

ASSIGNMENT NO: 01

/*

Name:

Kshitish Deshpande

Roll No.:

PF22

Subject:

DFCL

*/

Problem Statement:

Perform installation and employ any Android Mobile Forensics Open Source Tools for real time investigation of mobile forensics.

Objectives:

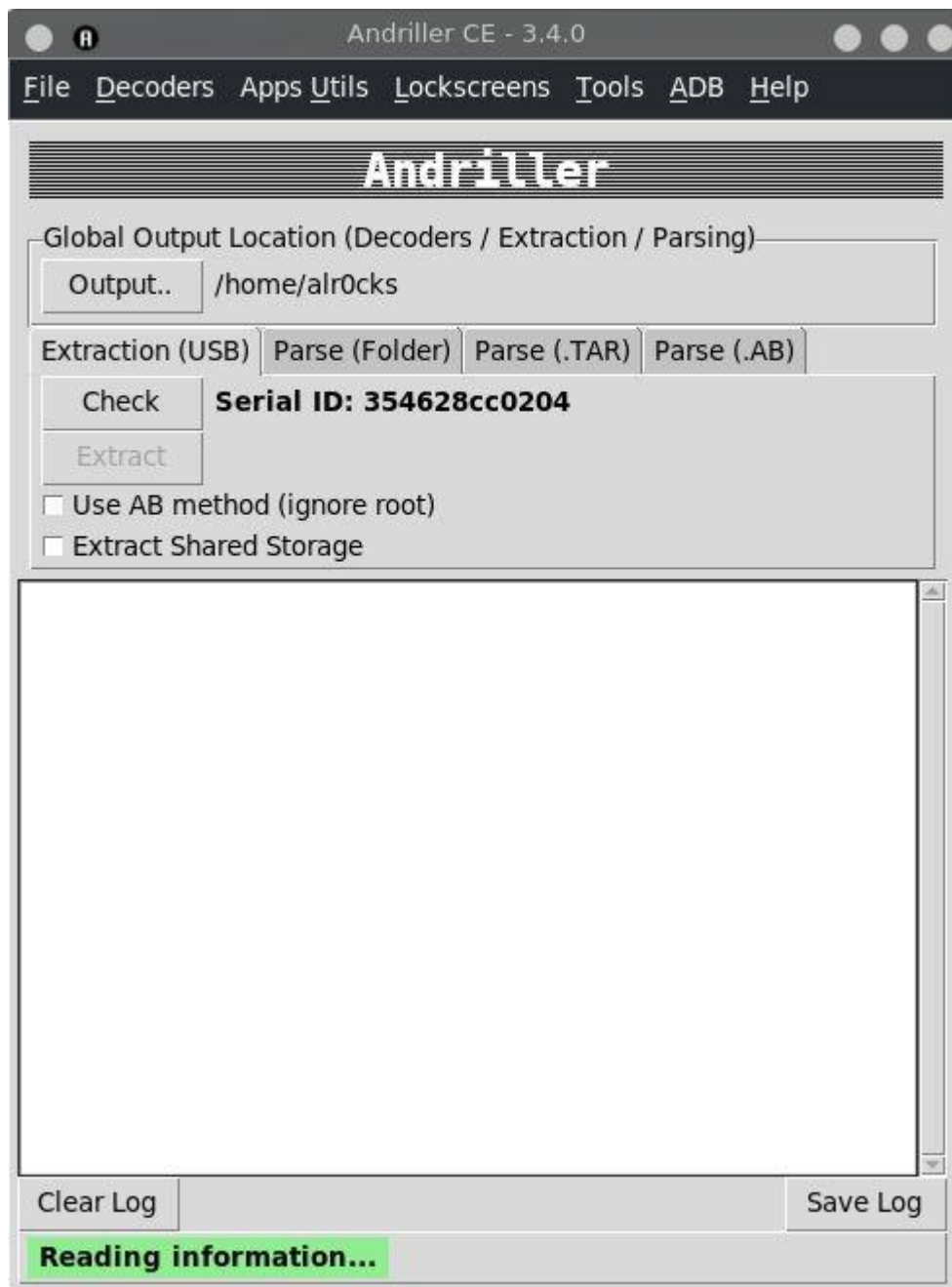
Explore the Andriller tool.

Theory:

Andriller - is software utility with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices.

Features of Andriller:

1. Database Decoders
 2. Data Extraction from Androids
 3. Data Parsing
 4. Reporting
-



Implementation:

- 1) Install Andriller using following commands:
 - a) `sudo apt-get install android-tools-adb python3-tk`
 - b) `pip install andriller -U`
- 2) Launch the app using:
 - a) `Python -m andriller`
- 3) Connect the mobile device and make sure usb debugging is on.
- 4) Extract data and take full back up from mobile
- 5) Generate a report:

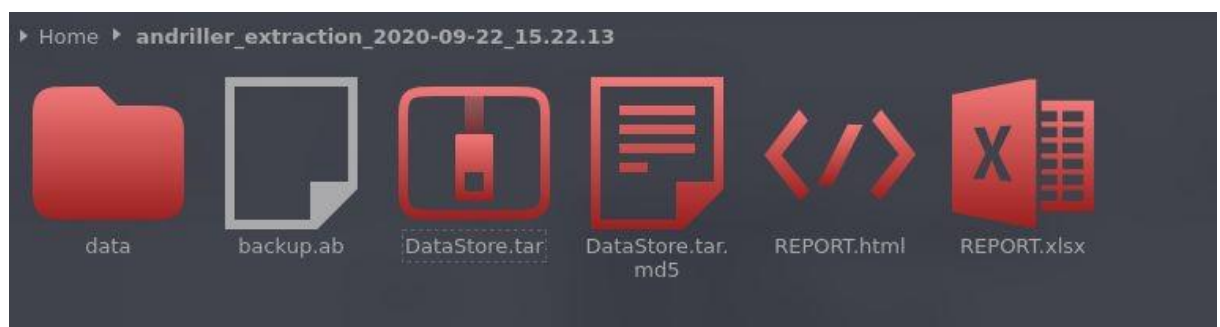
This report was generated using Andriller CE # (This field is editable in Preferences)

[Andriller Report]

Type	Data
Serial	354628cc0204
Status	device
Permisson	shell
Wifi Mac	02:00:00:00:00:00
Local_Time	2020-09-22 15:22:13 IST
Device_Time	2020-09-22 15:22:47 IST
Accounts	<ul style="list-style-type: none">• com.google: alok.bhawankar@gmail.com• com.google: alokbhawankar@thescriptgroup.in• com.google: alrocks29@gmail.com• com.google: boneslaw99@gmail.com• com.google: support@thescriptgroup.in• com.google.android.gm.legacyimap: alokbhawankar@outlook.com• com.google.android.gm.legacyimap: boneslaw99@outlook.com• com.whatsapp: WhatsApp• com.truecaller.account: Truecaller• org.thunderdog.challegram.sync.account: Telegram• com.facebook.auth.login: Facebook• com.cisco.webex.meetings.ACCOUNT: Webex Meet• com.github.android: alrocks29• com.microsoft.workaccount: 1032170126@mitwpu.ac.in• com.mgoogle: alok.bhawankar@gmail.com• com.adobe.creativesdk.foundation.auth.adobeID.DC: alrocks29@gmail.com• com.skype.raider: Skype• com.microsoft.android.enterprise15: Skype For Business

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

You can go through all the metadata now



Platform: 64 bit Linux OS

Conclusion: Hence learned how to use andriller app.