Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

School of Computer Engineering and Technology
Academic Year: 2023-2024 Sem V
Digital Forensics and Investigation

Lab Assignment : 01

TOOLS FOR DIGITAL FORENSICS AND INVESTIGATION FOR MOBILE DEVICES.

Prepared By
Saurabh Jitendra Jadhav
Roll No:-PA12
Batch A1

August 16,2023

1. Aim:

To study and understand the tools used for Digital Forensics and Investigation for Mobile Devices

2. Objective:

1.To understand the tools used for Digital Forensics and Investigation for Mobile Devices.
2.Find out the tools used for Mobile Forensics.
3. Study some of the tools used for Mobile Forensics.

3. Theory:

a) **Criminal Investigation:** Mobile devices are used for storing personal and business information, and they are also used for communication. Mobile devices are used for storing personal and business information, and they are also used for communication.

b) **Evidence Collection:** Mobile devices are frequently used to plan, coordinate, and execute criminal activities. Digital evidence retrieved from mobile devices can be used in court to establish timeline, connections, and intentions of suspects.

c) **CyberCrime Investigation:** Mobile devices can be involved in cybercrimes such as hacking, phishing, and spreading malware. Analyzing mobile devices can provide insights into the methods and targets of cybercriminals.

d) **Fraud and Financial Crimes:** Mobile devices are often used to access online banking, e-commerce, and financial applications. Mobile forensics can help trace financial transactions, uncover fraudulent activities, and identify individuals involved in financial crimes.

e) **Missing Persons Cases:** Mobile devices can provide information about a missing person’s last known location, contacts, and communications, aiding law enforcement in search and rescue efforts.

f) **Counter terrorism Efforts:** Mobile devices can provide insights into the communications and activities of individuals involved in terrorism, helping law enforcement agencies to prevent and respond to potential threats

g) **National Security:** Mobile forensics plays a crucial role in national security efforts, helping to gather intelligence and counter espionage activities.

4. Evidence Extraction Process:

Preparation and Documentation:

• Clearly define the purpose of the investigation and the specific types of evidence required.
• Obtain legal authorization, such as a search warrant or consent, to access and extract data from the mobile phone.
• Document the phone's physical condition, including any damage or alterations.
• Record the phone's make, model, serial number, IMEI (International Mobile Equipment Identity), and other identifying details.
• Note the phone's battery status, connectivity status, and any security measures (passcode, biometric authentication) in place.

Device Handling and Isolation:

• Handle the phone carefully to prevent accidental data alteration or contamination.
• Place the phone in airplane mode or power it off to prevent remote wiping or data transmission.
• If the phone is locked, document the type of lock (passcode, pattern, biometric) and make a note of any available recovery options.

Device Handling and Isolation:

• Handle the phone carefully to prevent accidental data alteration or contamination.
• Place the phone in airplane mode or power it off to prevent remote wiping or data transmission.
• If the phone is locked, document the type of lock (passcode, pattern, biometric) and make a note of any available recovery options.

Image Acquisition:

• Create a forensic image (bit-for-bit copy) of the phone's storage to preserve the original data.

• Use specialized forensic tools to create an image, ensuring data integrity and preventing modifications.

Data Extraction Methods:

• Choose the appropriate extraction method based on the phone’s operating system (iOS, Android) and the device’s state (locked vs unlocked).
• Logical Extraction: Retrieve data through available APIs without altering the original data.
• Physical Extraction: Extract raw data from the phone’s memory, including deleted and hidden data.
• File System Extraction: Extract specific files and folders from the device’s file system.

Data Analysis:

• Analyze the extracted data to identify relevant evidence.
• Review call logs, text messages, multimedia files, emails, app data, browsing history, and other pertinent information.
• Use forensic software to parse and decode data, and reconstruct conversations or activities.

Metadata Examination:

• Examine metadata to determine the phone’s location, movements, and activities.
• Review metadata from photos, videos, and audio files to determine when and where they were created.
• Analyze metadata from apps, such as social media, to determine when and where they were accessed.

Password Decryption and Cracking:

• Decrypt encrypted data or crack passwords to access locked content or encrypted apps.
• Employ password cracking techniques if necessary, adhering to ethical and legal guidelines.

Artifact Recovery:

• Recover deleted data and hidden data from the phone’s memory.

Report Generation:

• Document the entire extraction process, including the tools and techniques used.

• Create a detailed report of the findings, including relevant evidence and metadata. • Include screenshots, photos, and other visual aids to support the findings.

• Provide a summary of the findings and conclusions.

5 Tools Used For Mobile Forensics:

1 Cellebrite UFED:

A widely used mobile forensic tool that supports a range of devices and operating systems. It can perform physical and logical extractions, decode data, and analyze various apps and communication platforms.

2 Oxygen Forensic Detective:

his tool supports multiple device platforms and offers advanced capabilities for data extraction, analysis, and reporting. It can recover deleted data and analyze cloud services.

3 MSAB XRY:

Known for its support of a wide range of mobile devices and operating systems, XRY can perform physical, logical, and file system extractions, as well as decode encrypted data.

4 Magnet AXIOM:

A comprehensive digital forensics platform that includes mobile device analysis. It supports multiple devices, apps, and extraction methods, and offers advanced data visualization and reporting.

5 Paraben E3:

A mobile forensics tool that supports multiple devices and operating systems. It can perform physical and logical extractions, recover deleted data, and analyze cloud services.

6 Andriller:

Focused on Android devices, Andriller can extract a wide range of data and artifacts, including call logs, messages, and app data.

7 BlackBag Mobilyze:

A mobile forensics tool that supports iOS and Android devices. It can perform logical extractions, recover deleted data, and analyze cloud services.

8 Cellebrite Physical Analyzer:
Used in conjunction with Cellebrite UFED, this tool assists in in-depth analysis of extracted data, providing ad- vanced data parsing and visualization.

9 GrayKey:
A device used for unlocking and extracting data from iOS devices. It’s often used by law enforcement agencies for bypassing passcodes on locked iPhones.

PLATFORM USED: ANDRILLER TOOL

Steps to install Andriller tool:

- Create a virtual environment using Python 3:

```
python3 -m venv andriller
```

- Activate the virtual environment (Windows):

```
.\andriller\Scripts\activate
```

- Install Andriller with its Python dependencies (same command to upgrade it):

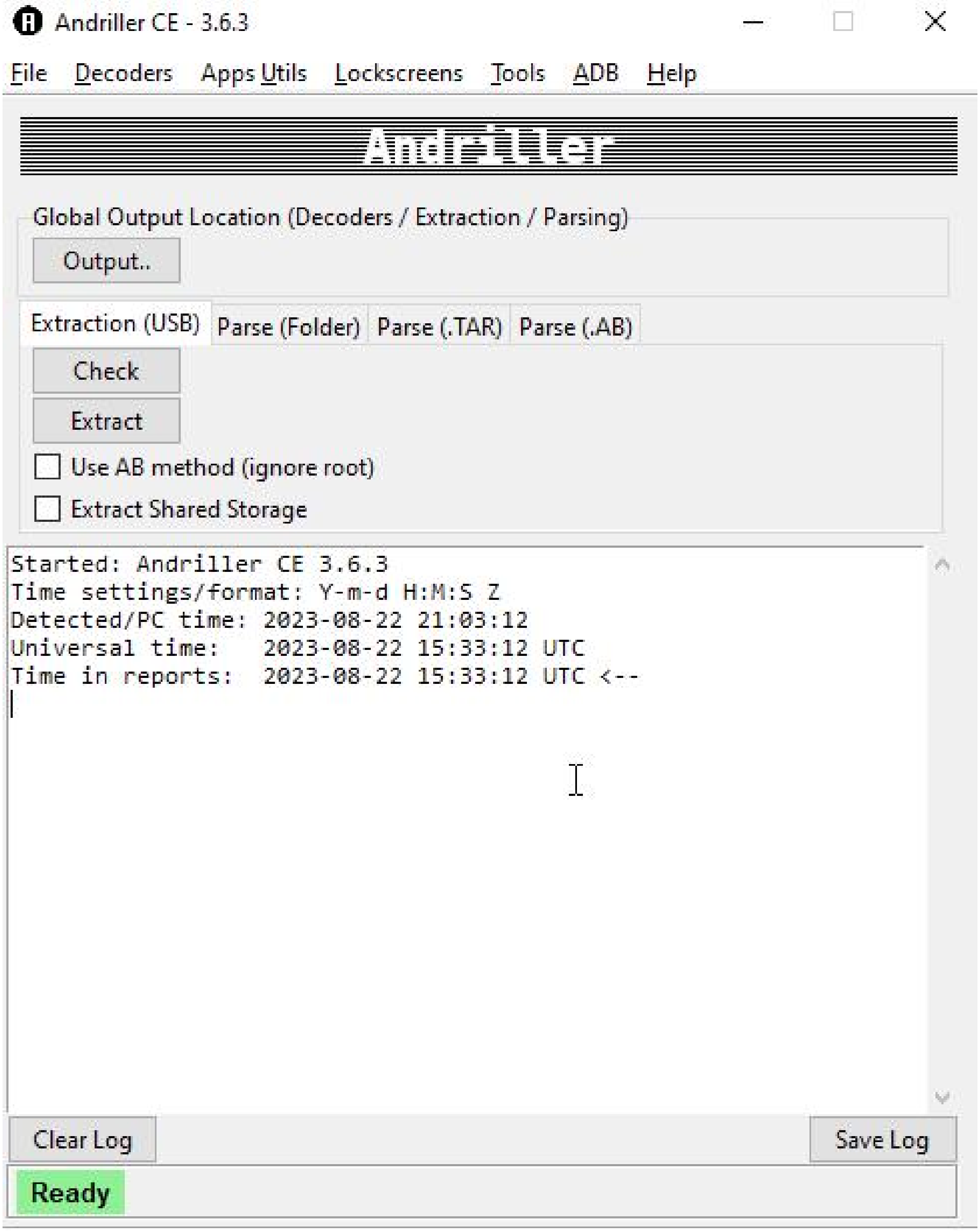
```
pip install andriller -U
```

To Quick Start Andriller(run GUI):

```
python -m andriller
```

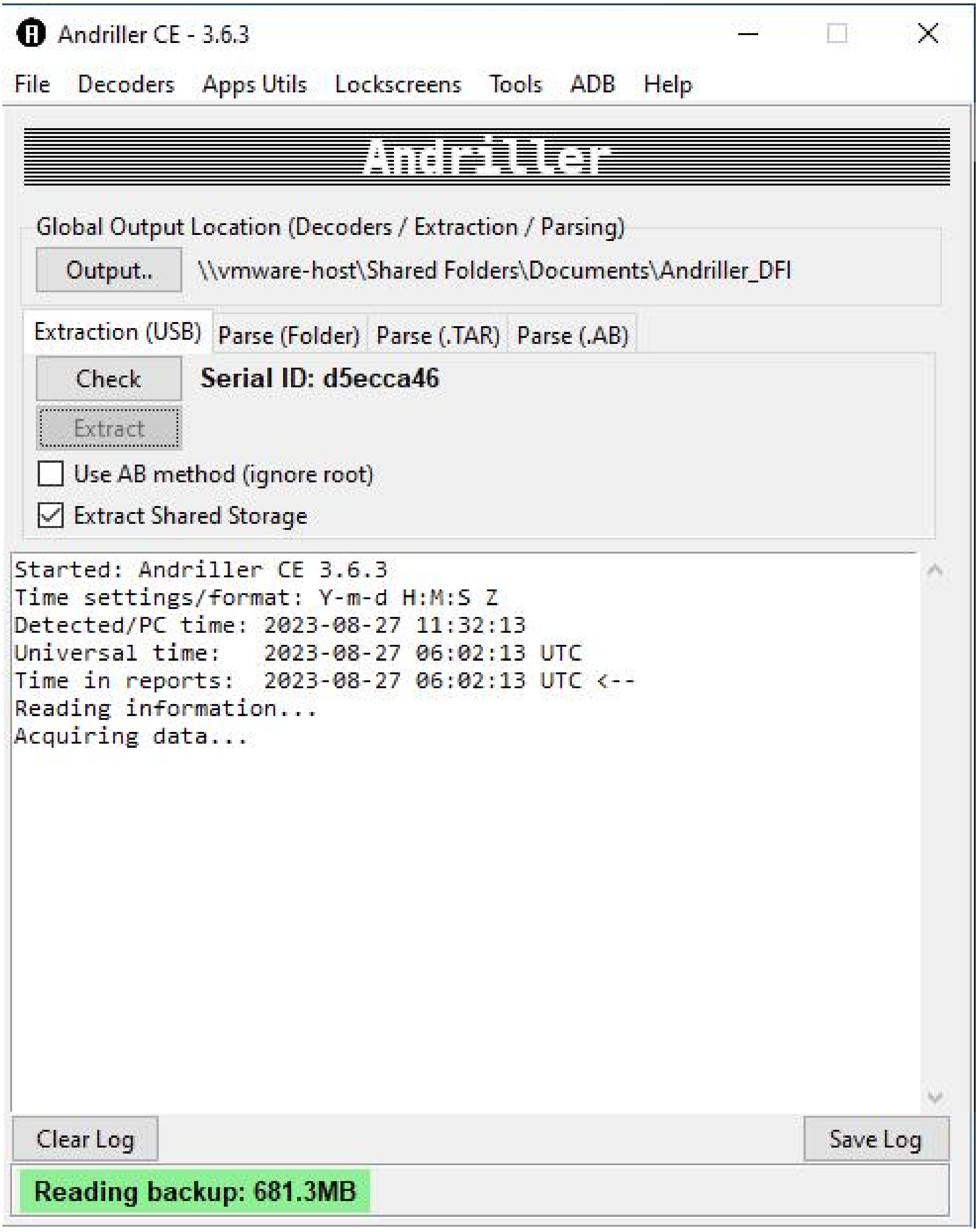
After Executing this Command Andriller GUI will start

Graphical Interface of Andriller:


Andriller CE - 3.6.3
File Decoders Apps Utils Lockscreens Tools ADB Help
Andriller
Global Output Location (Decoders / Extraction / Parsing)
Output..
Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB)
Check
Extract
□ Use AB method (ignore root)
□ Extract Shared Storage
Clear Log
Save Log
Ready

```
Started: Andriller CE 3.6.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2023-08-22 21:03:12
Universal time:   2023-08-22 15:33:12 UTC
Time in reports:  2023-08-22 15:33:12 UTC <--
```

Scanning Device:



\\vmware-host\Shared Folders\Documents\Andriller_DFI

Serial ID: d5ecca46

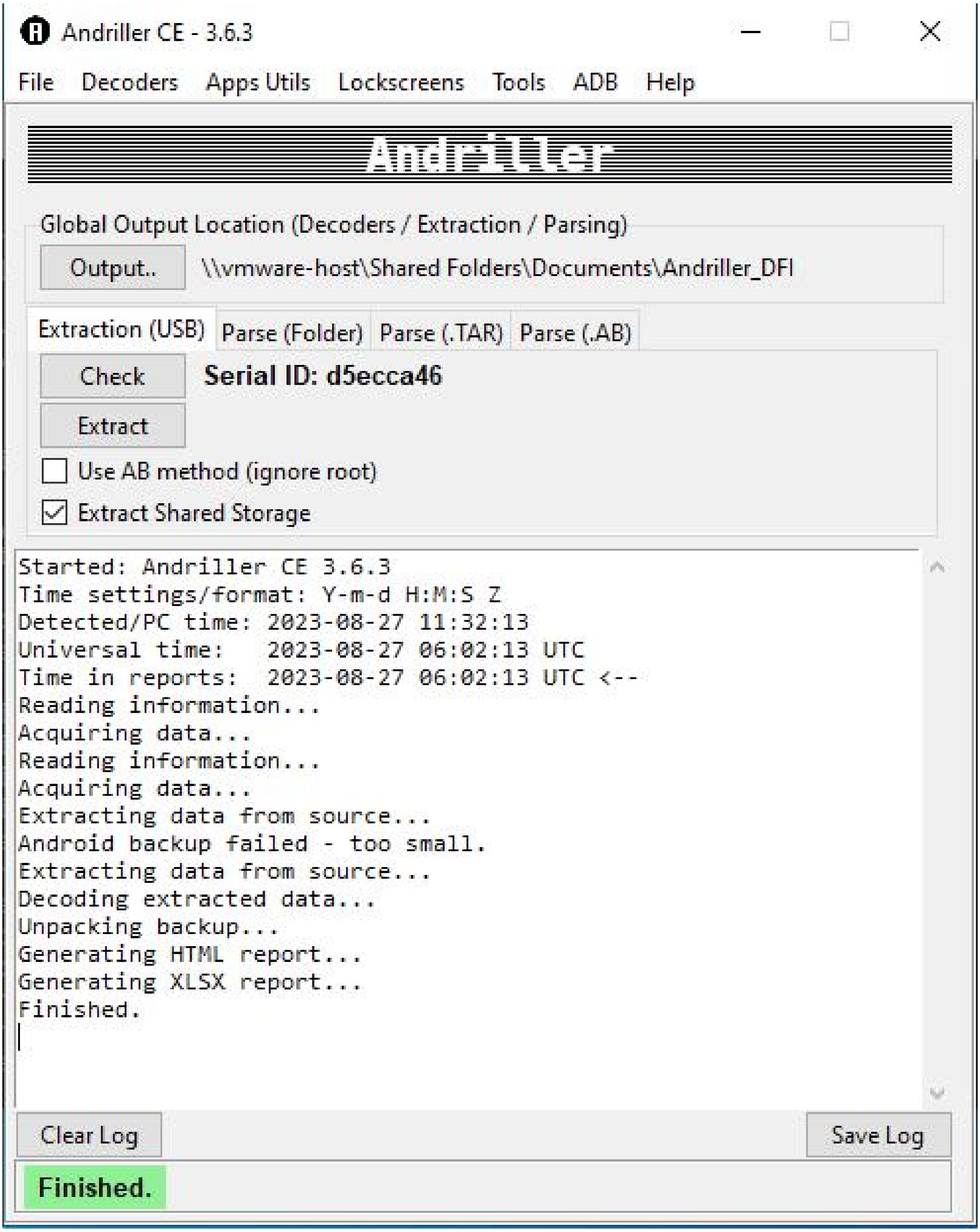
☐ Use AB method (ignore root)

☑ Extract Shared Storage

```
Started: Andriller CE 3.6.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2023-08-27 11:32:13
Universal time:   2023-08-27 06:02:13 UTC
Time in reports:  2023-08-27 06:02:13 UTC <--
Reading information...
Acquiring data...
```

Reading backup: 681.3MB

Data acquisition Complete :



Andriller CE - 3.6.3
File Decoders Apps Utils Lockscreens Tools ADB Help
Andriller
Global Output Location (Decoders / Extraction / Parsing)
Output..
Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB)
Check
Extract
Clear Log
Save Log

\\vmware-host\Shared Folders\Documents\Andriller_DFI

Serial ID: d5ecca46

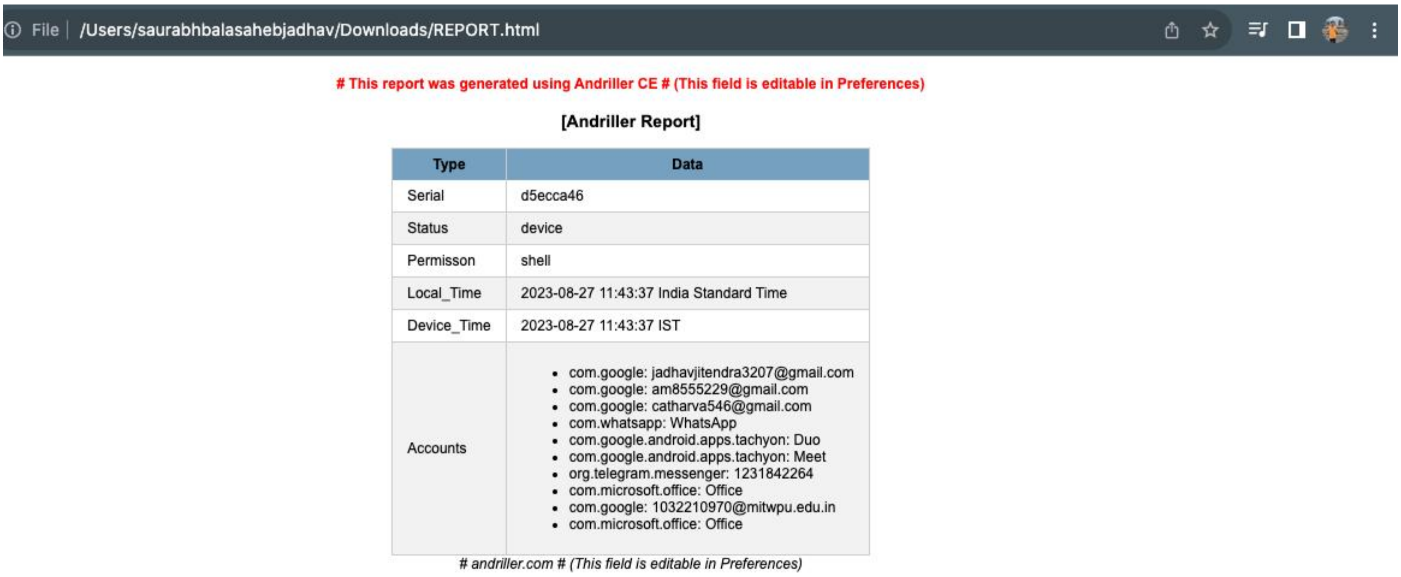
□ Use AB method (ignore root)

☑ Extract Shared Storage

```
Started: Andriller CE 3.6.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2023-08-27 11:32:13
Universal time:   2023-08-27 06:02:13 UTC
Time in reports:  2023-08-27 06:02:13 UTC <--
Reading information...
Acquiring data...
Reading information...
Acquiring data...
Extracting data from source...
Android backup failed - too small.
Extracting data from source...
Decoding extracted data...
Unpacking backup...
Generating HTML report...
Generating XLSX report...
Finished.
```

Finished.

FINAL REPORT:



File | /Users/saurabhbalasahebjadhav/Downloads/REPORT.html

This report was generated using Andriller CE # (This field is editable in Preferences)

[Andriller Report]

Type	Data
Serial	d5ecca46
Status	device
Permisson	shell
Local_Time	2023-08-27 11:43:37 India Standard Time
Device_Time	2023-08-27 11:43:37 IST
Accounts	• com.google: jadhavjitendra3207@gmail.com • com.google: am8555229@gmail.com • com.google: catharva546@gmail.com • com.whatsapp: WhatsApp • com.google.android.apps.tachyon: Duo • com.google.android.apps.tachyon: Meet • org.telegram.messenger: 1231842264 • com.microsoft.office: Office • com.google: 1032210970@mitwpu.edu.in • com.microsoft.office: Office

# andriller.com # (This field is editable in Preferences)

Conclusion:

Thus, we have studied and understood the tools used for Digital Forensics and Investigation for Mobile Devices. We have also found out the tools used for Mobile Forensics and studied some of the tools used for Mobile Forensics.