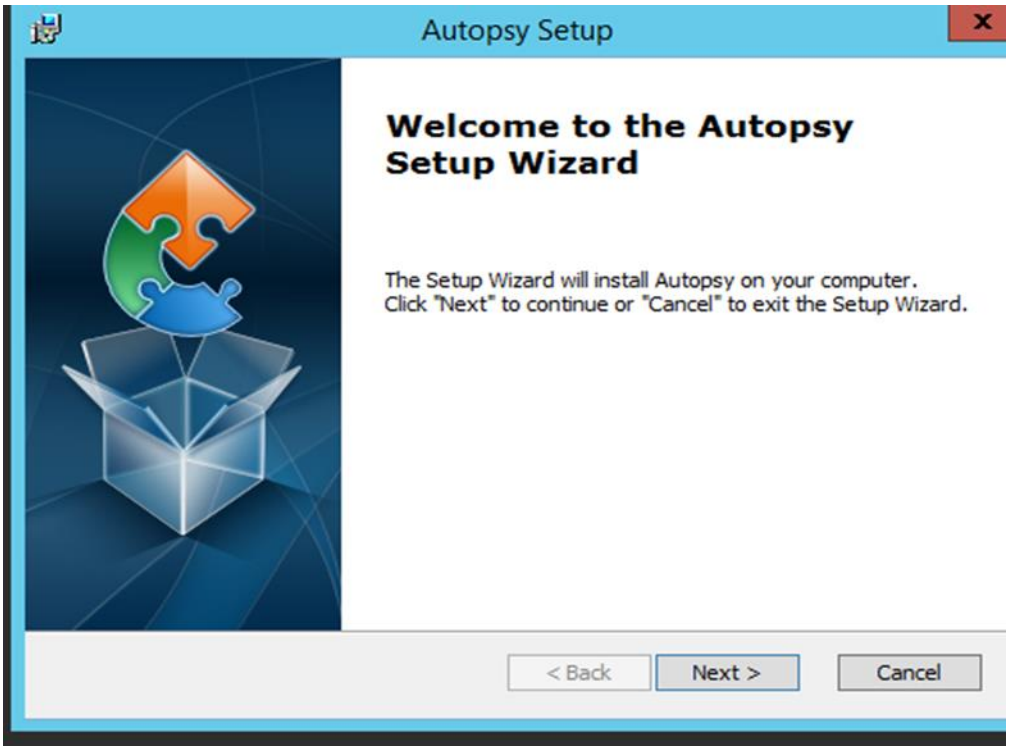
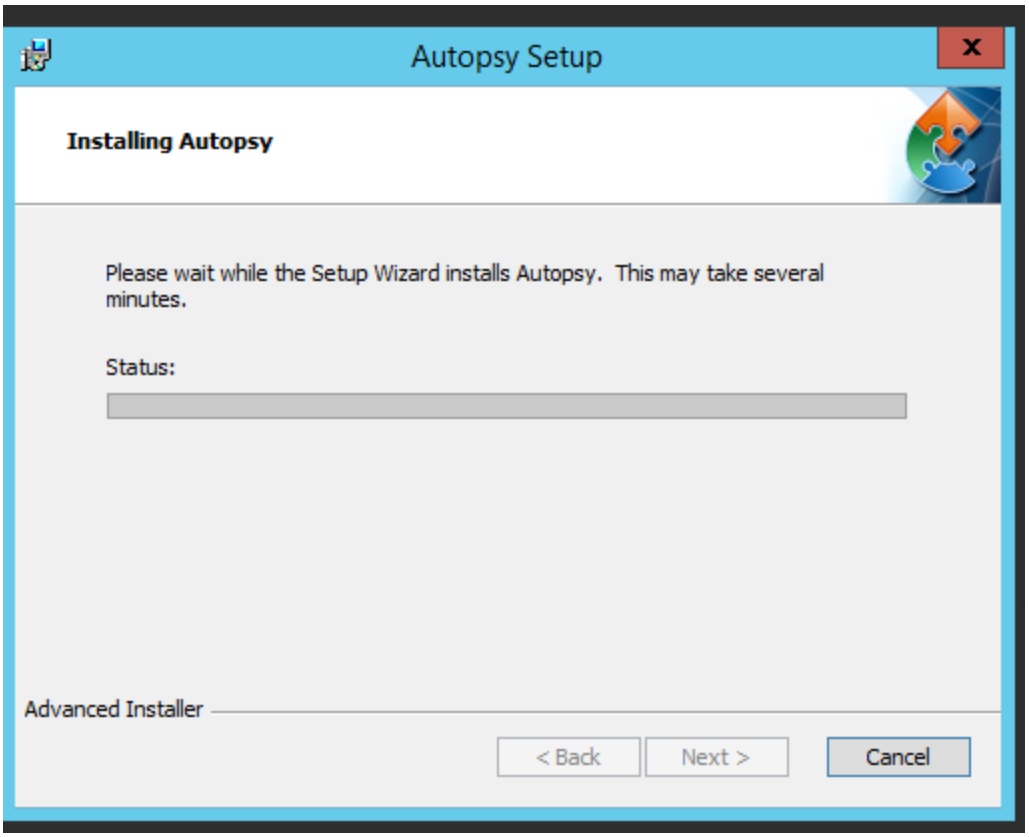
MOBILE FORENSICS LAB WORK

LAB 1: ANALYZING FORENSIC IMAGE AND CARVING DELETED FILES USING AUTOPSY

- Double click the autopsy exe file on the desktop to begin the installation process the dialog box below appears. Click next.

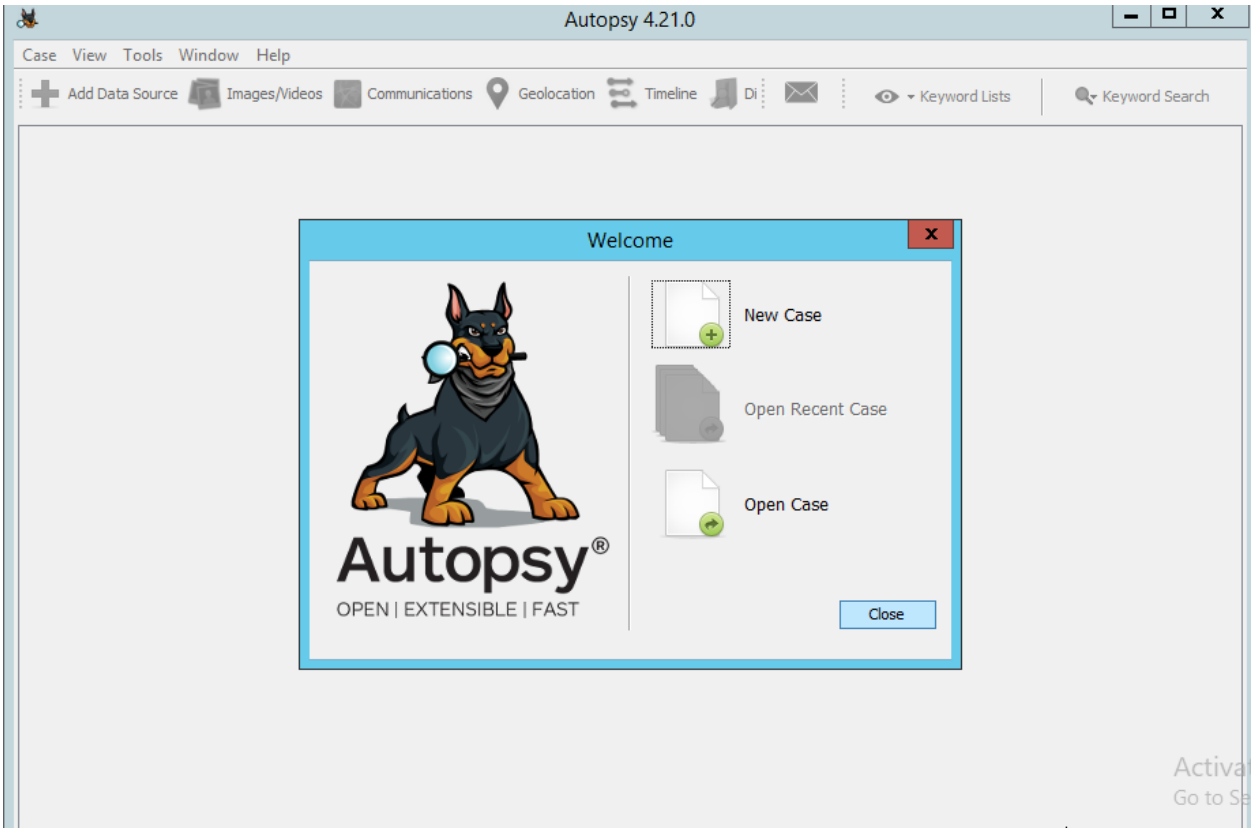


- The installation begins as shown below.

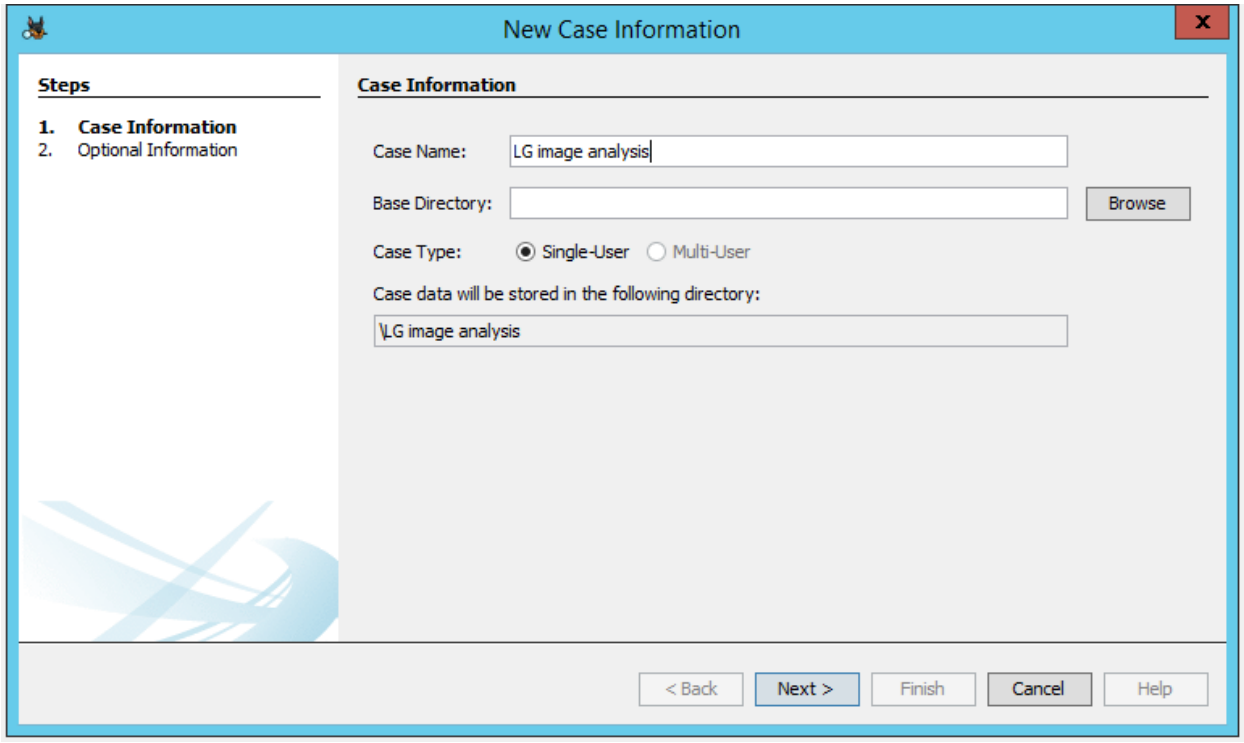


- Double click the autopsy icon on the desktop to launch autopsy.

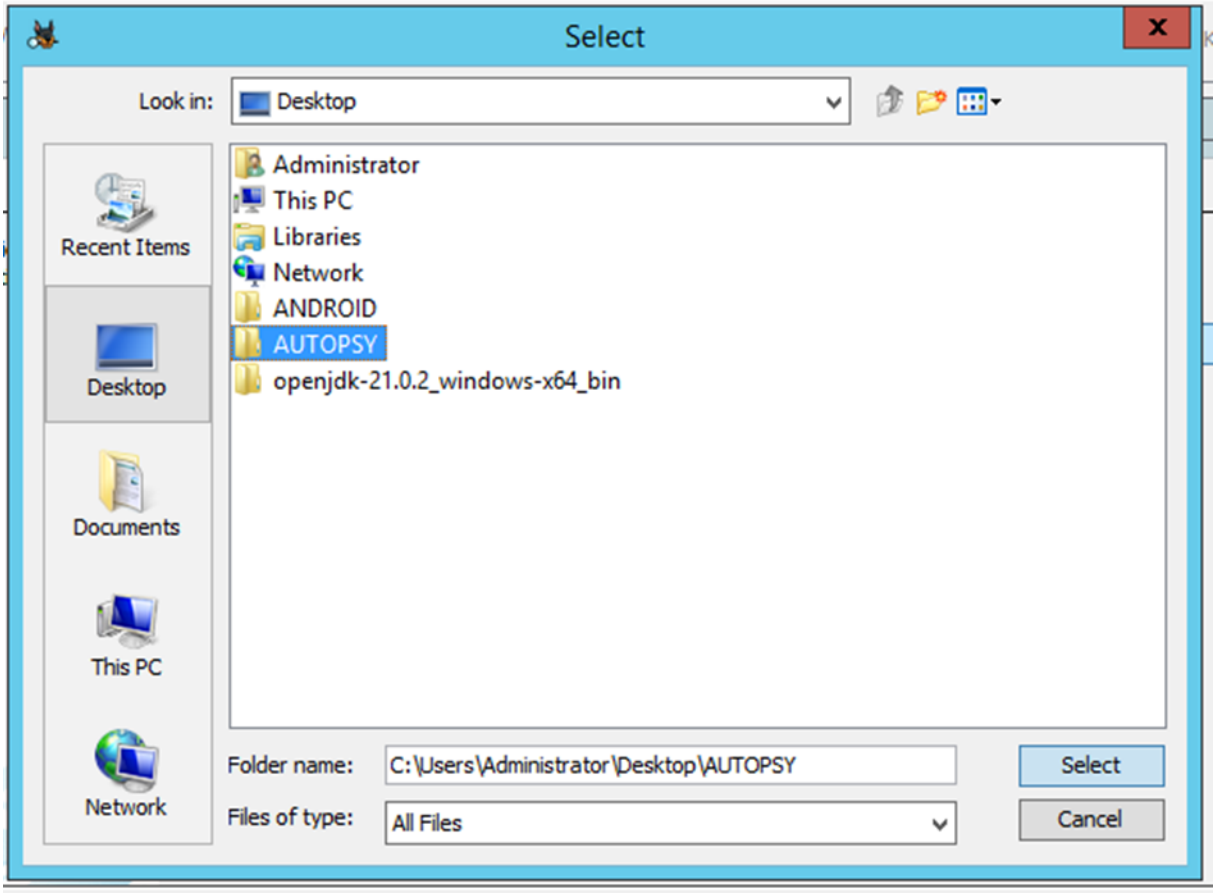
- Once the autopsy is launched as shown in the screenshot below, click on “new case”.



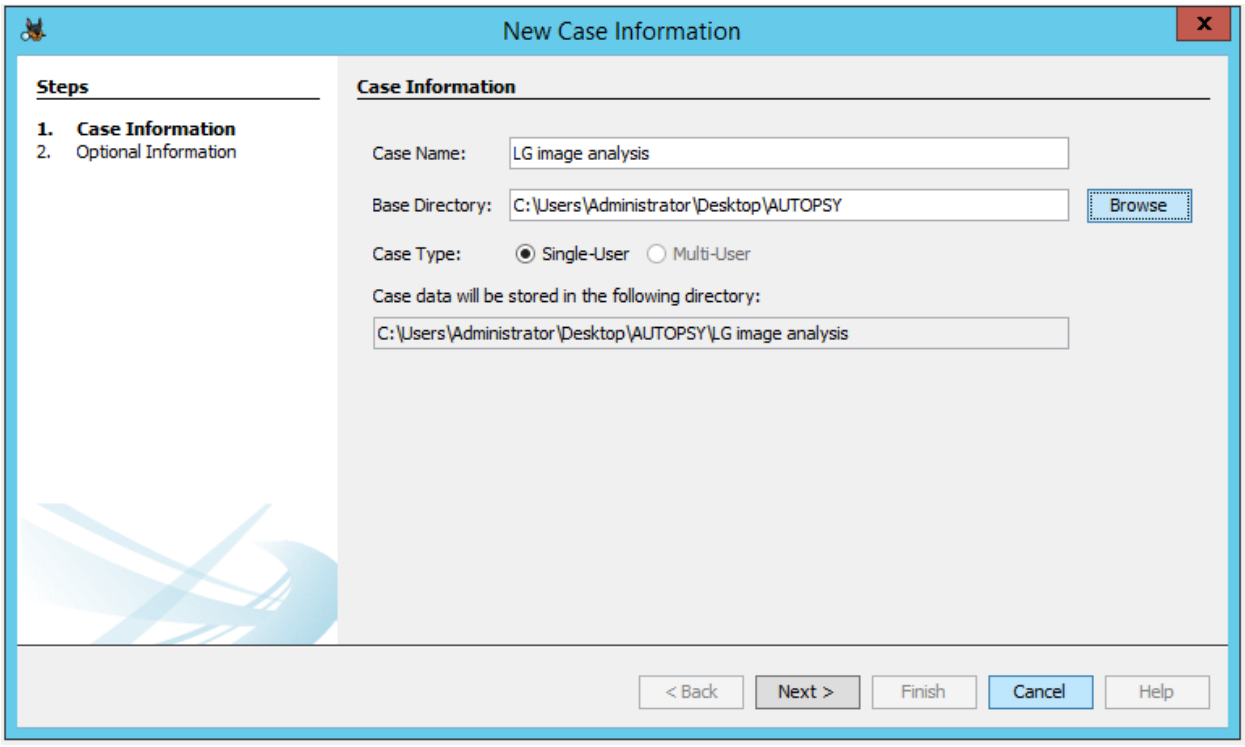
- The new case information window appears. under the Case Name enter a name.



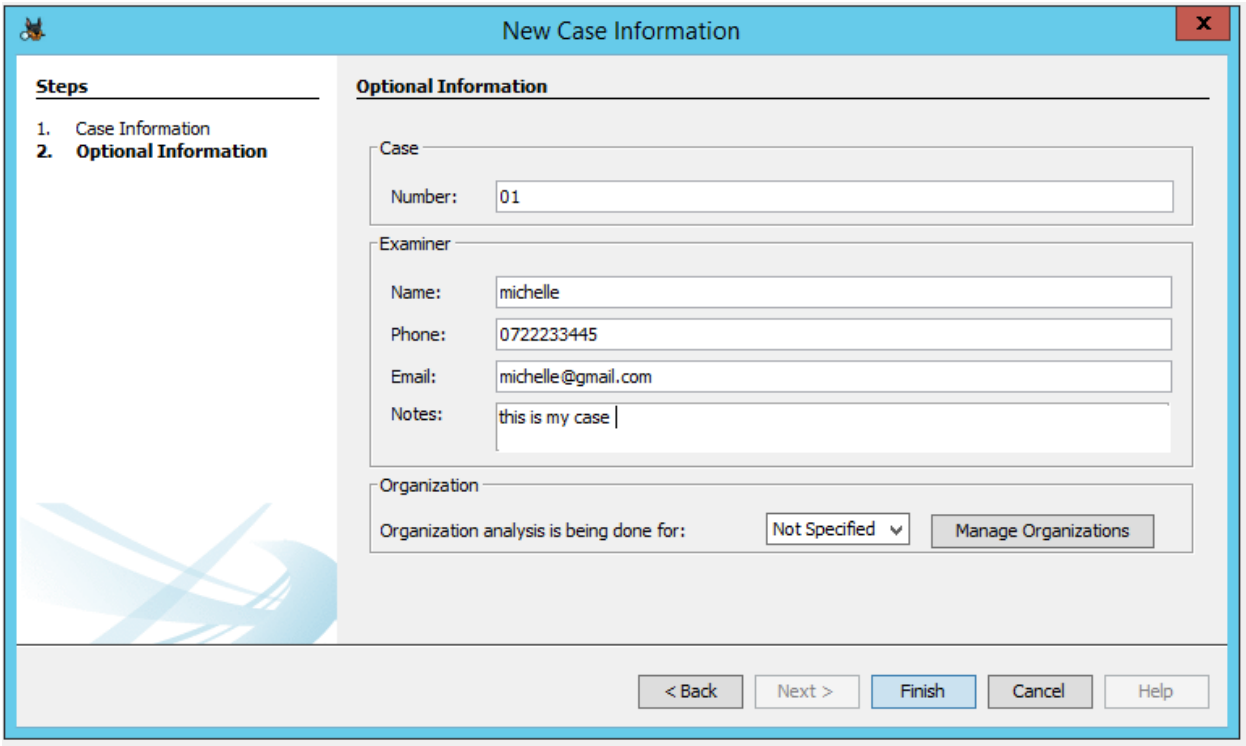
- Click browse button and navigate to desktop and select autopsy folder as shown below then click select.

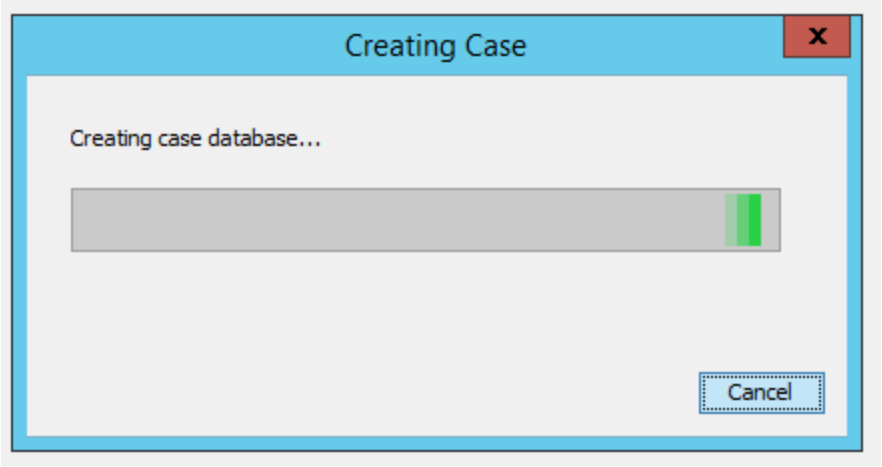


- After updating the base directory as shown below click “Next”.

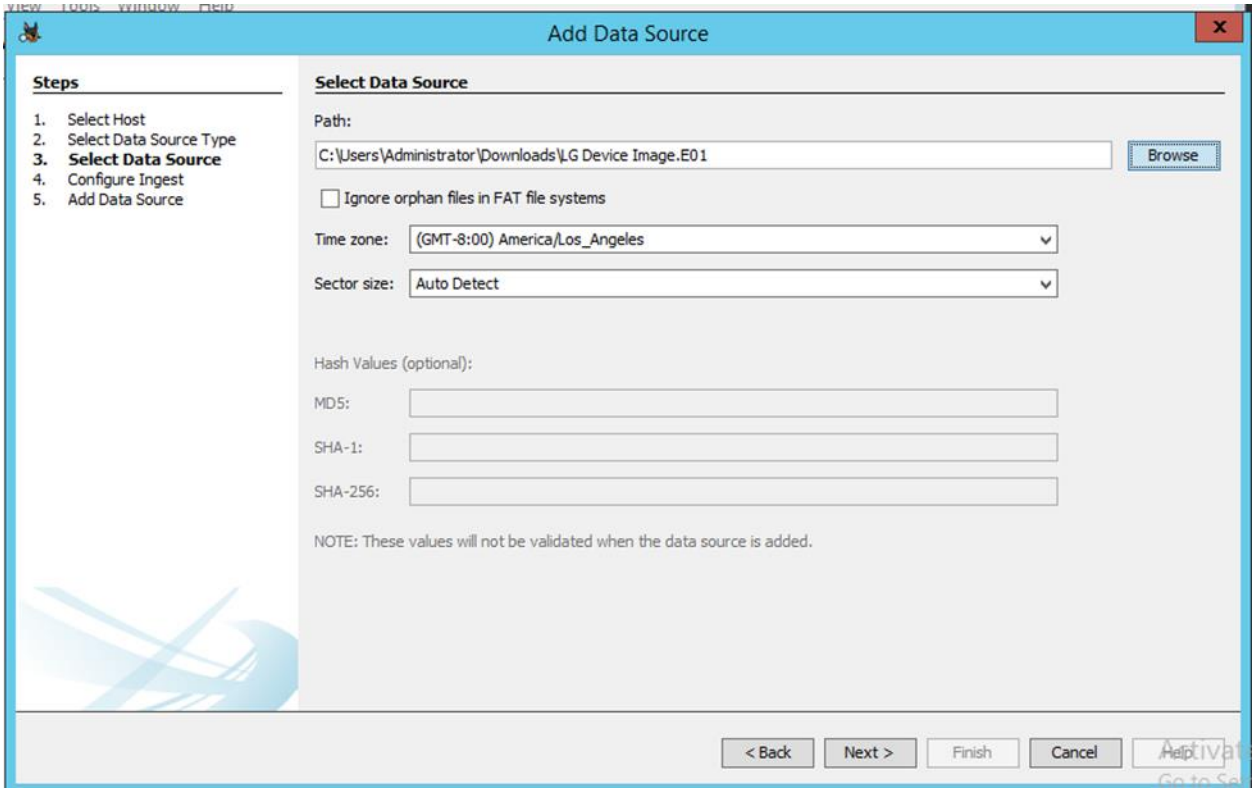


- Enter optional information as shown below and click and click “Finish”.

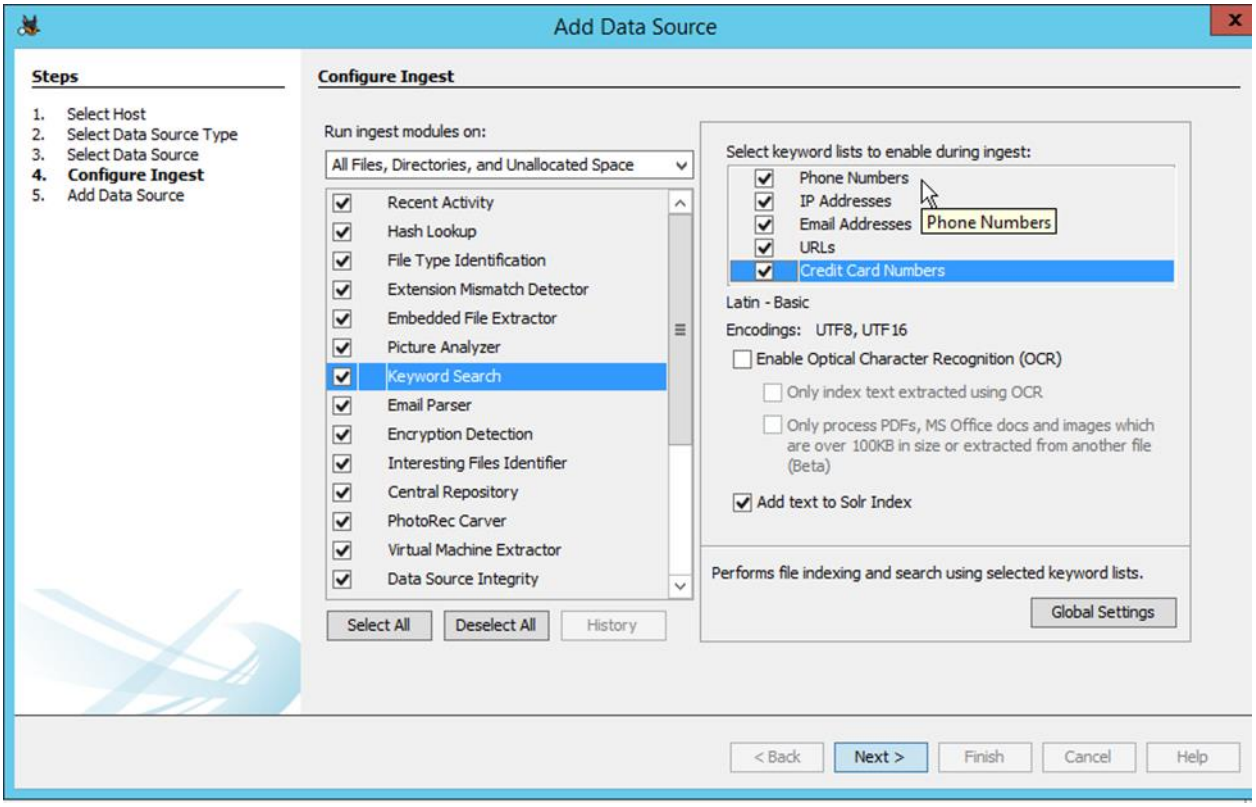




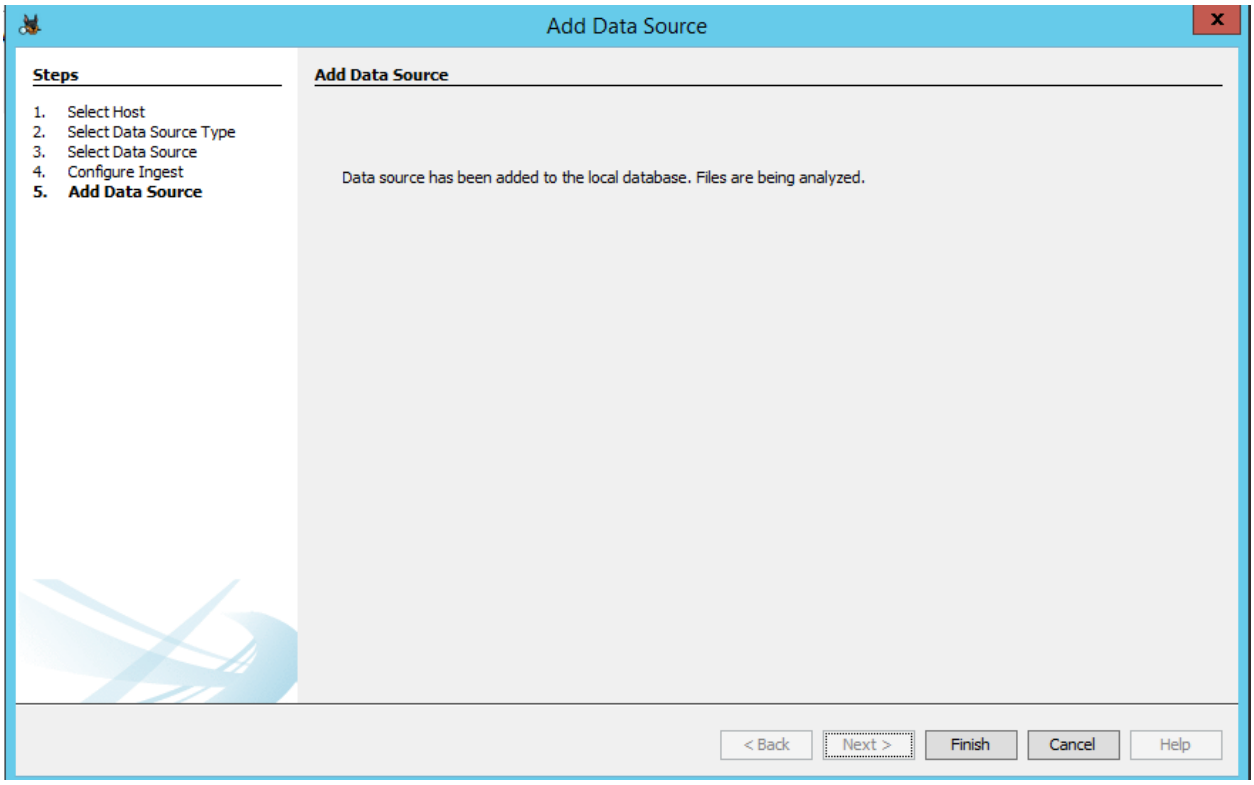
- The add data source window appears as below, under step 3 enter the path to the LG Device Image and then click next.



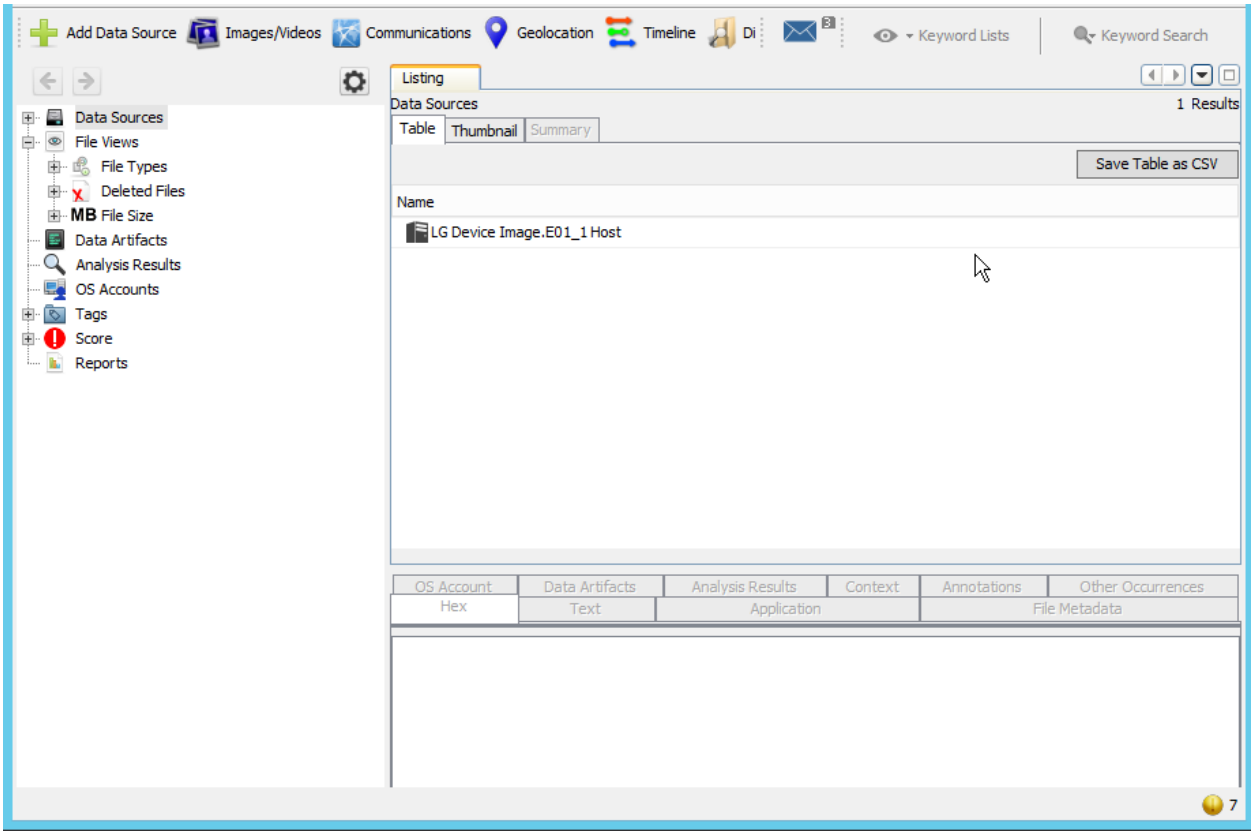
- Under the configure ingest module ensure to check all modules as shown below. Select each module on the left pane with their associated keywords to appear on the right pane. Ensure to check all the keywords for each selected module and click “Next”.



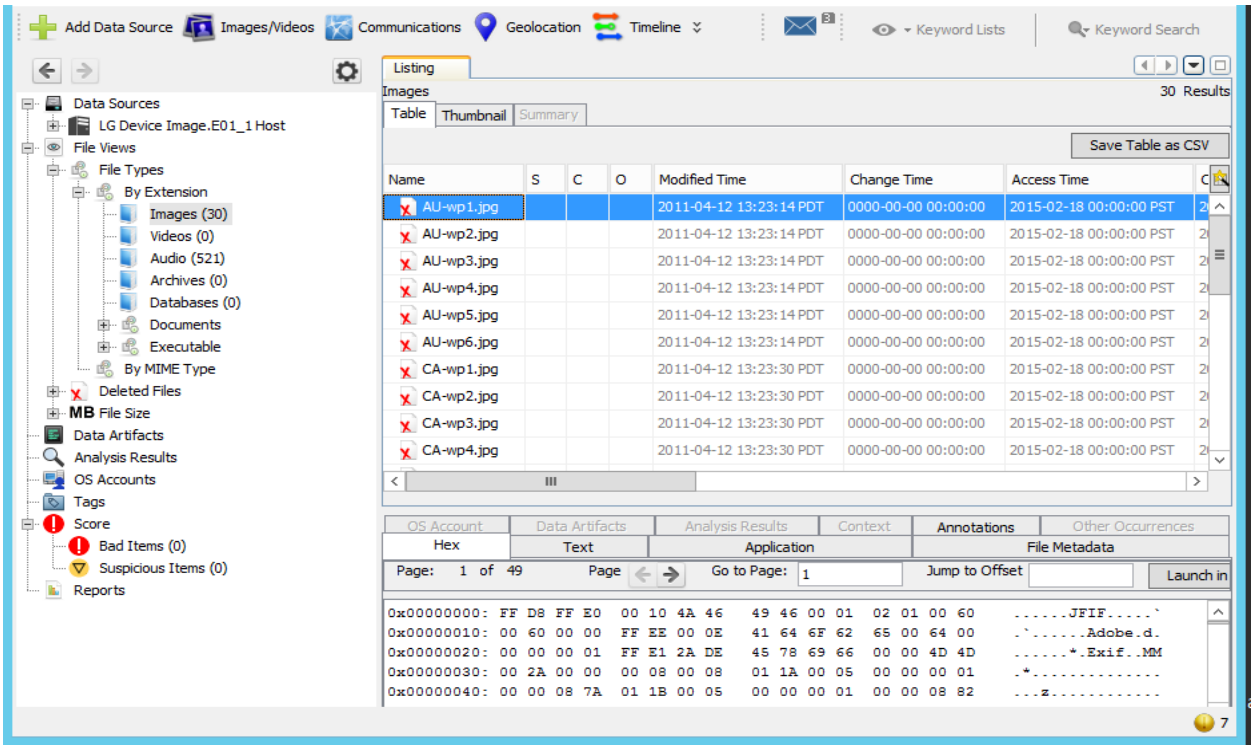
- Autopsy will analyze the files in the image file and a data source wizard appears as shown below, click on “Finish”.



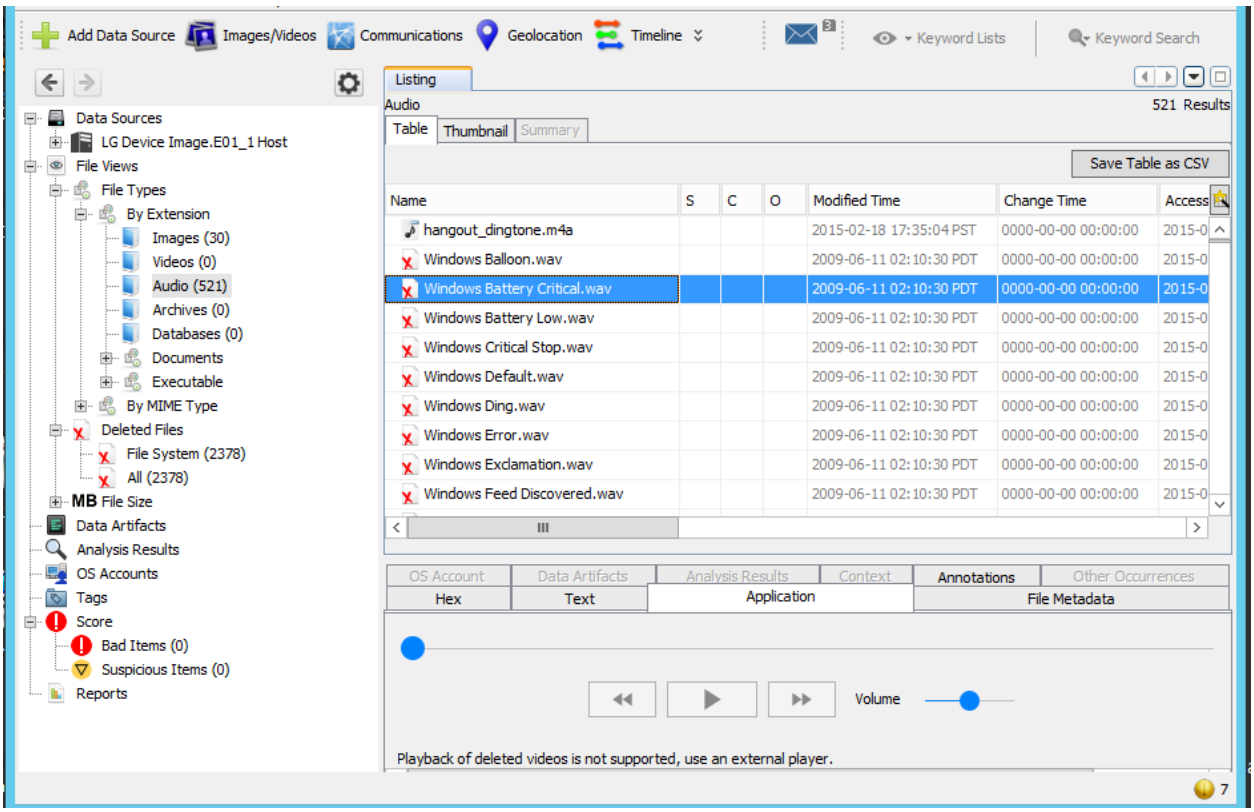
- The below appears, wait until autopsy completes analyzing the image file. observe the status at the lower right corner of the autopsy window.



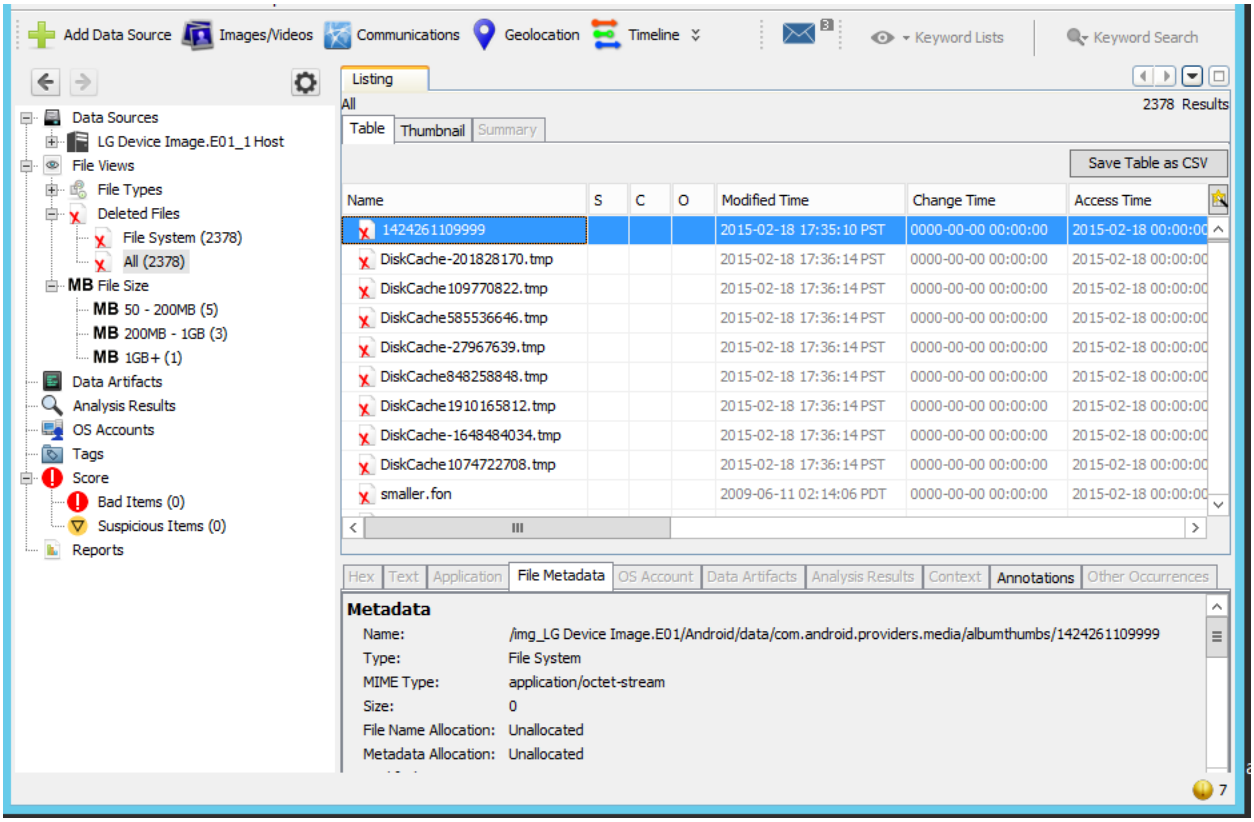
- On the left pane, expand the file views -> file type ->by extension, select images; it displays important information such as modified time, changed time and access time.



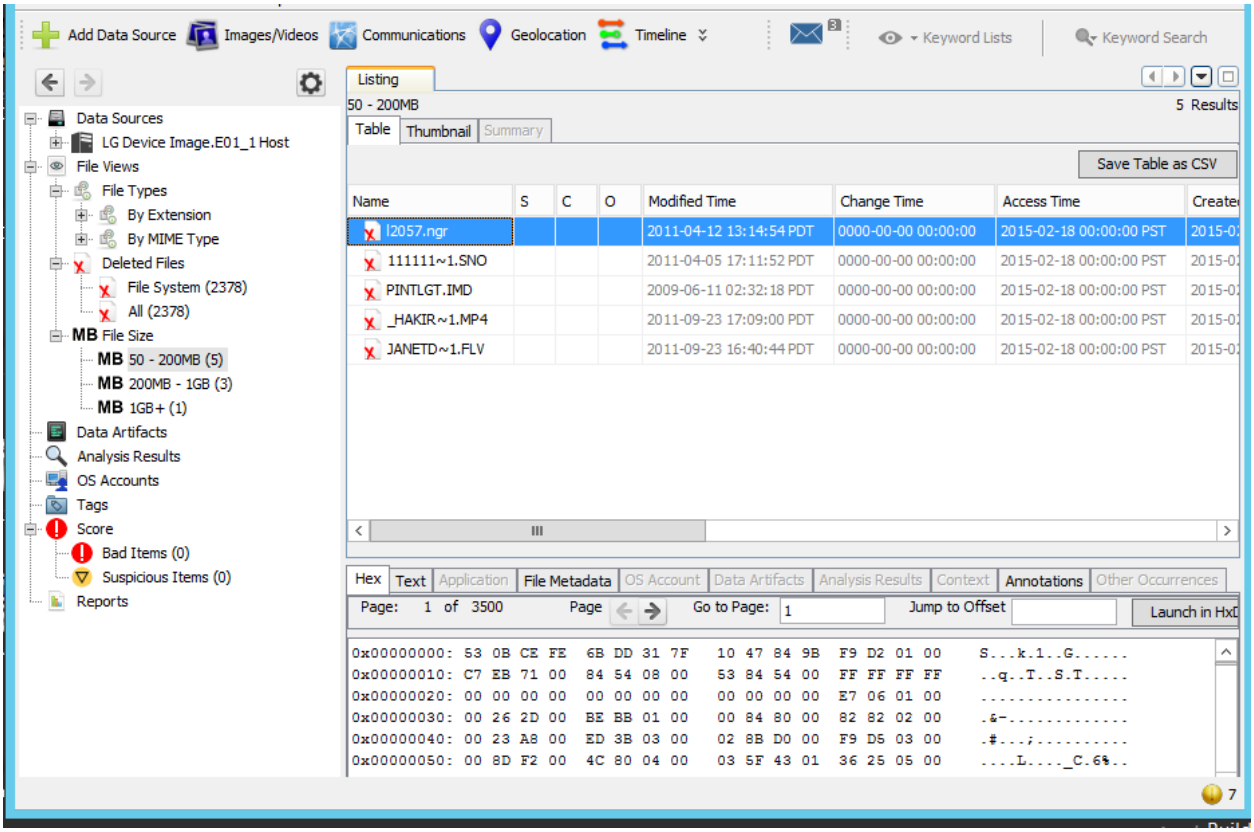
- Audio node lists all the audios contained in the audio file.



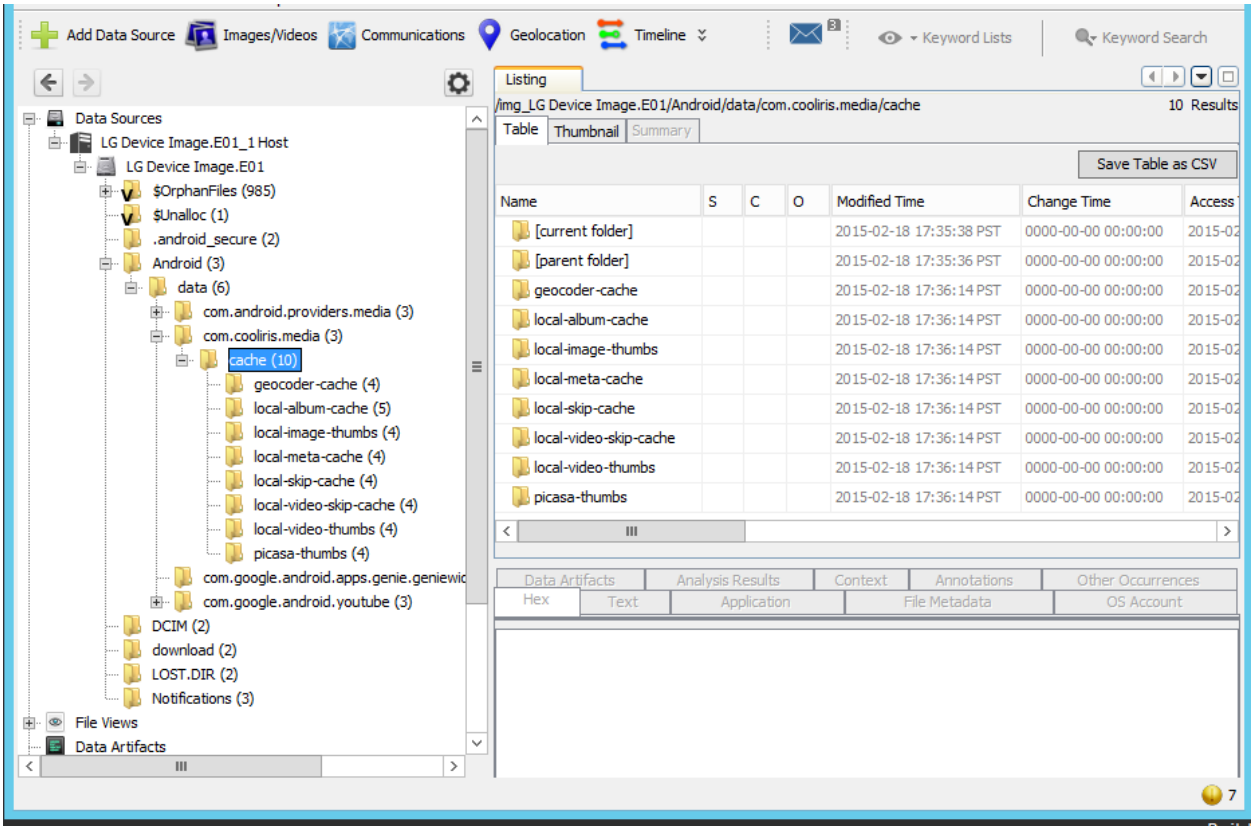
- Expand views -> deleted files ->all on the left pane as shown below, it displays all the deleted files that have been recovered indicated by a red colored cross mark.



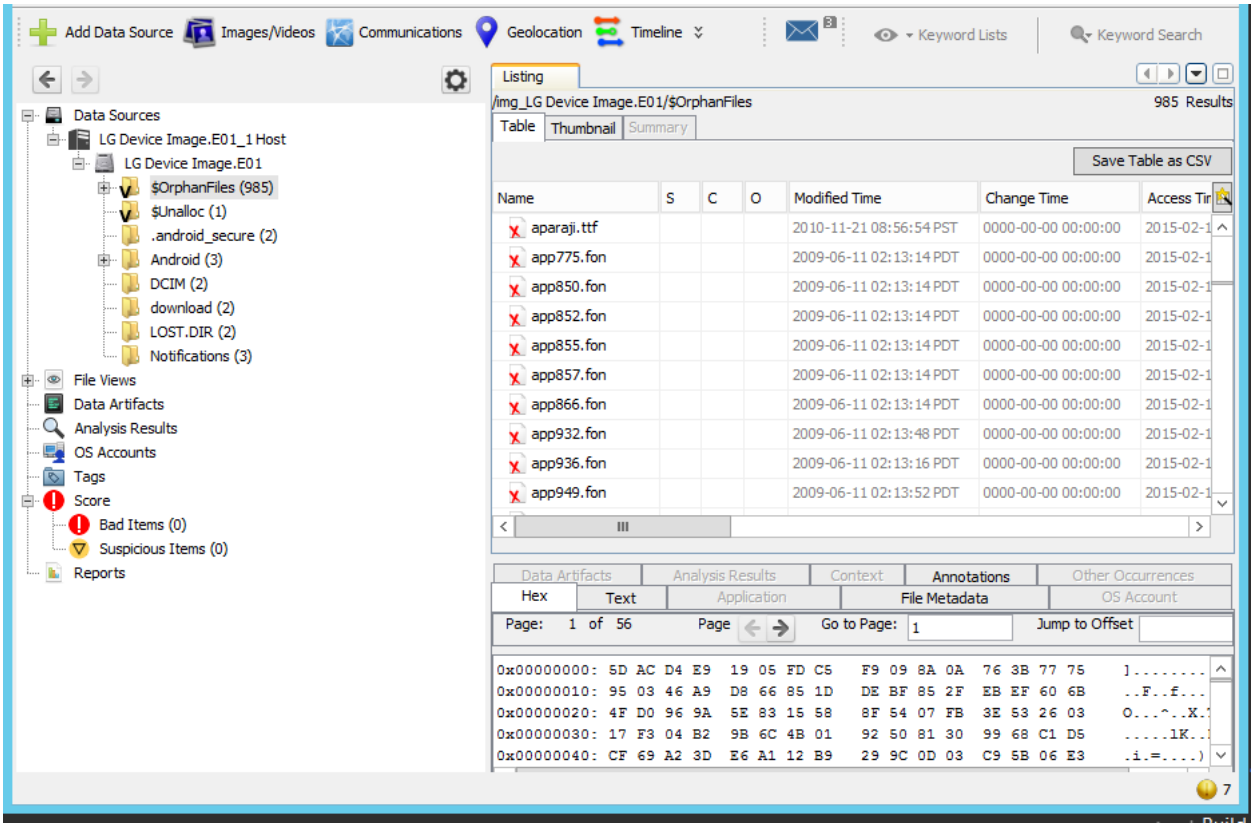
- Autopsy classifies files based on sizes in three sections as shown in the below screenshot.



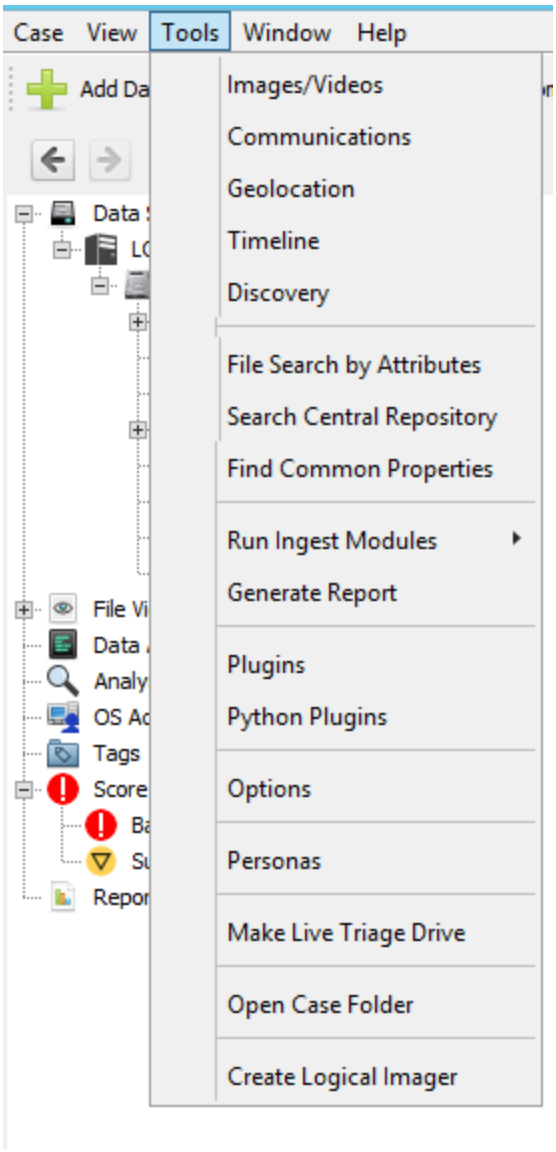
- Expand data sources ->image file [LG Device Image.E01]->android->data->com. cooliris. media ->cache. It displays all files stored in cache.



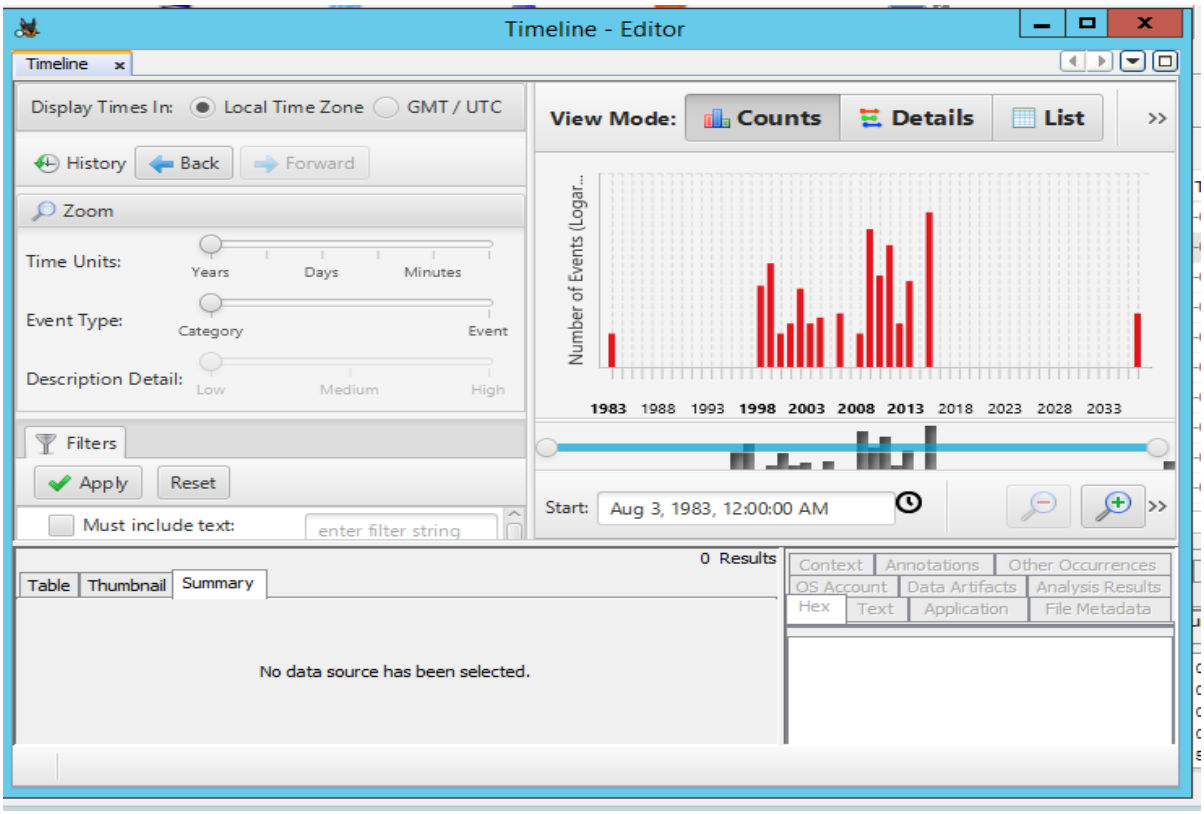
- Autopsy displays directory named OrphanFiles that contain broken files as shown below.



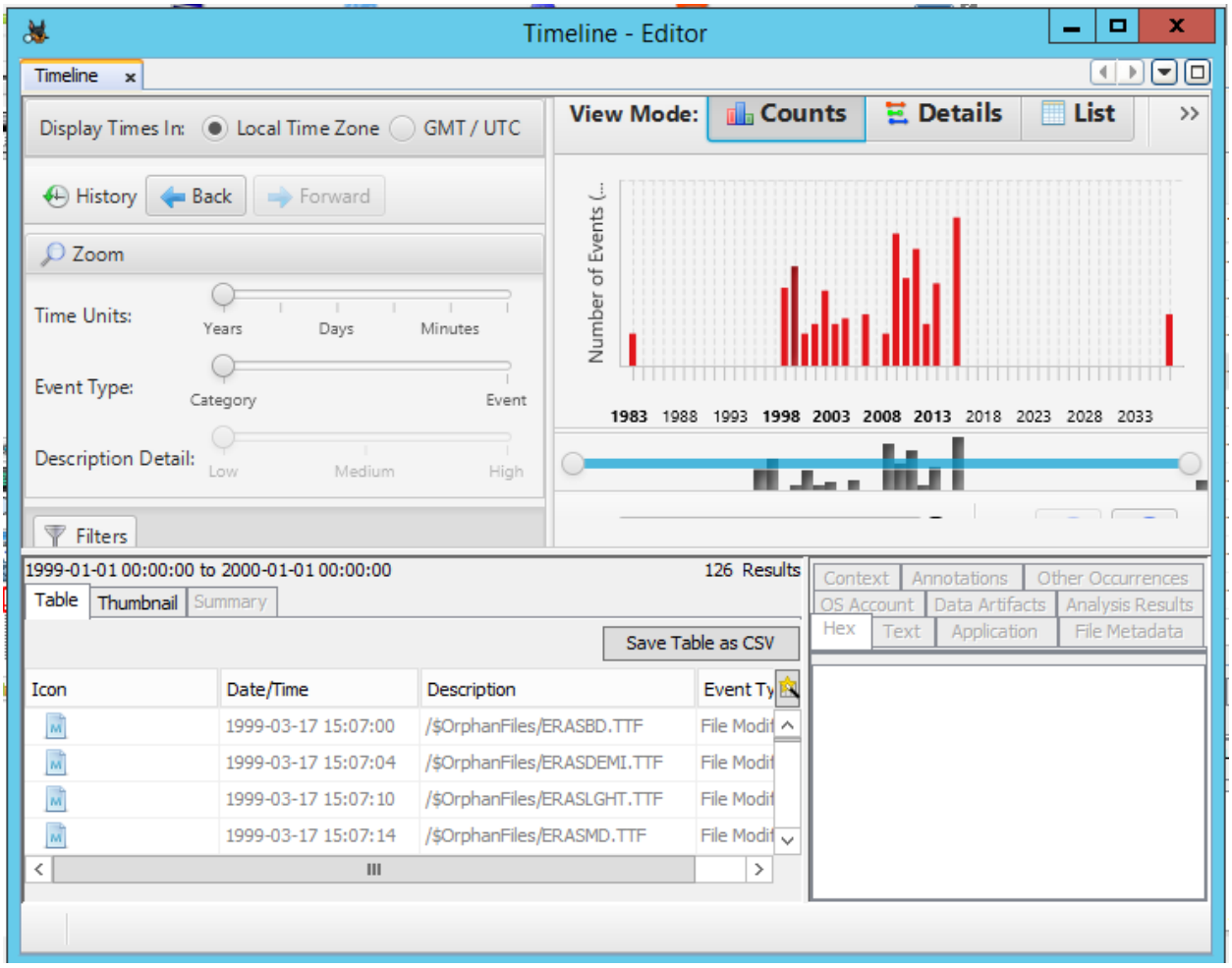
- Timeline helps to determine filesystem events on the device during a selected period.



- The red color bars represent filesystem activities.

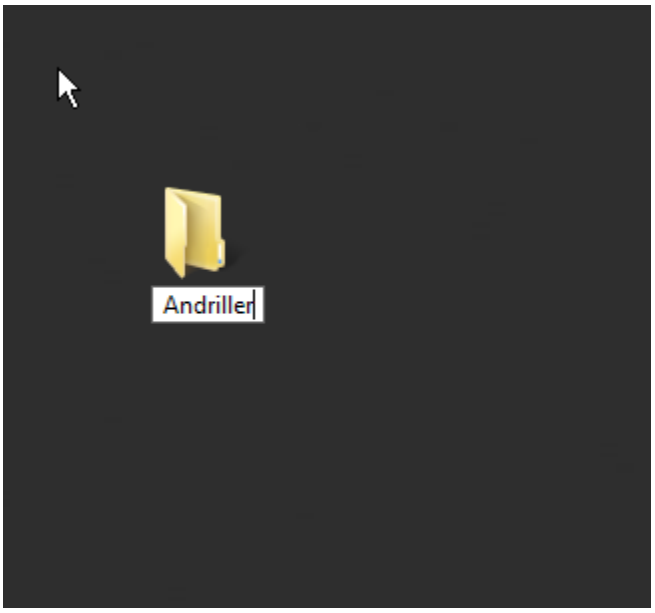


- Choose a time interval and select a bar from the graph autopsy displays all the filesystem events that occurred during the time interval associated with the selected bar.

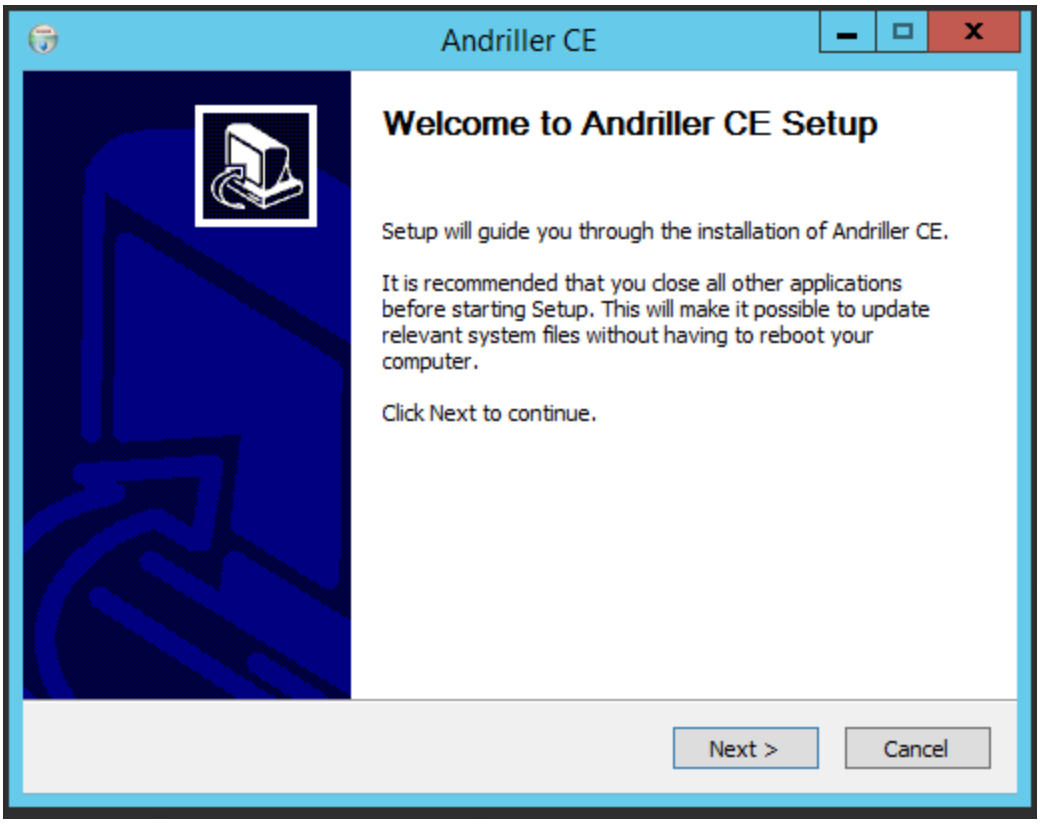

Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail: Low Medium High
Filters
View Mode: Counts Details List
Number of Events (...
1983 1988 1993 1998 2003 2008 2013 2018 2023 2028 2033
1999-01-01 00:00:00 to 2000-01-01 00:00:00
126 Results
Table Thumbnail Summary
Save Table as CSV
Icon Date/Time Description Event Ty
1999-03-17 15:07:00 /$OrphanFiles/ERASBD.TTF File Modif
1999-03-17 15:07:04 /$OrphanFiles/ERASDEMI.TTF File Modif
1999-03-17 15:07:10 /$OrphanFiles/ERASLGHT.TTF File Modif
1999-03-17 15:07:14 /$OrphanFiles/ERASMD.TTF File Modif
Context Annotations Other Occurrences
OS Account Data Artifacts Analysis Results
Hex Text Application File Metadata

LAB 2: ANALYZING AN ANDROID DEVICE USING ANDRILLER

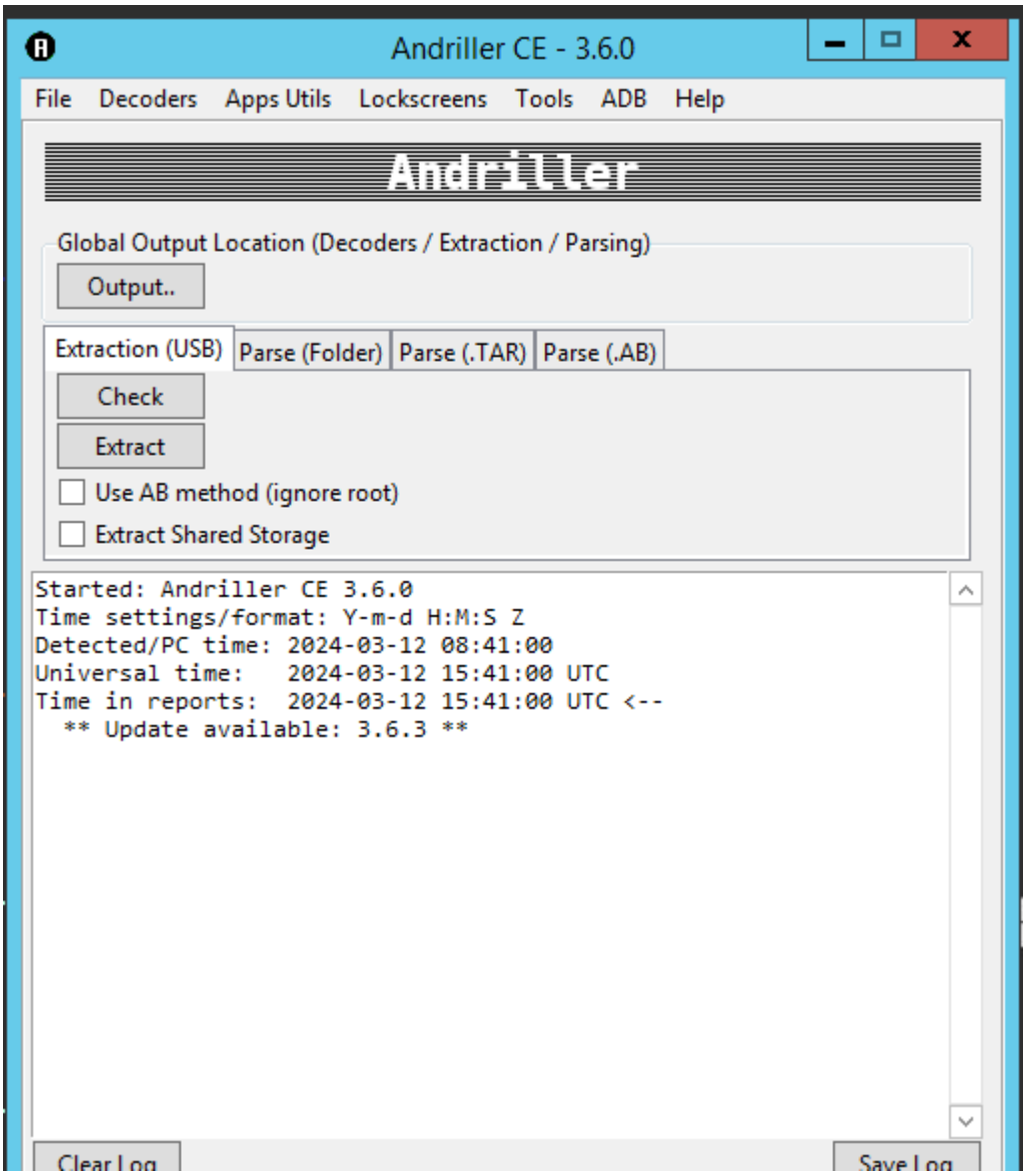
- Log on to window server 2012 virtual machine and create a folder named Andriller on the Desktop.



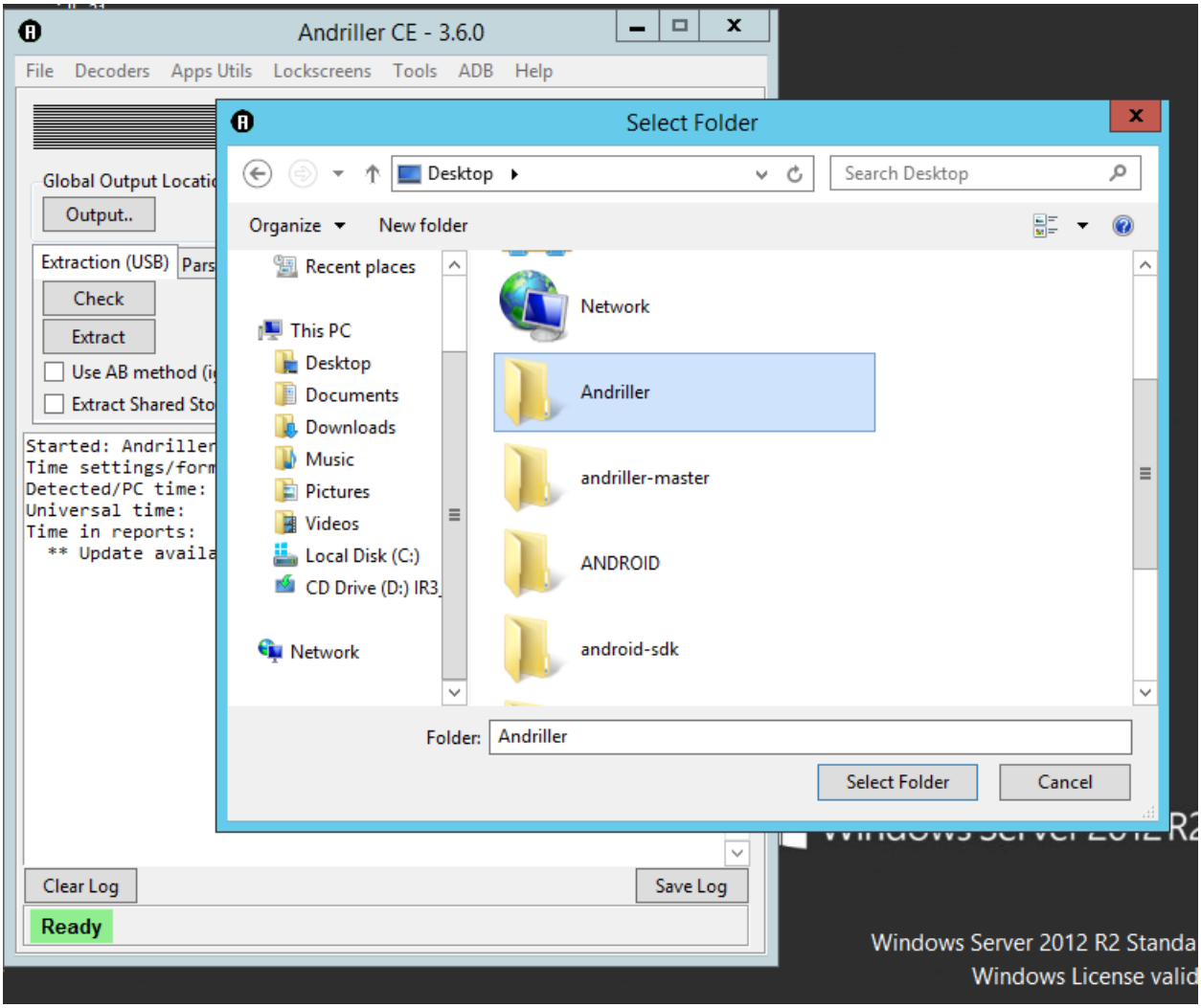
- Double the Andriller exe file and follow the wizard.

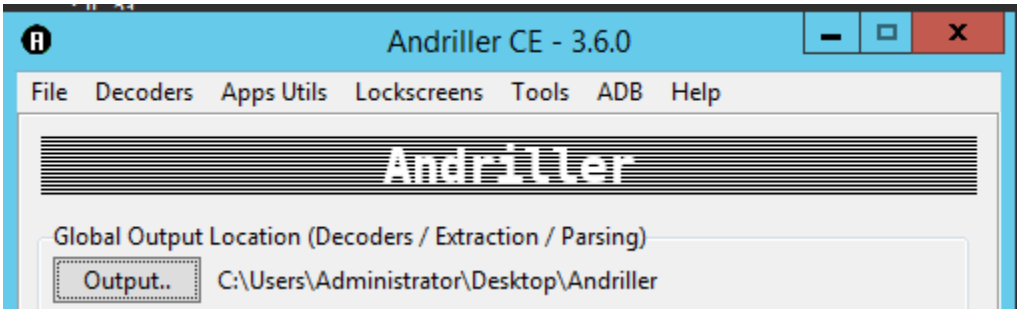


- Andriller main window appears as shown in the screenshot below.

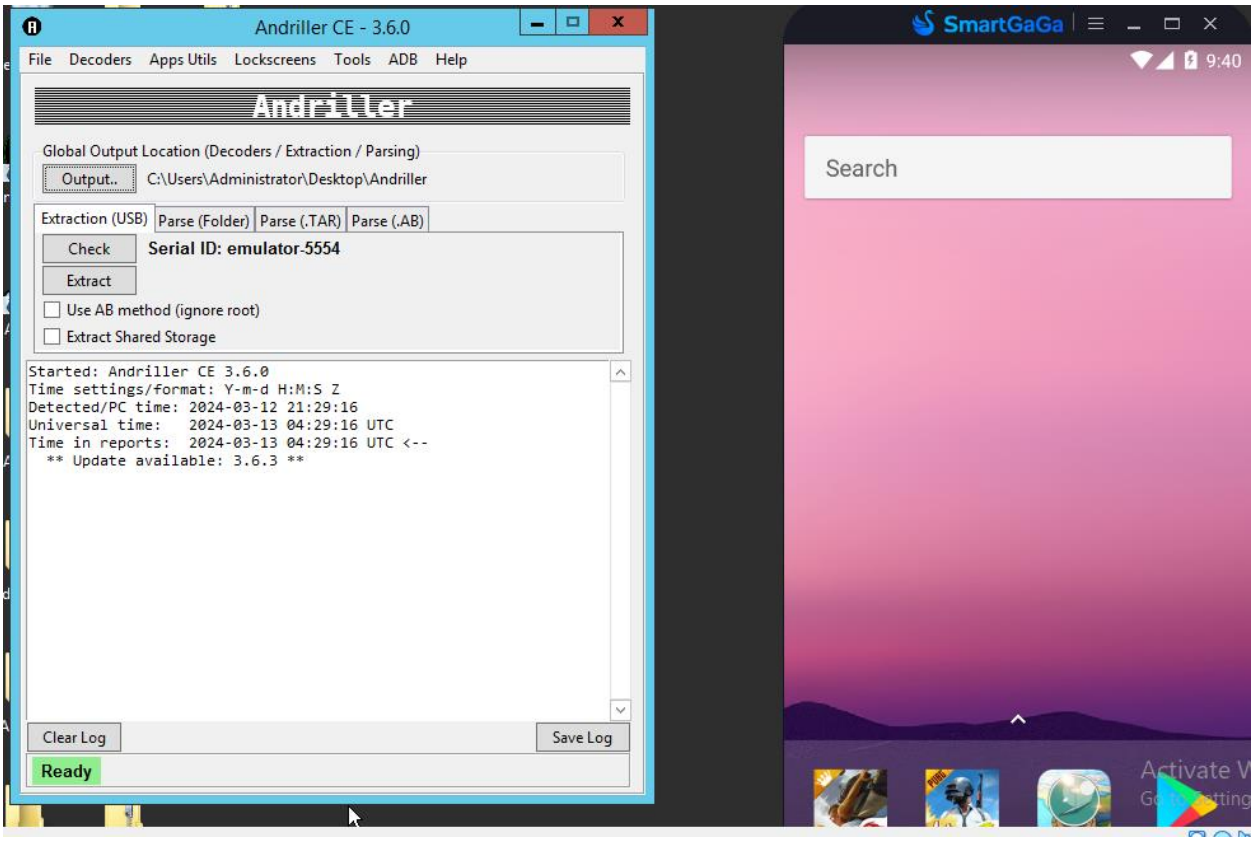


- To specify output location to store all the logs and data for andriller, click the "output" in the andriller window and navigate to Desktop and select the Andriller folder which we created earlier as shown on the screenshot below and click on select folder.

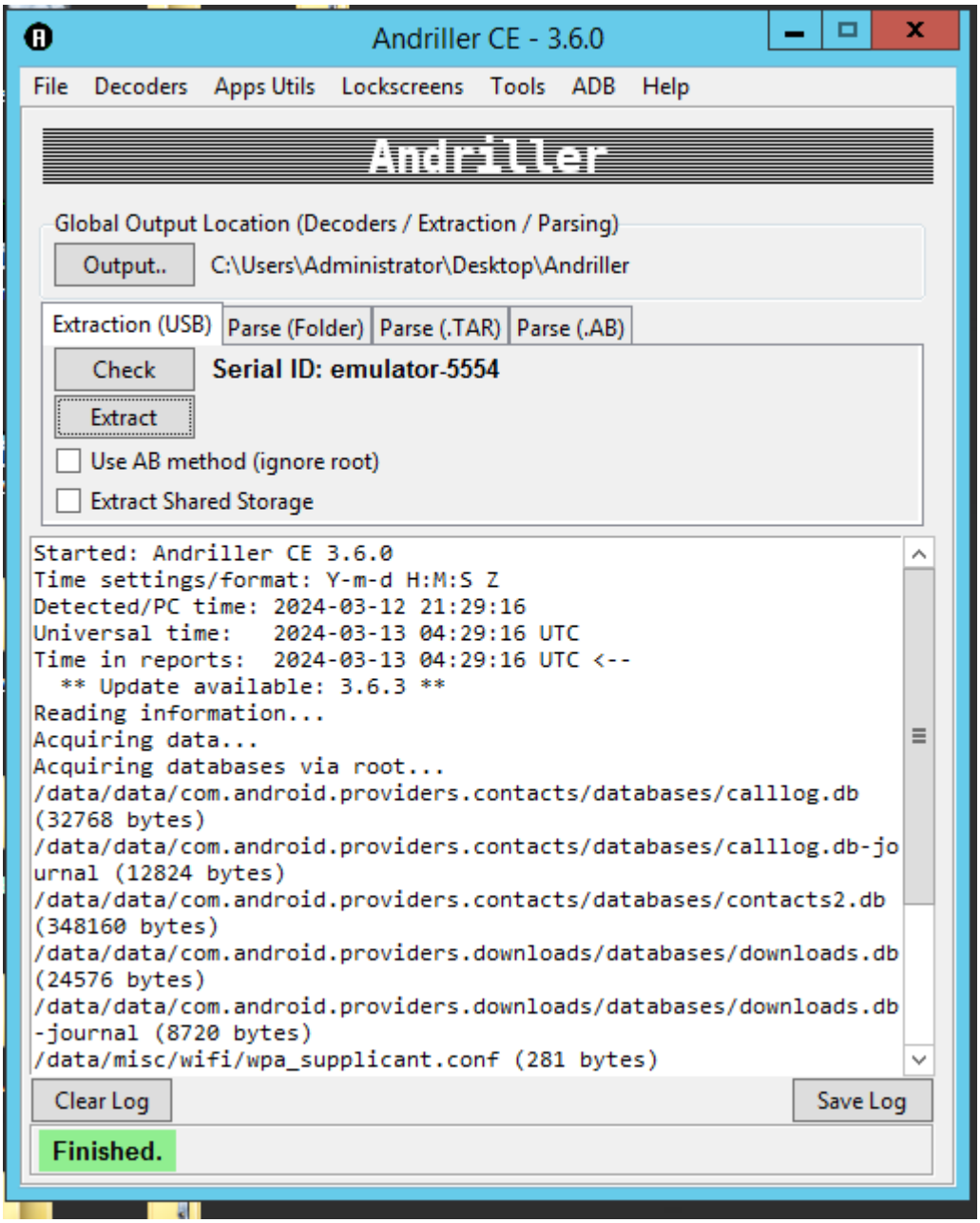




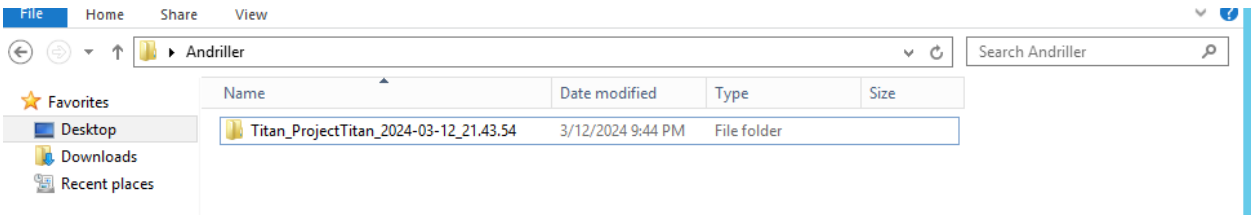
- Next, we click on “check” to see if android emulator is connected to andriller. The serial id of the emulator displayed as shown below rendering a success in the connection between andriller and the android emulator.



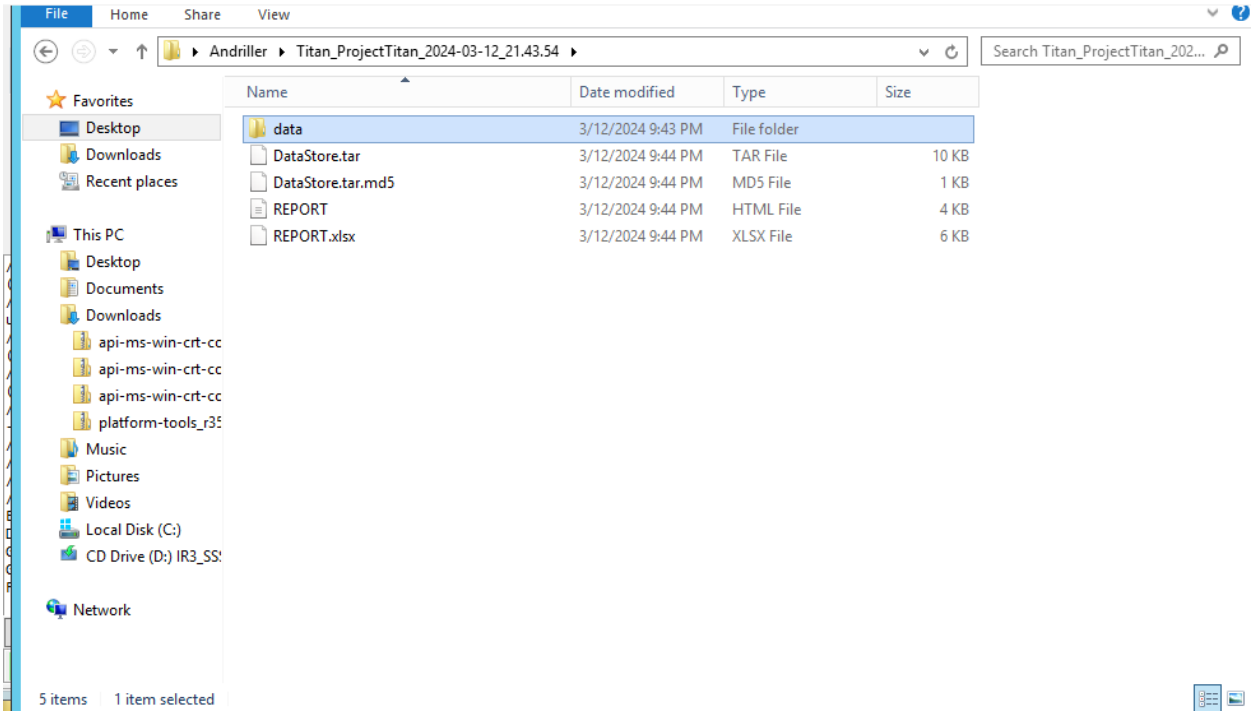
- Once the device is detected, click on “Extract”. To begin extraction. Andriller extracts the databases and other useful information as shown in the following screenshot.



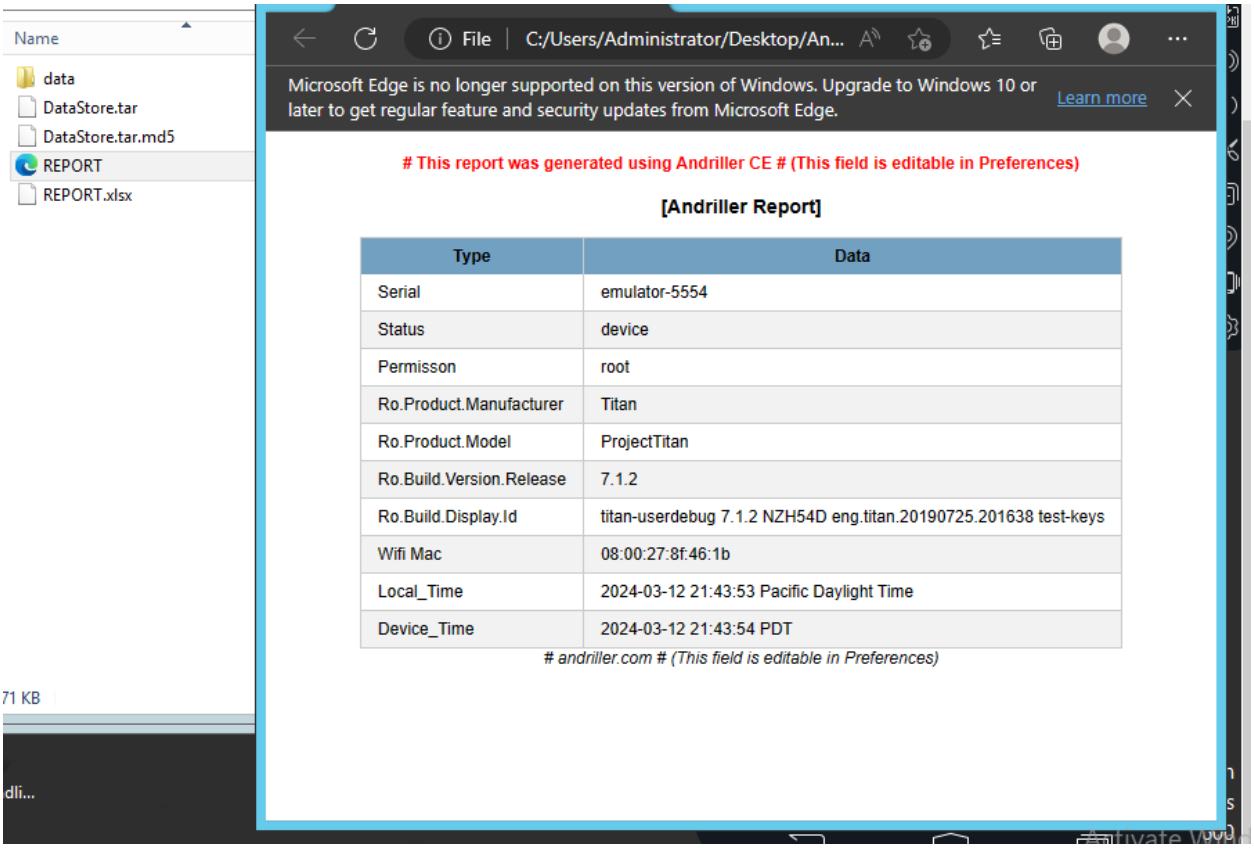
- Andriller creates a directory inside the Andriller folder with the name of the device followed by the timestamp as shown below.



- Navigate to the Andriller folder located on the Desktop and open the folder which stored the extracted files and databases. Double click on “REPORT” to open it. It appears in the default browser and displays import information like device id, model etc.
  NOTE: click on the “REPORT” without the .xlsx extension.



- The below screenshot is the results displayed after opening the “REPORT” file.


Name
data
DataStore.tar
DataStore.tar.md5
REPORT
REPORT.xlsx
71 KB
File | C:/Users/Administrator/Desktop/An...
Microsoft Edge is no longer supported on this version of Windows. Upgrade to Windows 10 or later to get regular feature and security updates from Microsoft Edge.
Learn more
This report was generated using Andriller CE # (This field is editable in Preferences)
[Andriller Report]
Type
Data
Serial
emulator-5554
Status
device
Permisson
root
Ro.Product.Manufacturer
Titan
Ro.Product.Model
ProjectTitan
Ro.Build.Version.Release
7.1.2
Ro.Build.Display.Id
titan-userdebug 7.1.2 NZH54D eng.titan.20190725.201638 test-keys
Wifi Mac
08:00:27:8f:46:1b
Local_Time
2024-03-12 21:43:53 Pacific Daylight Time
Device_Time
2024-03-12 21:43:54 PDT
andriller.com # (This field is editable in Preferences)