data is maintained throughout the process.
2. **Data Extraction via ADB**: Utilizing Android Debug Bridge (ADB) and other forensic tools to create a comprehensive image of the phone's data, including messages, call logs, emails, application data, and any other relevant digital evidence.
3. **Forensic Analysis**: Systematically examining the extracted data to identify evidence related to the financial misconduct. This includes tracing transactions, identifying communication patterns, and uncovering any hidden or deleted files that may provide insight into the methods used to commit the theft.
4. **Identification of Security Loopholes**: Analyzing the data to pinpoint vulnerabilities or procedural weaknesses within the organization's systems that may have been exploited. This information will be used to recommend improvements to prevent similar incidents in the future.

The goal of this project is not only to support the ongoing investigation by providing digital evidence but also to help the organization understand how the breach occurred. By identifying the loopholes that were exploited, the project aims to contribute to strengthening the organization's security protocols and preventing future incidents of this nature.

Step 1: Device Unlocking and Preservation of Logged-In States

The initial phase of our forensic investigation focused on unlocking the suspect's Android phone. To achieve this, we systematically attempted to bypass the device's security by entering multiple password combinations. It is a common oversight for individuals to set easily guessable passwords, such as the last four digits of their phone number or the phone number itself. In this particular case, the suspect had indeed used such a predictable password, which allowed us to successfully unlock the device.

A critical aspect of forensic best practices is to ensure that, once the device is unlocked, it remains disconnected from any Wi-Fi or mobile networks. This precaution is essential to prevent the device from communicating with external servers, which could result in automatic logouts from important applications or the remote wiping of data. By keeping the device offline, we preserved the logged-in states of all relevant accounts and applications, thereby maintaining the integrity of potential digital evidence.

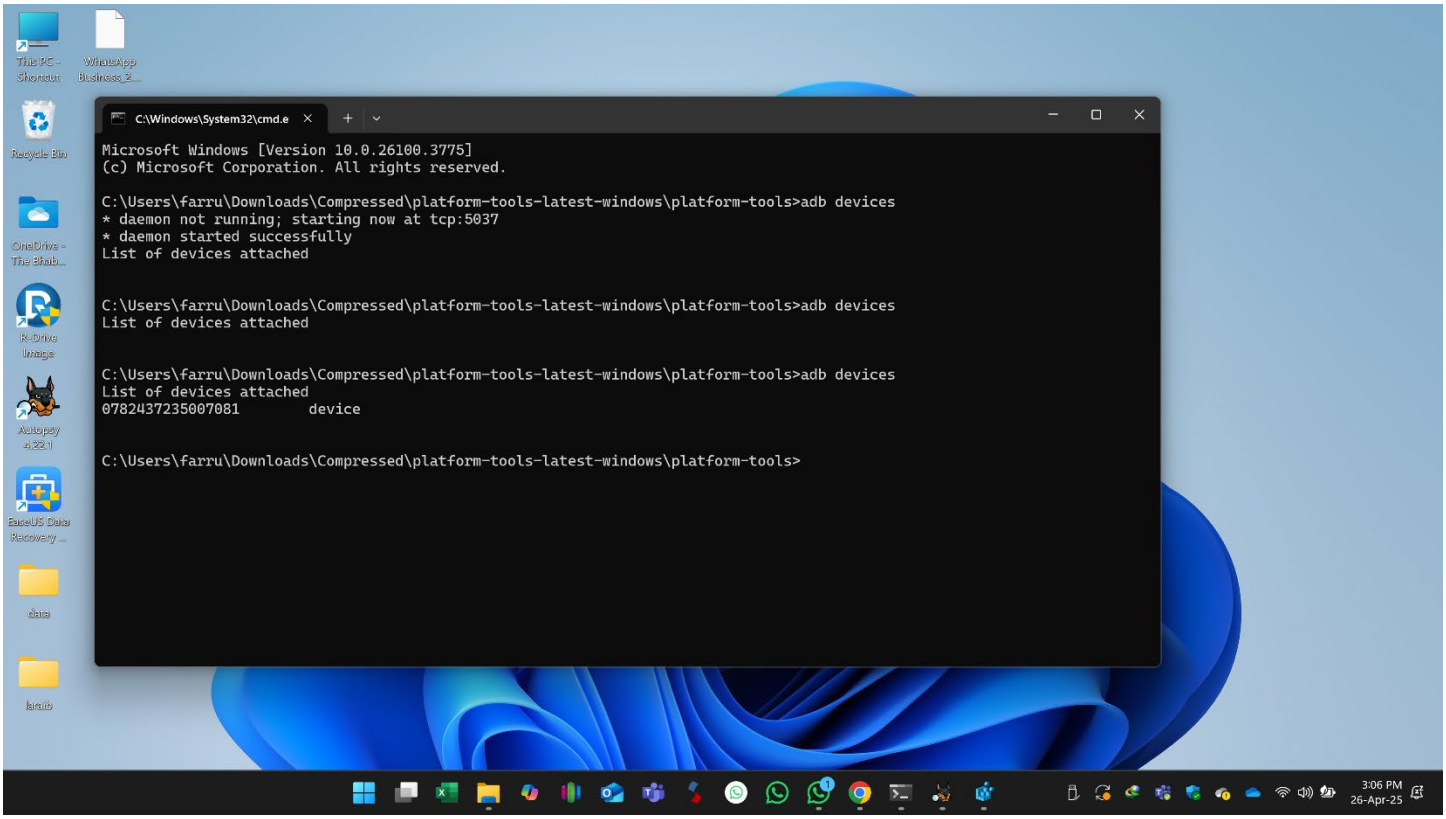
As a result of these measures, we were able to unlock the phone without triggering any security responses or data loss. All accounts and applications remained accessible in their logged-in state, providing us with a comprehensive and unaltered dataset for subsequent forensic analysis.

Step 2: Data Extraction Using ADB Tool

In the second phase of the project, we utilized the Android Debug Bridge (ADB) tool, which is recognized as a safe and legally accepted method for conducting forensic investigations on Android devices. ADB is a versatile command-line utility that allows investigators to communicate directly with an Android device from a host computer, enabling a wide range of actions such as accessing files, creating backups, and extracting digital evidence.

To begin, we enabled USB debugging on the device and established a secure connection between the phone and our forensic workstation. Using ADB, we systematically copied the internal media and data from the phone, including files, application data, and other relevant artifacts. This process ensures that a comprehensive image of the device's contents is created for further analysis, while maintaining the integrity and authenticity of the evidence.

Throughout this step, we adhered to forensic best practices by documenting each action, preserving the original state of the device, and ensuring that the extraction process did not alter or compromise the data. The use of ADB in this context is widely regarded as an effective and forensically sound approach for acquiring digital evidence from Android phones.



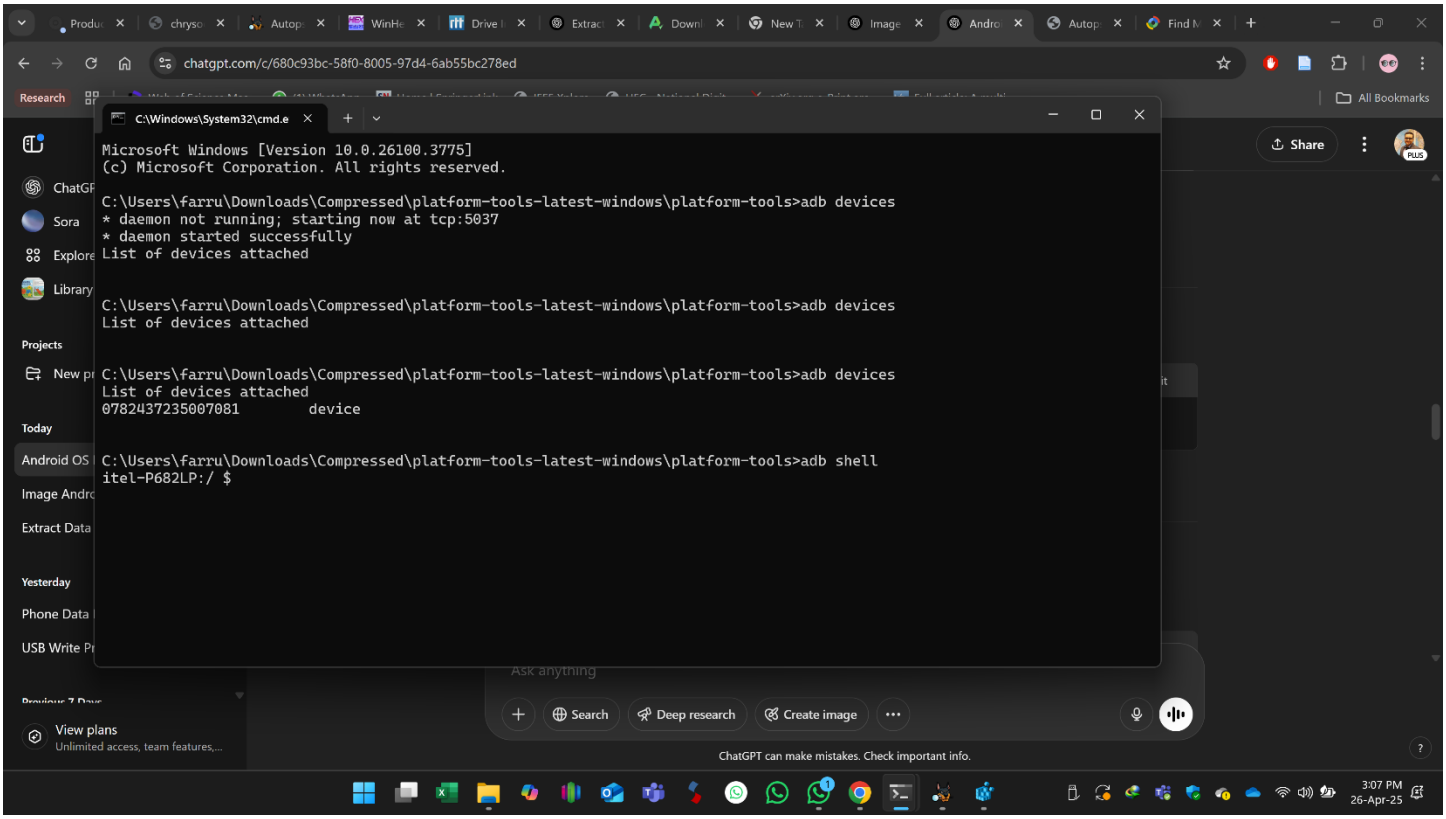
Step 3: Locating and Imaging Media Data via ADB Shell

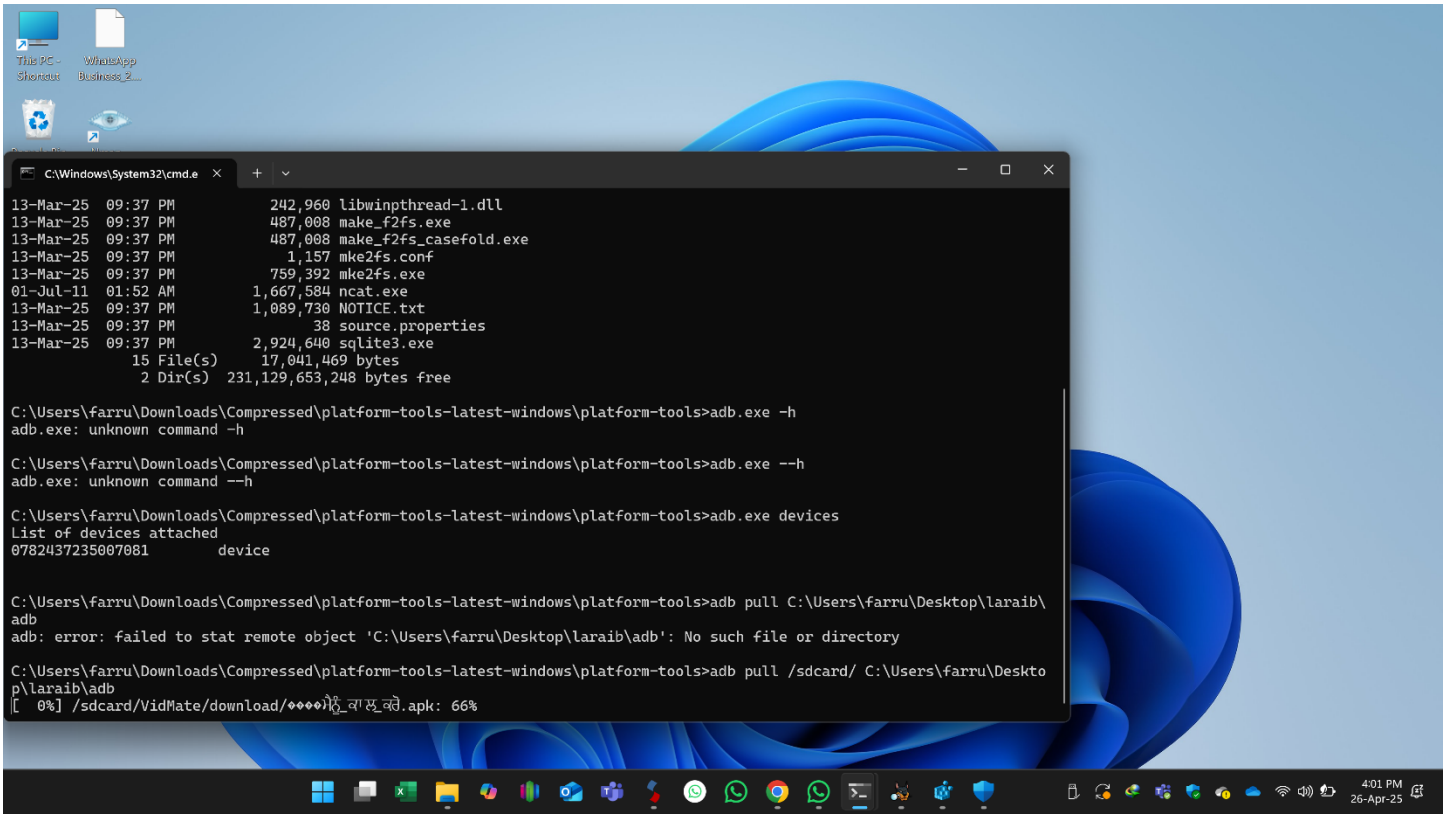
After establishing a shell session on the device using ADB, we proceeded to identify the specific directory paths where media files were stored. This typically involves navigating through the device's file system—commonly targeting directories such as /sdcard/DCIM, /sdcard/Pictures, or other relevant locations where photos, videos, and other media are saved.

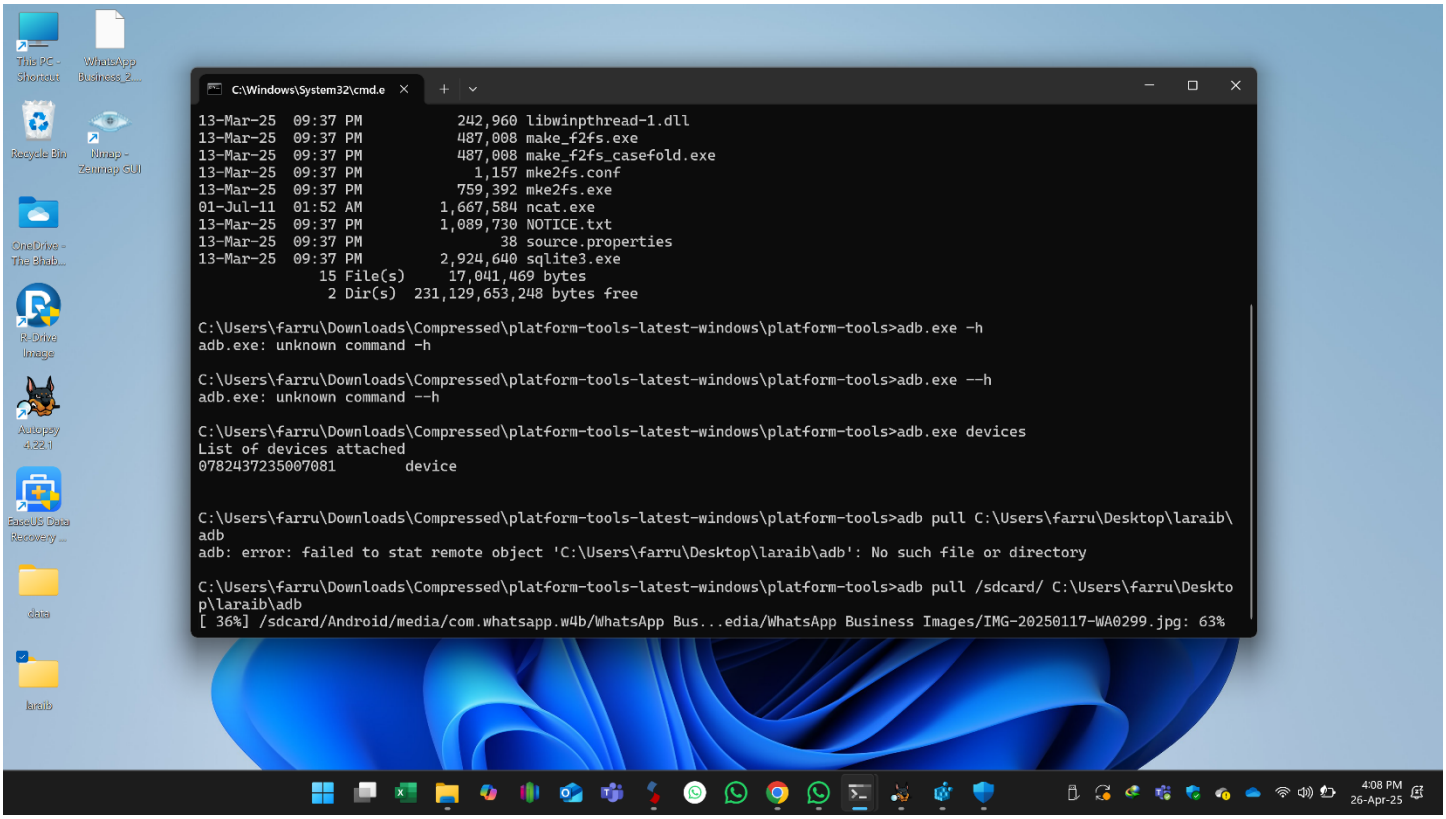
Once the correct paths were identified, we created a forensic image of the media data. This was accomplished by using ADB commands to either directly copy the files or, for a more comprehensive approach, by utilizing tools like dd to generate a bit-by-bit image of the relevant storage partitions. For example, the dd command can be used within the shell to create an image file of a partition or directory, which is then transferred to the forensic workstation using adb pull.

Throughout this process, all actions were carefully documented to maintain the chain of custody and ensure the integrity of the evidence. The resulting image files were stored securely on our analysis system, ready for detailed forensic examination using specialized tools.

This methodical approach ensures that all relevant media data is preserved in its original state, enabling thorough and reliable forensic analysis.




C:\Windows\System32\cmd.e
13-Mar-25 09:37 PM   242,960 libwinpthread-1.dll
13-Mar-25 09:37 PM   487,008 make_f2fs.exe
13-Mar-25 09:37 PM   487,008 make_f2fs_casefold.exe
13-Mar-25 09:37 PM   1,157 mke2fs.conf
13-Mar-25 09:37 PM   759,392 mke2fs.exe
01-Jul-11 01:52 AM   1,667,584 ncat.exe
13-Mar-25 09:37 PM   1,089,730 NOTICE.txt
13-Mar-25 09:37 PM   38 source.properties
13-Mar-25 09:37 PM   2,924,640 sqlite3.exe
              15 File(s)   17,041,469 bytes
               2 Dir(s) 231,129,653,248 bytes free
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe -h
adb.exe: unknown command -h
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe --h
adb.exe: unknown command --h
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe devices
List of devices attached
0782437235007081   device
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb pull C:\Users\farru\Desktop\laraib\
adb
adb: error: failed to stat remote object 'C:\Users\farru\Desktop\laraib\adb': No such file or directory
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb pull /sdcard/ C:\Users\farru\Deskto
p\laraib\adb
[0%] /sdcard/VidMate/download/
.apk: 66%
4:01 PM
26-Apr-25


C:\Windows\System32\cmd.e
13-Mar-25 09:37 PM   242,960 libwinpthread-1.dll
13-Mar-25 09:37 PM   487,008 make_f2fs.exe
13-Mar-25 09:37 PM   487,008 make_f2fs_casefold.exe
13-Mar-25 09:37 PM   1,157 mke2fs.conf
13-Mar-25 09:37 PM   759,392 mke2fs.exe
01-Jul-11 01:52 AM   1,667,584 ncat.exe
13-Mar-25 09:37 PM   1,089,730 NOTICE.txt
13-Mar-25 09:37 PM   38 source.properties
13-Mar-25 09:37 PM   2,924,640 sqlite3.exe
              15 File(s)   17,041,469 bytes
               2 Dir(s) 231,129,653,248 bytes free
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe -h
adb.exe: unknown command -h
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe --h
adb.exe: unknown command --h
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe devices
List of devices attached
0782437235007081   device
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb pull C:\Users\farru\Desktop\laraib\
adb
adb: error: failed to stat remote object 'C:\Users\farru\Desktop\laraib\adb': No such file or directory
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb pull /sdcard/ C:\Users\farru\Deskto
p\laraib\adb
[36%] /sdcard/Android/media/com.whatsapp.w4b/WhatsApp Bus...edia/WhatsApp Business Images/IMG-20250117-WA0299.jpg: 63%
4:08 PM
26-Apr-25

Step 4: Creating a Full Device Backup via Fastboot

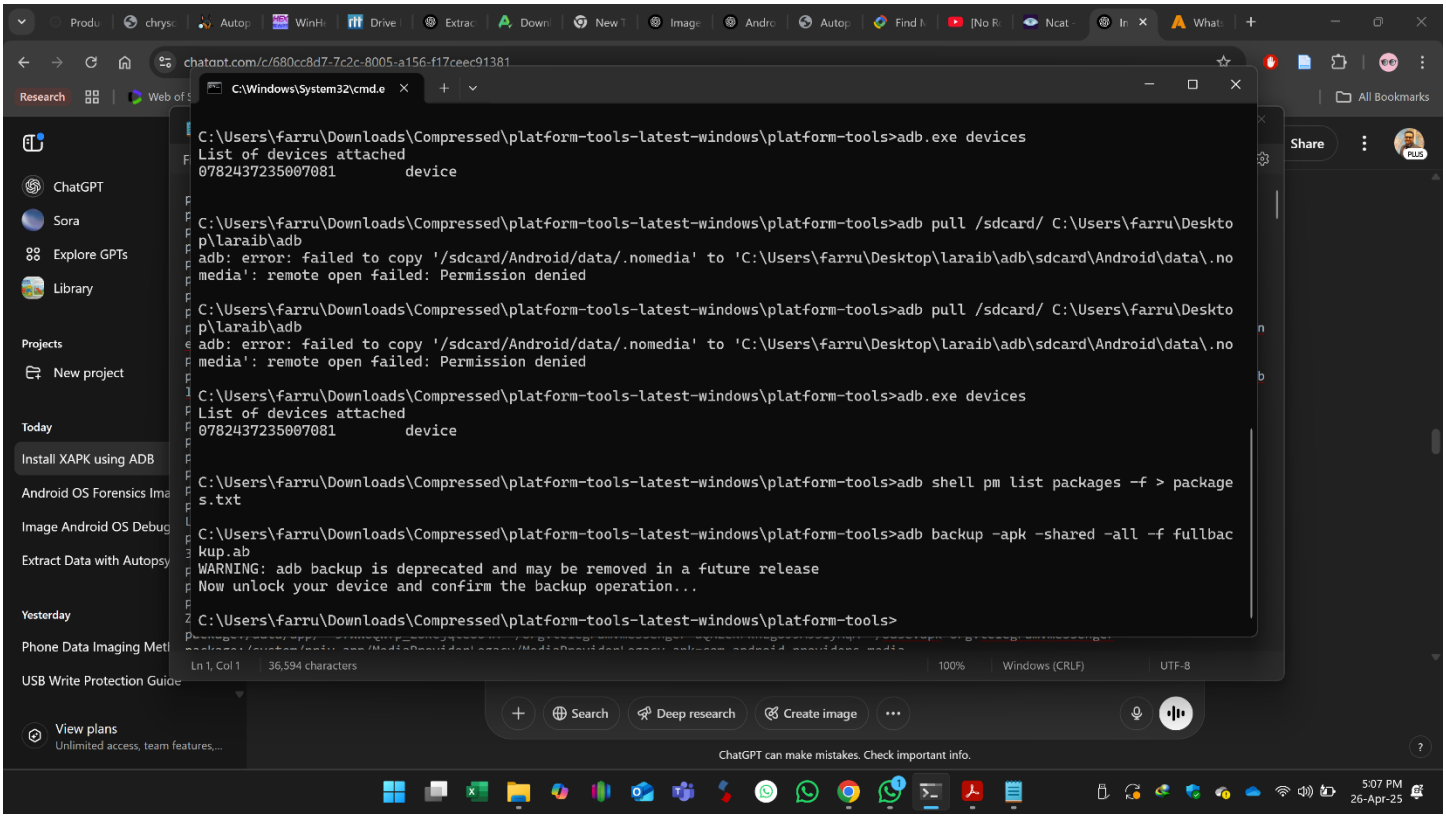
After successfully imaging the media files, the next step involved creating a comprehensive backup of the entire phone. For this purpose, we utilized the **Fastboot** tool, which is a powerful utility commonly used in Android forensics to access and extract low-level device data.

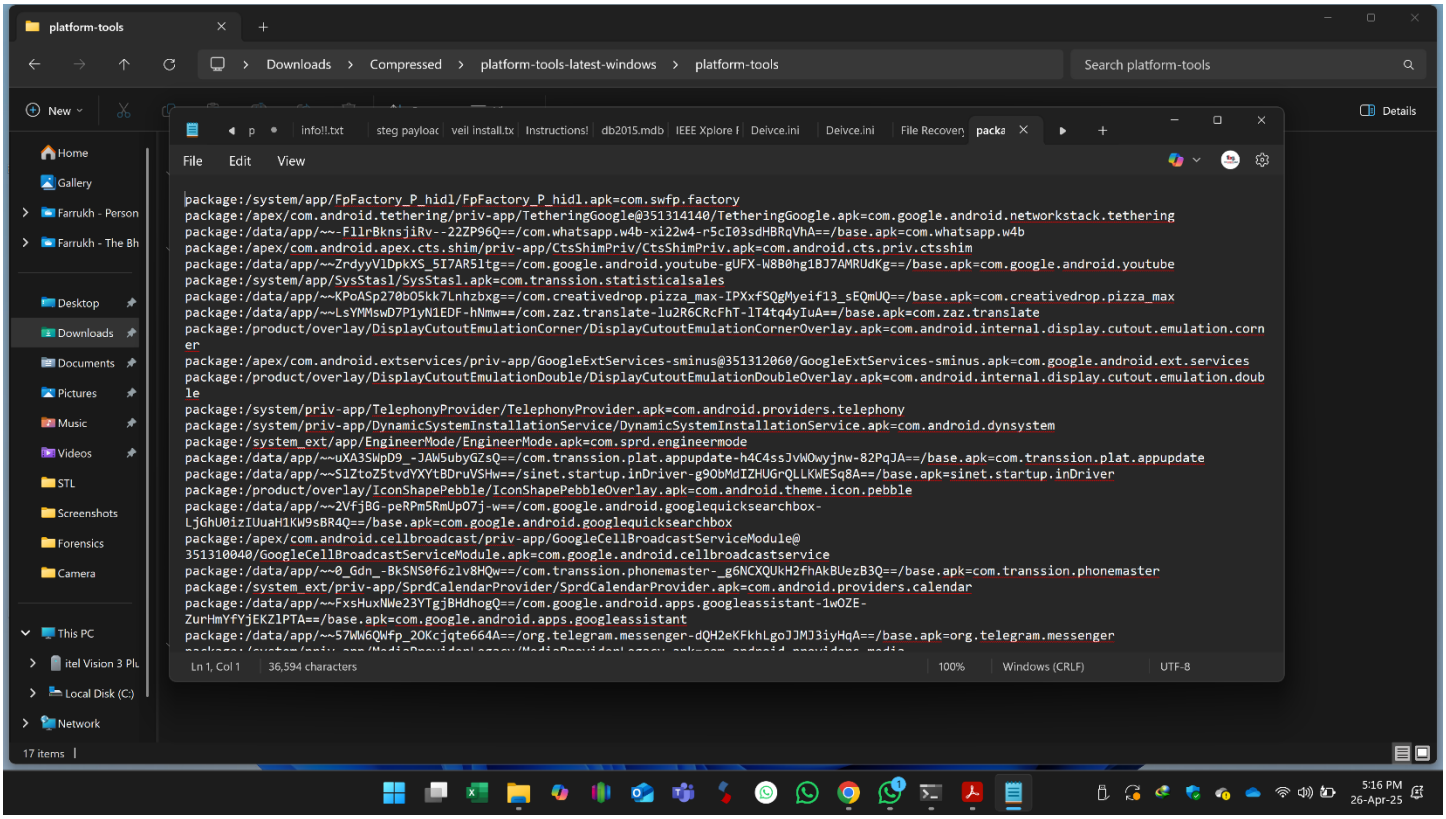
By booting the device into Fastboot mode, we were able to perform a full backup that included:

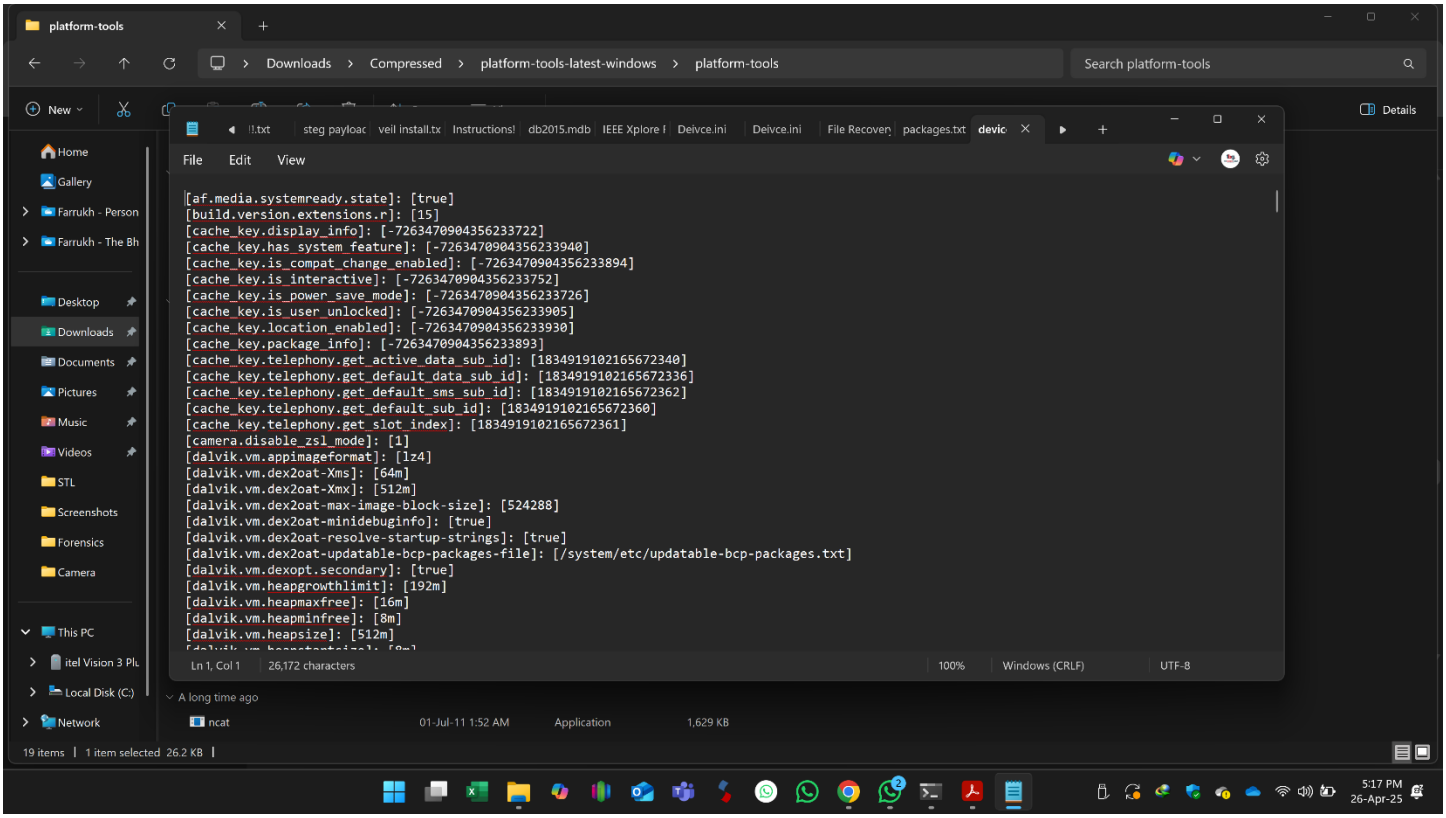
- **Running Processes:** Capturing the current state of processes and services running on the device at the time of acquisition.
- **Installed Applications:** Creating a record of all apps installed on the device, which can provide insight into user activity and potential tools used in the alleged misconduct.
- **System Dumps:** Extracting system-level data, including configuration files, logs, and system partitions, which are crucial for understanding how the device was used and whether any tampering or data manipulation occurred.
- **Device Information:** Collecting metadata such as device model, serial number, firmware version, and other identifying details necessary for forensic documentation.

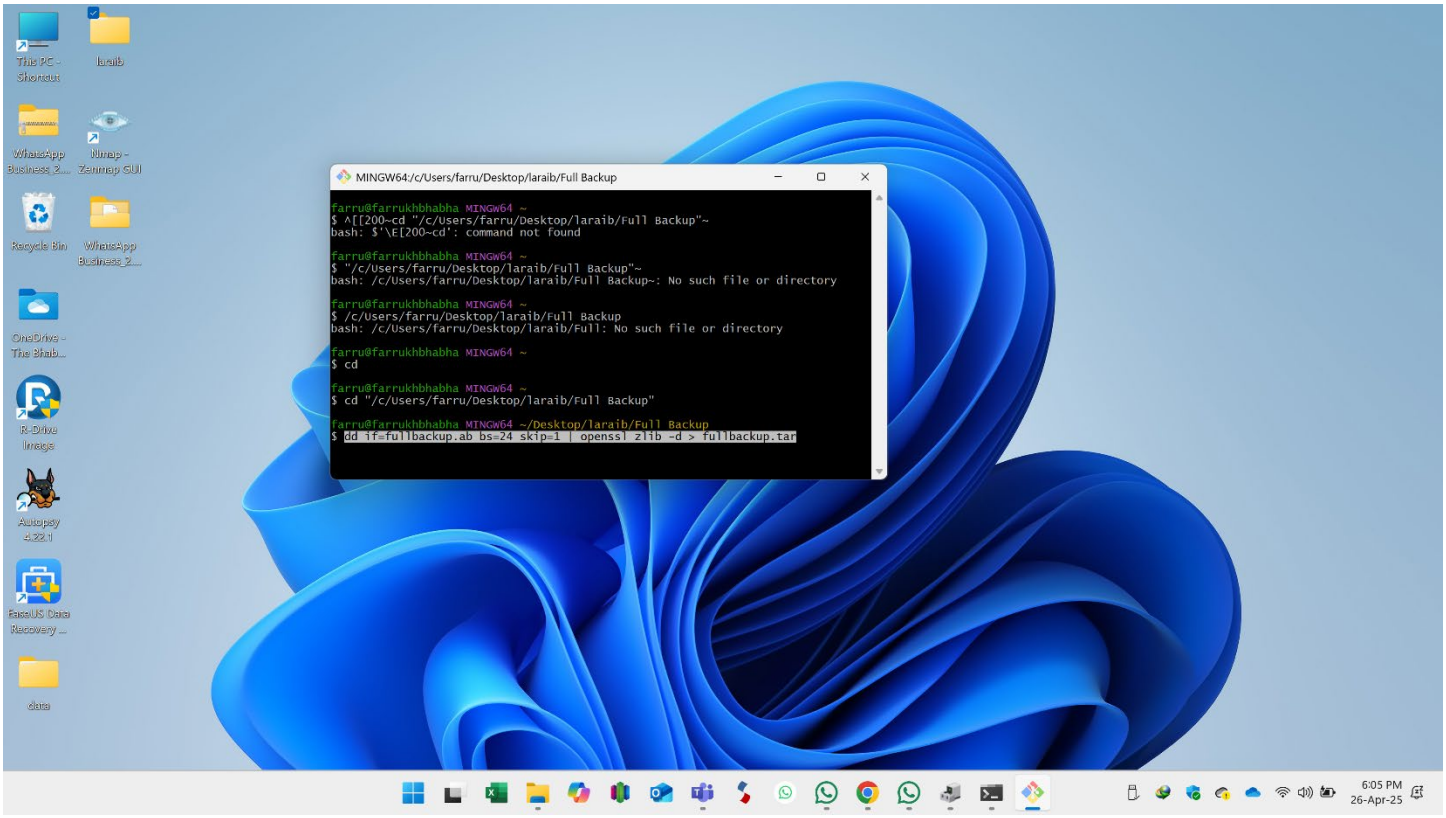
This full backup approach is essential in forensic investigations, as it ensures that all possible evidence is preserved for subsequent analysis. By acquiring a complete snapshot of the device's state, we maximize the chances of uncovering critical information related to the case, such as hidden files, deleted data, or traces of suspicious activity.

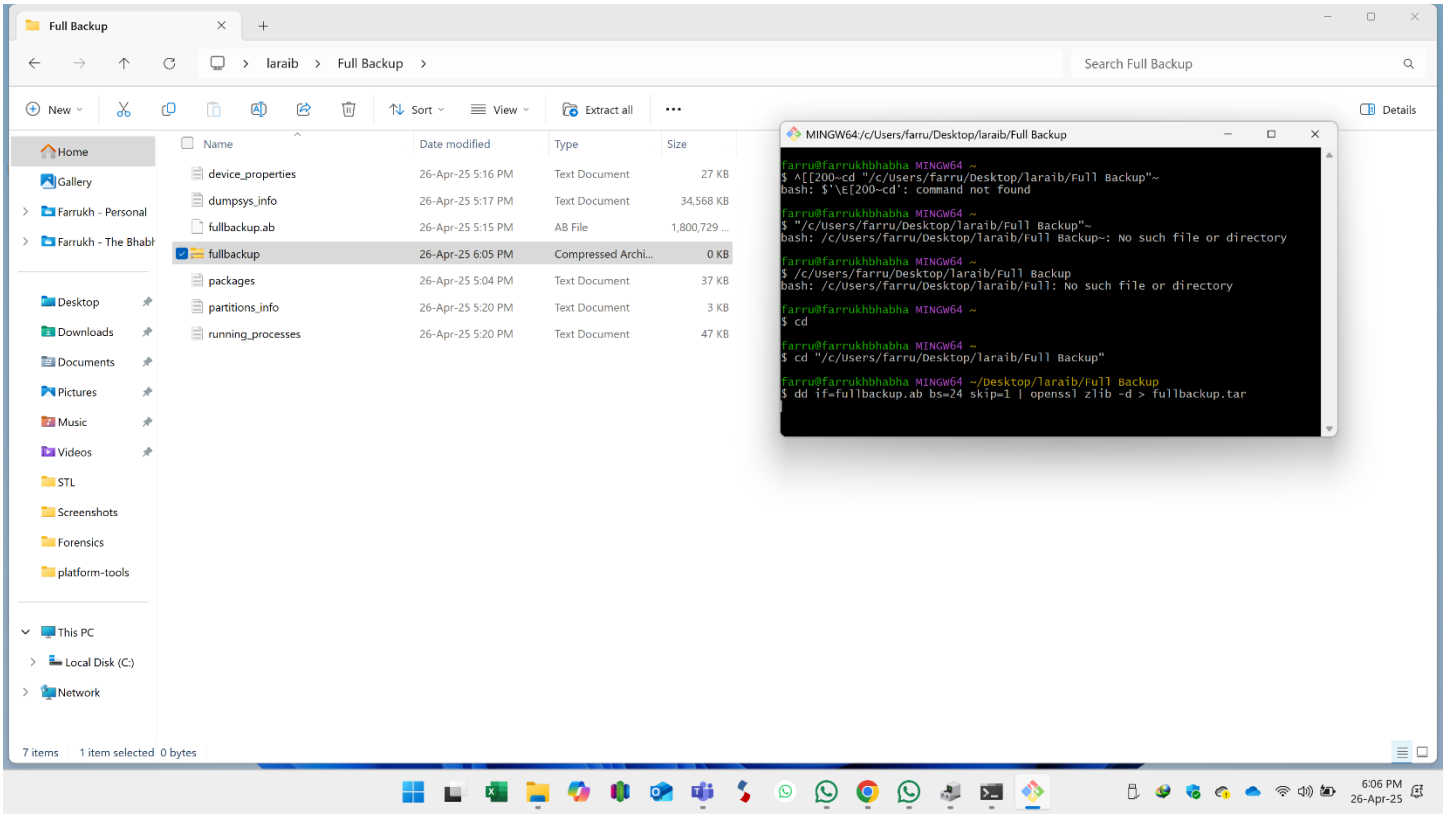
All steps were performed while maintaining forensic best practices, including detailed documentation and ensuring the integrity and authenticity of the acquired data. This comprehensive backup forms the foundation for a thorough and reliable forensic examination.

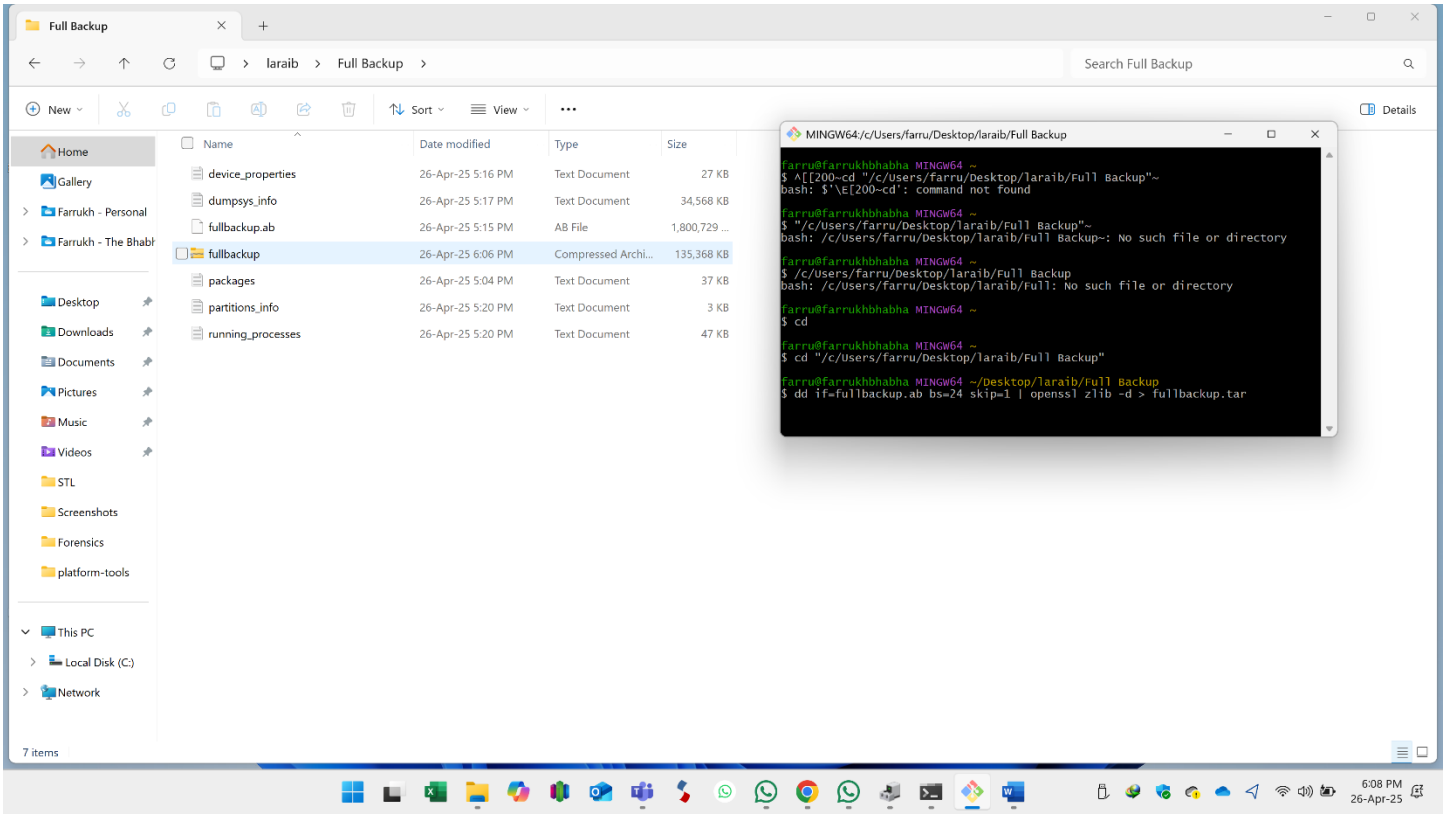

C:\Windows\System32\cmd.e
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe devices
List of devices attached
0782437235007081 device
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb pull /sdcard/ C:\Users\farru\Desktop\laraib\adb
adb: error: failed to copy '/sdcard/Android/data/.nomedia' to 'C:\Users\farru\Desktop\laraib\adb\sdcard\Android\data\.nomedia': remote open failed: Permission denied
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb pull /sdcard/ C:\Users\farru\Desktop\laraib\adb
adb: error: failed to copy '/sdcard/Android/data/.nomedia' to 'C:\Users\farru\Desktop\laraib\adb\sdcard\Android\data\.nomedia': remote open failed: Permission denied
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb.exe devices
List of devices attached
0782437235007081 device
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb shell pm list packages -f > packages.txt
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>adb backup -apk -shared -all -f fullbackup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
C:\Users\farru\Downloads\Compressed\platform-tools-latest-windows\platform-tools>
ChatGPT
Sora
Explore GPTs
Library
Projects
New project
Today
Install XAPK using ADB
Android OS Forensics Ima
Image Android OS Debug
Extract Data with Autopsy
Yesterday
Phone Data Imaging Meth
USB Write Protection Guide
View plans
Unlimited access, team features,...
Search
Deep research
Create image
ChatGPT can make mistakes. Check important info.
Share
5:07 PM
26-Apr-25

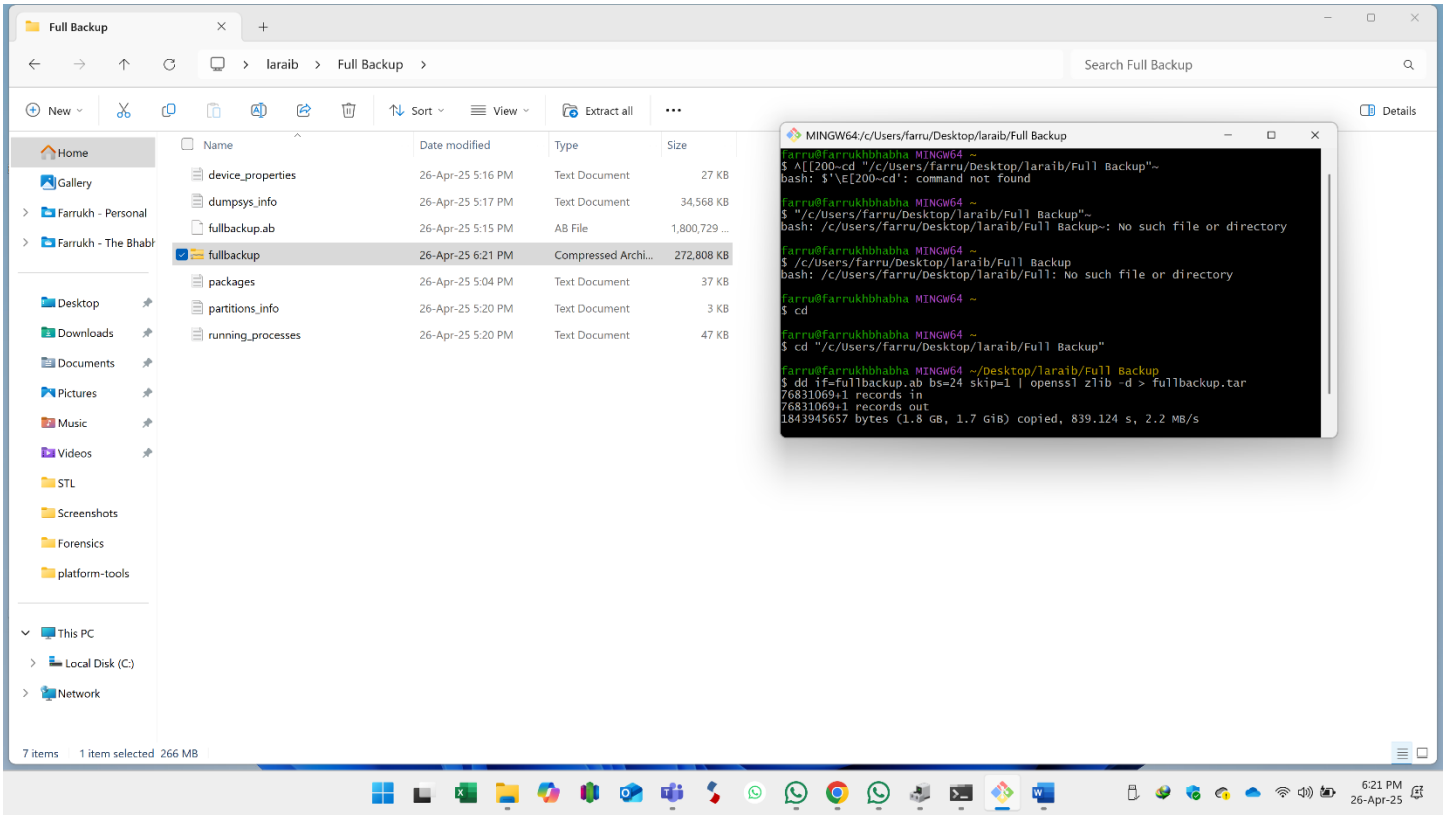

platform-tools
Downloads › Compressed › platform-tools-latest-windows › platform-tools
Search platform-tools
File Edit View
package:/system/app/FpFactory_P_hidl/FpFactory_P_hidl.apk=com.swfp.factory
package:/apex/com.android.tethering/priv-app/TetheringGoogle@351314140/TetheringGoogle.apk=com.google.android.networkstack.tethering
package:/data/app/~~-F1lrBknsjiRv--22ZP96Q==/com.whatsapp.w4b-xi22w4-r5cI03sdHBRqVhA==/base.apk=com.whatsapp.w4b
package:/apex/com.android.apex.cts.shim/priv-app/CtsShimPriv/CtsShimPriv.apk=com.android.cts.priv.ctsshim
package:/data/app/~~ZrdyyVlDpkXS_5I7AR5ltg==/com.google.android.youtube-gUFX-W8B0hg1BJ7AMRUdKg==/base.apk=com.google.android.youtube
package:/system/app/SysStas1/SysStas1.apk=com.transsion.statisticalsales
package:/data/app/~~KPoASp270bO5kk7Lnhzbxg==/com.creativedrop.pizza_max-IPXxfSQgMyeif13_sEQmUQ==/base.apk=com.creativedrop.pizza_max
package:/data/app/~~LsYMMswD7P1yN1EDF-hNmw==/com.zaz.translate-lu2R6CRcFhT-lT4tq4yIuA==/base.apk=com.zaz.translate
package:/product/overlay/DisplayCutoutEmulationCorner/DisplayCutoutEmulationCornerOverlay.apk=com.android.internal.display.cutout.emulation.corner
package:/apex/com.android.extservices/priv-app/GoogleExtServices-sminus@351312060/GoogleExtServices-sminus.apk=com.google.android.ext.services
package:/product/overlay/DisplayCutoutEmulationDouble/DisplayCutoutEmulationDoubleOverlay.apk=com.android.internal.display.cutout.emulation.double
package:/system/priv-app/TelephonyProvider/TelephonyProvider.apk=com.android.providers.telephony
package:/system/priv-app/DynamicSystemInstallationService/DynamicSystemInstallationService.apk=com.android.dynsystem
package:/system_ext/app/EngineerMode/EngineerMode.apk=com.sprd.engineermode
package:/data/app/~~uXA3SWpD9_-JAW5ubyGZsQ==/com.transsion.plat.appupdate-h4C4ssJvWOwyjnw-82PqJA==/base.apk=com.transsion.plat.appupdate
package:/data/app/~~SlZtoZ5tvdYXYtBDruVSHw==/sinet.startup.inDriver-g9ObMdIZHUGrQLLKWESq8A==/base.apk=sinet.startup.inDriver
package:/product/overlay/IconShapePebble/IconShapePebbleOverlay.apk=com.android.theme.icon.pebble
package:/data/app/~~2VfjBG-peRPm5RmUpO7j-w==/com.google.android.googlequicksearchbox-LjGhU0izIUuaH1KW9sBR4Q==/base.apk=com.google.android.googlequicksearchbox
package:/apex/com.android.cellbroadcast/priv-app/GoogleCellBroadcastServiceModule@351310040/GoogleCellBroadcastServiceModule.apk=com.google.android.cellbroadcastservice
package:/data/app/~~0_Gdn_-BkSNS0f6zlv8HQw==/com.transsion.phonemaster-_g6NCXQUkH2fhAkBUezB3Q==/base.apk=com.transsion.phonemaster
package:/system_ext/priv-app/SprdCalendarProvider/SprdCalendarProvider.apk=com.android.providers.calendar
package:/data/app/~~FxsHuxNWe23YTgjBHdhogQ==/com.google.android.apps.googleassistant-1wOZE-ZurHmYfYjEKZlPTA==/base.apk=com.google.android.apps.googleassistant
package:/data/app/~~57WW6QWfp_2OKcjqte664A==/org.telegram.messenger-dQH2eKFkhLgoJJMJ3iyHqA==/base.apk=org.telegram.messenger
Ln 1, Col 1 36,594 characters 100% Windows (CRLF) UTF-8
Home
Gallery
Farrukh - Person
Farrukh - The Bh
Desktop
Downloads
Documents
Pictures
Music
Videos
STL
Screenshots
Forensics
Camera
This PC
itel Vision 3 Plu
Local Disk (C:)
Network
17 items
Details
5:16 PM
26-Apr-25

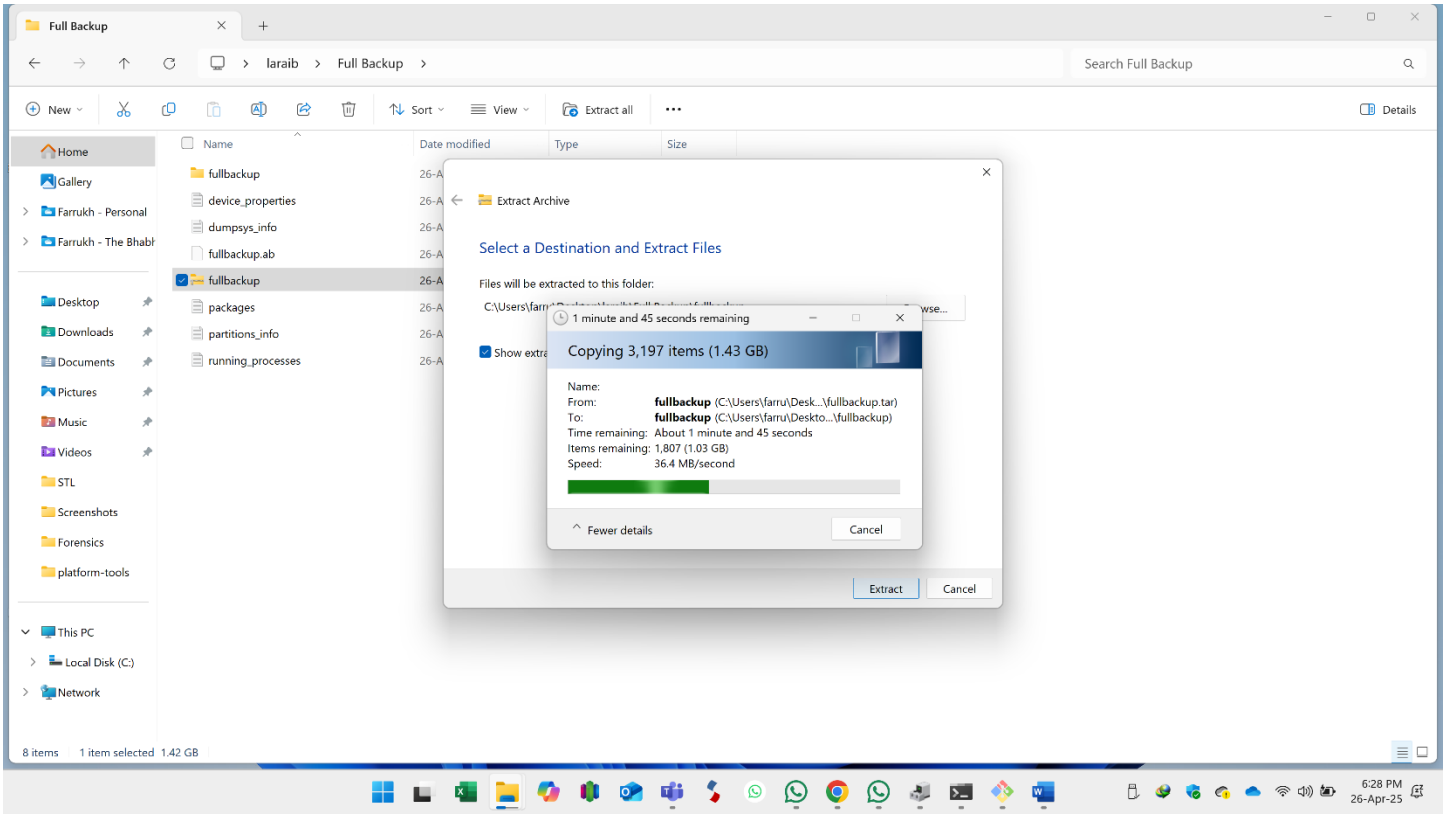

platform-tools
Downloads › Compressed › platform-tools-latest-windows › platform-tools
Search platform-tools
New
Details
Home
Gallery
Farrukh - Person
Farrukh - The Bh
Desktop
Downloads
Documents
Pictures
Music
Videos
STL
Screenshots
Forensics
Camera
This PC
itel Vision 3 Pl
Local Disk (C:)
Network
!!.txt
steg payloac
veil install.tx
Instructions!
db2015.mdb
IEEE Xplore f
Deivce.ini
Deivce.ini
File Recoven
packages.txt
devic
File
Edit
View
[af.media.systemready.state]: [true]
[build.version.extensions.r]: [15]
[cache_key.display_info]: [-7263470904356233722]
[cache_key.has_system_feature]: [-7263470904356233940]
[cache_key.is_compat_change_enabled]: [-7263470904356233894]
[cache_key.is_interactive]: [-7263470904356233752]
[cache_key.is_power_save_mode]: [-7263470904356233726]
[cache_key.is_user_unlocked]: [-7263470904356233905]
[cache_key.location_enabled]: [-7263470904356233930]
[cache_key.package_info]: [-7263470904356233893]
[cache_key.telephony.get_active_data_sub_id]: [1834919102165672340]
[cache_key.telephony.get_default_data_sub_id]: [1834919102165672336]
[cache_key.telephony.get_default_sms_sub_id]: [1834919102165672362]
[cache_key.telephony.get_default_sub_id]: [1834919102165672360]
[cache_key.telephony.get_slot_index]: [1834919102165672361]
[camera.disable_zsl_mode]: [1]
[dalvik.vm.appimageformat]: [lz4]
[dalvik.vm.dex2oat-Xms]: [64m]
[dalvik.vm.dex2oat-Xmx]: [512m]
[dalvik.vm.dex2oat-max-image-block-size]: [524288]
[dalvik.vm.dex2oat-minidebuginfo]: [true]
[dalvik.vm.dex2oat-resolve-startup-strings]: [true]
[dalvik.vm.dex2oat-updatable-bcp-packages-file]: [/system/etc/updatable-bcp-packages.txt]
[dalvik.vm.dexopt.secondary]: [true]
[dalvik.vm.heapgrowthlimit]: [192m]
[dalvik.vm.heapmaxfree]: [16m]
[dalvik.vm.heapminfree]: [8m]
[dalvik.vm.heapsize]: [512m]
Ln 1, Col 1
26,172 characters
100%
Windows (CRLF)
UTF-8
A long time ago
ncat
01-Jul-11 1:52 AM
Application
1,629 KB
19 items | 1 item selected 26.2 KB
5:17 PM
26-Apr-25

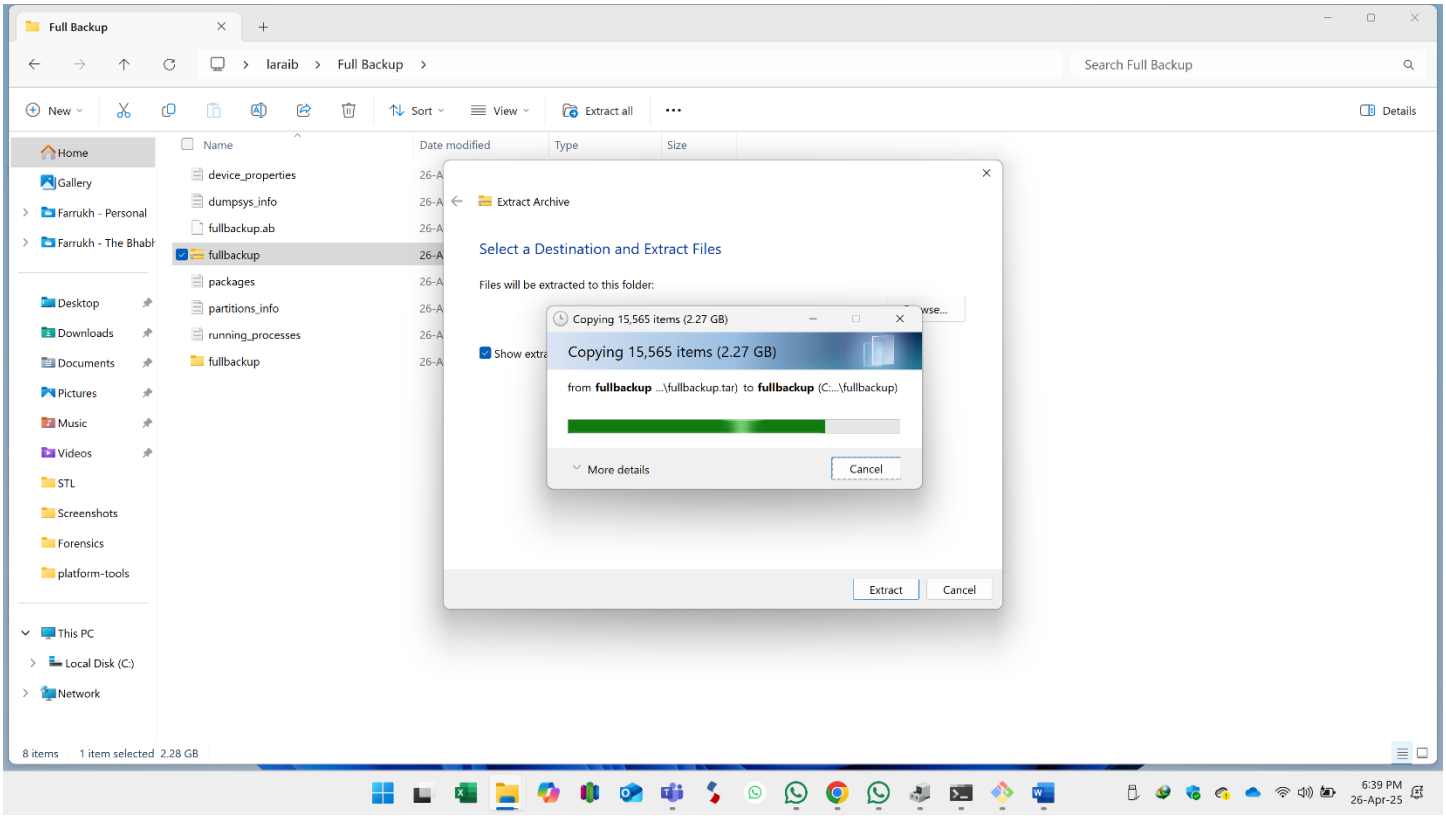

This PC - Shortcut
laraib
WhatsApp Business 2...
Nmap - Zenmap GUI
Recycle Bin
WhatsApp Business 2...
OneDrive - The Shab...
R-Drive Image
Autopsy 4.22.1
FassUS Data Recovery ...
data
MINGW64:/c/Users/farru/Desktop/laraib/Full Backup
farru@farrukhbhabha MINGW64 ~
$ ^[[200~cd "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: $'\E[200~cd': command not found
farru@farrukhbhabha MINGW64 ~
$ "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: /c/Users/farru/Desktop/laraib/Full Backup~: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ /c/Users/farru/Desktop/laraib/Full Backup
bash: /c/Users/farru/Desktop/laraib/Full: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ cd
farru@farrukhbhabha MINGW64 ~
$ cd "/c/Users/farru/Desktop/laraib/Full Backup"
farru@farrukhbhabha MINGW64 ~/Desktop/laraib/Full Backup
$ dd if=fullbackup.ab bs=24 skip=1 | openssl zlib -d > fullbackup.tar
6:05 PM
26-Apr-25


Full Backup
laraib
Full Backup
Search Full Backup
New
Sort
View
Extract all
Details
Home
Gallery
Farrukh - Personal
Farrukh - The Bhabh
Desktop
Downloads
Documents
Pictures
Music
Videos
STL
Screenshots
Forensics
platform-tools
This PC
Local Disk (C:)
Network
Name
Date modified
Type
Size
device_properties 26-Apr-25 5:16 PM Text Document 27 KB
dumpsys_info 26-Apr-25 5:17 PM Text Document 34,568 KB
fullbackup.ab 26-Apr-25 5:15 PM AB File 1,800,729 ...
fullbackup 26-Apr-25 6:05 PM Compressed Archi... 0 KB
packages 26-Apr-25 5:04 PM Text Document 37 KB
partitions_info 26-Apr-25 5:20 PM Text Document 3 KB
running_processes 26-Apr-25 5:20 PM Text Document 47 KB
7 items
1 item selected 0 bytes
MINGW64:/c/Users/farru/Desktop/laraib/Full Backup
farru@farrukhbhabha MINGW64 ~
$ ^[[200~cd "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: $'\E[200~cd': command not found
farru@farrukhbhabha MINGW64 ~
$ "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: /c/Users/farru/Desktop/laraib/Full Backup~: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ /c/Users/farru/Desktop/laraib/Full Backup
bash: /c/Users/farru/Desktop/laraib/Full: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ cd
farru@farrukhbhabha MINGW64 ~
$ cd "/c/Users/farru/Desktop/laraib/Full Backup"
farru@farrukhbhabha MINGW64 ~/Desktop/laraib/Full Backup
$ dd if=fullbackup.ab bs=24 skip=1 | openssl zlib -d > fullbackup.tar
6:06 PM
26-Apr-25


Full Backup
laraib › Full Backup ›
Search Full Backup
New
Sort
View
Details
Home
Gallery
Farrukh - Personal
Farrukh - The Bhabh
Desktop
Downloads
Documents
Pictures
Music
Videos
STL
Screenshots
Forensics
platform-tools
This PC
Local Disk (C:)
Network
Name
Date modified
Type
Size
device_properties 26-Apr-25 5:16 PM Text Document 27 KB
dumpsys_info 26-Apr-25 5:17 PM Text Document 34,568 KB
fullbackup.ab 26-Apr-25 5:15 PM AB File 1,800,729 ...
fullbackup 26-Apr-25 6:06 PM Compressed Archi... 135,368 KB
packages 26-Apr-25 5:04 PM Text Document 37 KB
partitions_info 26-Apr-25 5:20 PM Text Document 3 KB
running_processes 26-Apr-25 5:20 PM Text Document 47 KB
7 items
MINGW64:/c/Users/farru/Desktop/laraib/Full Backup
farru@farrukhbhabha MINGW64 ~
$ ^[[200~cd "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: $'\E[200~cd': command not found
farru@farrukhbhabha MINGW64 ~
$ "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: /c/Users/farru/Desktop/laraib/Full Backup~: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ /c/Users/farru/Desktop/laraib/Full Backup
bash: /c/Users/farru/Desktop/laraib/Full: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ cd
farru@farrukhbhabha MINGW64 ~
$ cd "/c/Users/farru/Desktop/laraib/Full Backup"
farru@farrukhbhabha MINGW64 ~/Desktop/laraib/Full Backup
$ dd if=fullbackup.ab bs=24 skip=1 | openssl zlib -d > fullbackup.tar
6:08 PM
26-Apr-25


Full Backup
laraib › Full Backup ›
Search Full Backup
New
Sort
View
Extract all
Details
Home
Gallery
Farrukh - Personal
Farrukh - The Bhabh
Desktop
Downloads
Documents
Pictures
Music
Videos
STL
Screenshots
Forensics
platform-tools
This PC
Local Disk (C:)
Network
Name
Date modified
Type
Size
device_properties 26-Apr-25 5:16 PM Text Document 27 KB
dumpsys_info 26-Apr-25 5:17 PM Text Document 34,568 KB
fullbackup.ab 26-Apr-25 5:15 PM AB File 1,800,729 ...
fullbackup 26-Apr-25 6:21 PM Compressed Archi... 272,808 KB
packages 26-Apr-25 5:04 PM Text Document 37 KB
partitions_info 26-Apr-25 5:20 PM Text Document 3 KB
running_processes 26-Apr-25 5:20 PM Text Document 47 KB
7 items
1 item selected 266 MB
MINGW64:/c/Users/farru/Desktop/laraib/Full Backup
farru@farrukhbhabha MINGW64 ~
$ ^[[200~cd "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: $'\E[200~cd': command not found
farru@farrukhbhabha MINGW64 ~
$ "/c/Users/farru/Desktop/laraib/Full Backup"~
bash: /c/Users/farru/Desktop/laraib/Full Backup~: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ /c/Users/farru/Desktop/laraib/Full Backup
bash: /c/Users/farru/Desktop/laraib/Full: No such file or directory
farru@farrukhbhabha MINGW64 ~
$ cd
farru@farrukhbhabha MINGW64 ~
$ cd "/c/Users/farru/Desktop/laraib/Full Backup"
farru@farrukhbhabha MINGW64 ~/Desktop/laraib/Full Backup
$ dd if=fullbackup.ab bs=24 skip=1 | openssl zlib -d > fullbackup.tar
76831069+1 records in
76831069+1 records out
1843945657 bytes (1.8 GB, 1.7 GiB) copied, 839.124 s, 2.2 MB/s
6:21 PM
26-Apr-25


Full Backup
laraib › Full Backup ›
Search Full Backup
New
Sort
View
Extract all
Details
Home
Gallery
Farrukh - Personal
Farrukh - The Bhabh
Desktop
Downloads
Documents
Pictures
Music
Videos
STL
Screenshots
Forensics
platform-tools
This PC
Local Disk (C:)
Network
Name
Date modified
Type
Size
fullbackup
device_properties
dumpsys_info
fullbackup.ab
fullbackup
packages
partitions_info
running_processes
Extract Archive
Select a Destination and Extract Files
Files will be extracted to this folder:
Show extra
1 minute and 45 seconds remaining
Copying 3,197 items (1.43 GB)
Name:
From: fullbackup (C:\Users\farru\Desk...\fullbackup.tar)
To: fullbackup (C:\Users\farru\Deskto...\fullbackup)
Time remaining: About 1 minute and 45 seconds
Items remaining: 1,807 (1.03 GB)
Speed: 36.4 MB/second
Fewer details
Cancel
Extract
Cancel
8 items
1 item selected 1.42 GB
6:28 PM
26-Apr-25


Full Backup
laraib › Full Backup ›
Search Full Backup
New
Sort
View
Extract all
Details
Home
Gallery
Farrukh - Personal
Farrukh - The Bhabh
Desktop
Downloads
Documents
Pictures
Music
Videos
STL
Screenshots
Forensics
platform-tools
This PC
Local Disk (C:)
Network
Name
Date modified
Type
Size
device_properties
dumpsys_info
fullbackup.ab
fullbackup
packages
partitions_info
running_processes
fullbackup
Extract Archive
Select a Destination and Extract Files
Files will be extracted to this folder:
Show extra
Copying 15,565 items (2.27 GB)
Copying 15,565 items (2.27 GB)
from fullbackup ...\fullbackup.tar) to fullbackup (C:...\fullbackup)
More details
Cancel
Extract
Cancel
8 items
1 item selected 2.28 GB
6:39 PM
26-Apr-25

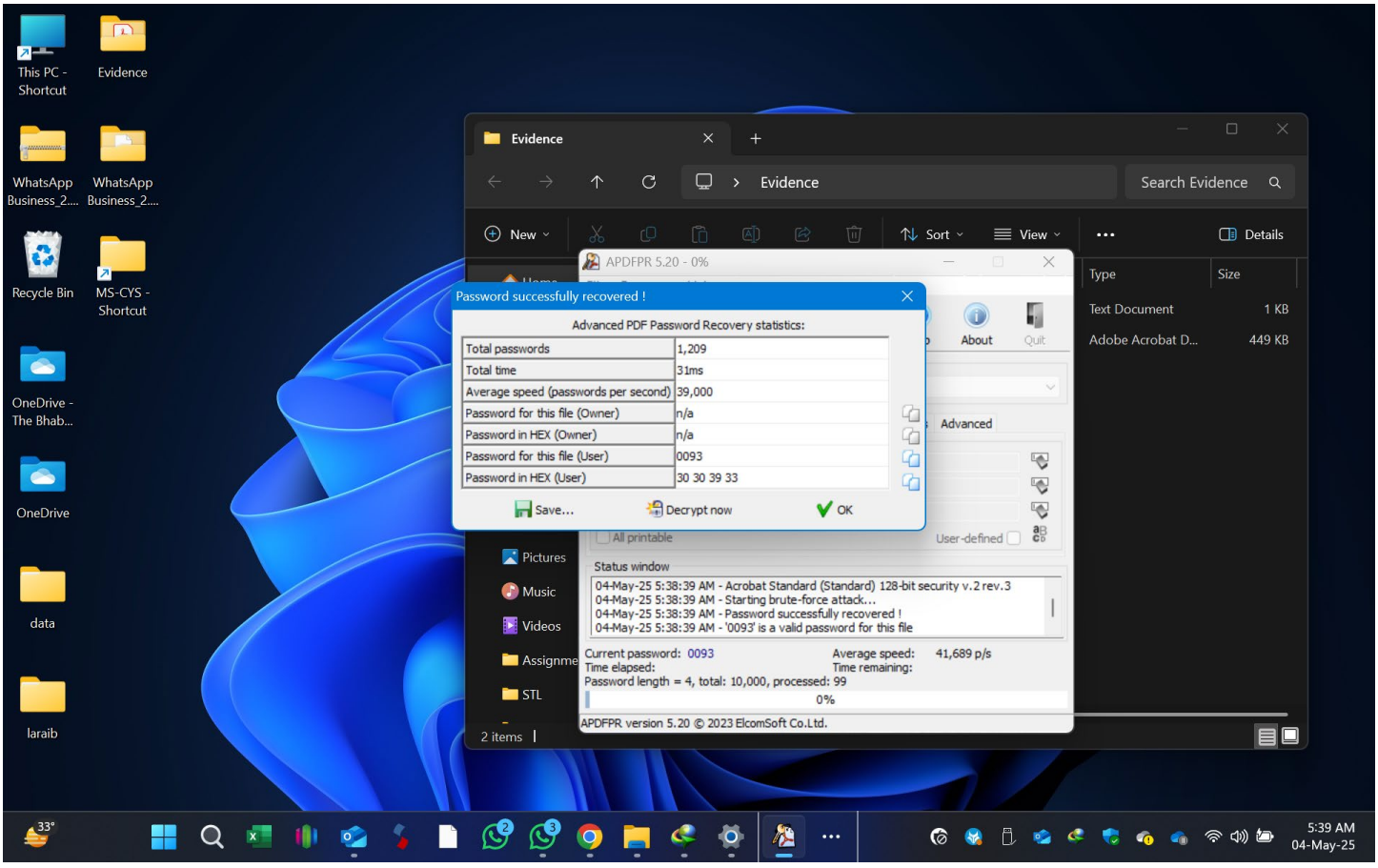
Step 5: Accessing and Analyzing Password-Protected Bank Statements

After obtaining complete access to the device, we discovered a bank statement stored on the phone. This document was password-protected, which initially prevented direct access to its contents. To proceed, we utilized specialized forensic tools designed to recover or bypass passwords on protected files.

By applying these tools, we successfully broke the password and unlocked the bank statement. Upon examination, the document revealed crucial information regarding the financial transactions conducted by the suspect. Specifically, we were able to identify:

- **Transaction Details:** Dates, times, and amounts of money transferred.
- **Frequency and Pattern:** How often and in what manner the transactions were carried out.
- **Recipient Information:** Where the funds were sent, including account numbers or recipient names if available.

This step was particularly significant for the investigation, as it provided direct evidence of the unauthorized transfers. By analyzing the bank statement, we could establish a clear connection between the suspect's actions and the financial discrepancies identified in the office accounts.



Step 6: Examination of Messages and Call Records

Following the analysis of the bank statement, we proceeded to examine the suspect's messages and phone call records. This step was critical for uncovering further evidence related to the financial misconduct.

By carefully reviewing the call logs, we identified the recipient of the most recent outgoing call. This information provided valuable leads regarding individuals who may have been in contact with the suspect around the time of the alleged transactions.

Additionally, the analysis of SMS and messaging app records revealed detailed transaction information. Through these messages, we were able to determine:

- **Transaction Details:** The frequency, amount, and timing of transactions conducted from various bank accounts.
- **Bank Account Usage:** The number of different bank accounts the suspect was operating, as indicated by transaction alerts and confirmations received via SMS or messaging applications.

These findings were instrumental in mapping out the suspect's financial activities and establishing a timeline of events. By correlating the information from messages and call records with the data obtained from the bank statement, we gained a comprehensive understanding of how the theft was executed and the extent of the suspect's involvement.

Step 7: Tracing the Theft, Identifying Loopholes, and Ensuring Data Confidentiality

Through the comprehensive analysis of all the extracted data—including bank statements, messages, call records, and other digital evidence—we were able to reconstruct the entire sequence of events related to the theft. This digital trail provided clear insights into how the crime was committed and revealed the specific security loopholes within the company's systems that were exploited by the suspect.

Based on these findings, we took the following actions:

- **Identification and Closure of Security Loopholes:** We documented the vulnerabilities that allowed the unauthorized transactions to occur and implemented appropriate security measures to prevent similar incidents in the future.
- **Documentation and Chain of Custody:** Every step of the investigation was thoroughly documented, ensuring a clear chain of custody for all evidence collected. This is essential for maintaining the integrity and admissibility of the evidence in any legal proceedings.
- **Data Confidentiality and Ethical Handling:** Throughout the forensic process, we handled all sensitive information with the utmost care. We only accessed and analyzed data that was necessary for the investigation, keeping all other information confidential to protect the individual's privacy and prevent identity theft or data misuse.

- **Responsible Reporting:** Any confidential findings were securely stored and only shared with authorized personnel. Our approach ensured that the investigation remained focused, ethical, and compliant with legal and organizational standards.

In summary, this step not only helped us understand the mechanics of the theft and address the underlying security flaws but also demonstrated our commitment to ethical forensic practices and the responsible handling of sensitive data.