

MOBILE FORENSICS LAB WORK

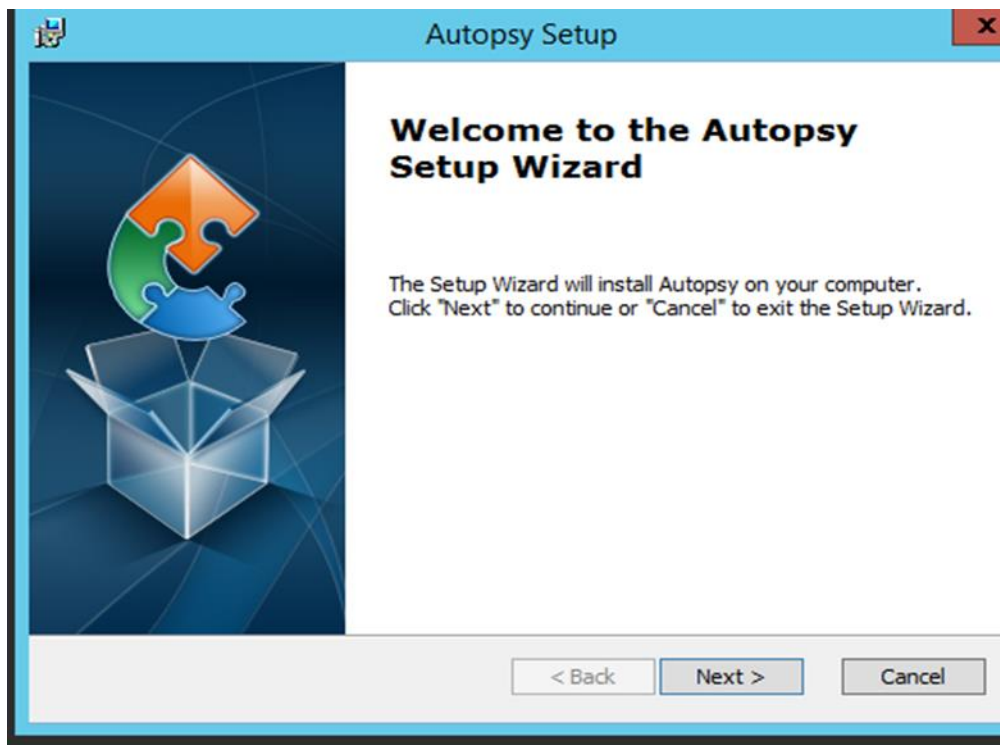
BY

Dewton Kiprop

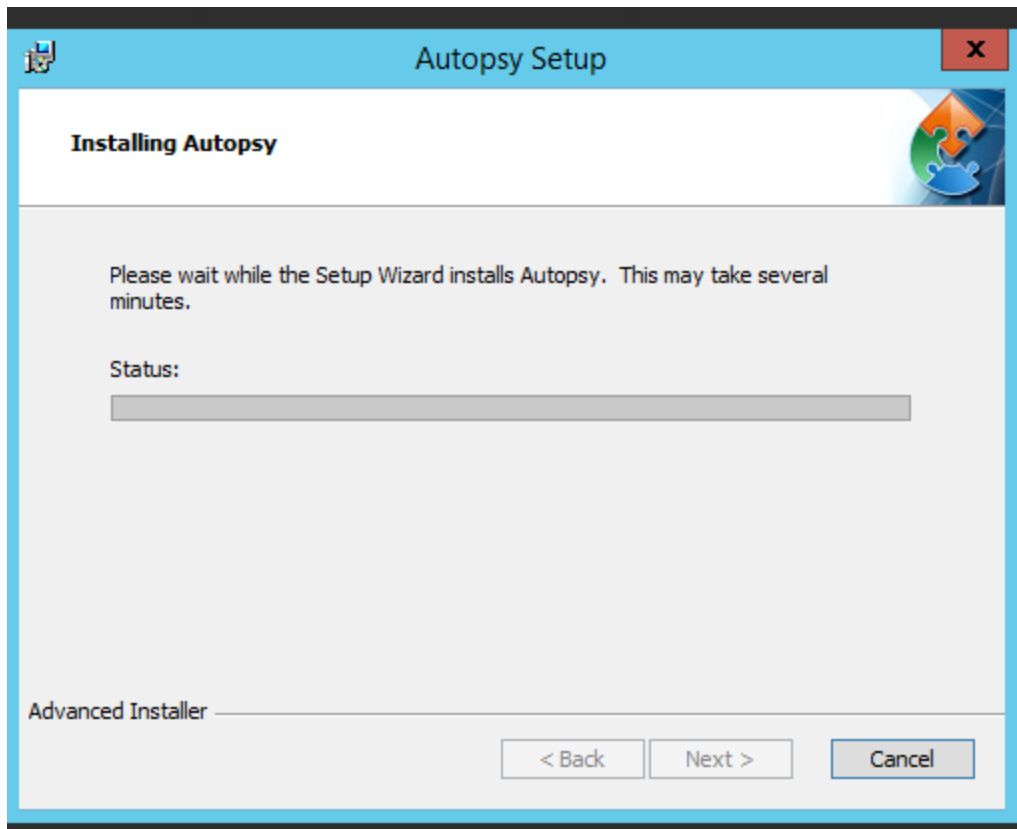


LAB 1: ANALYZING FORENSIC IMAGE AND CARVING DELETED FILES USING AUTOPSY

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



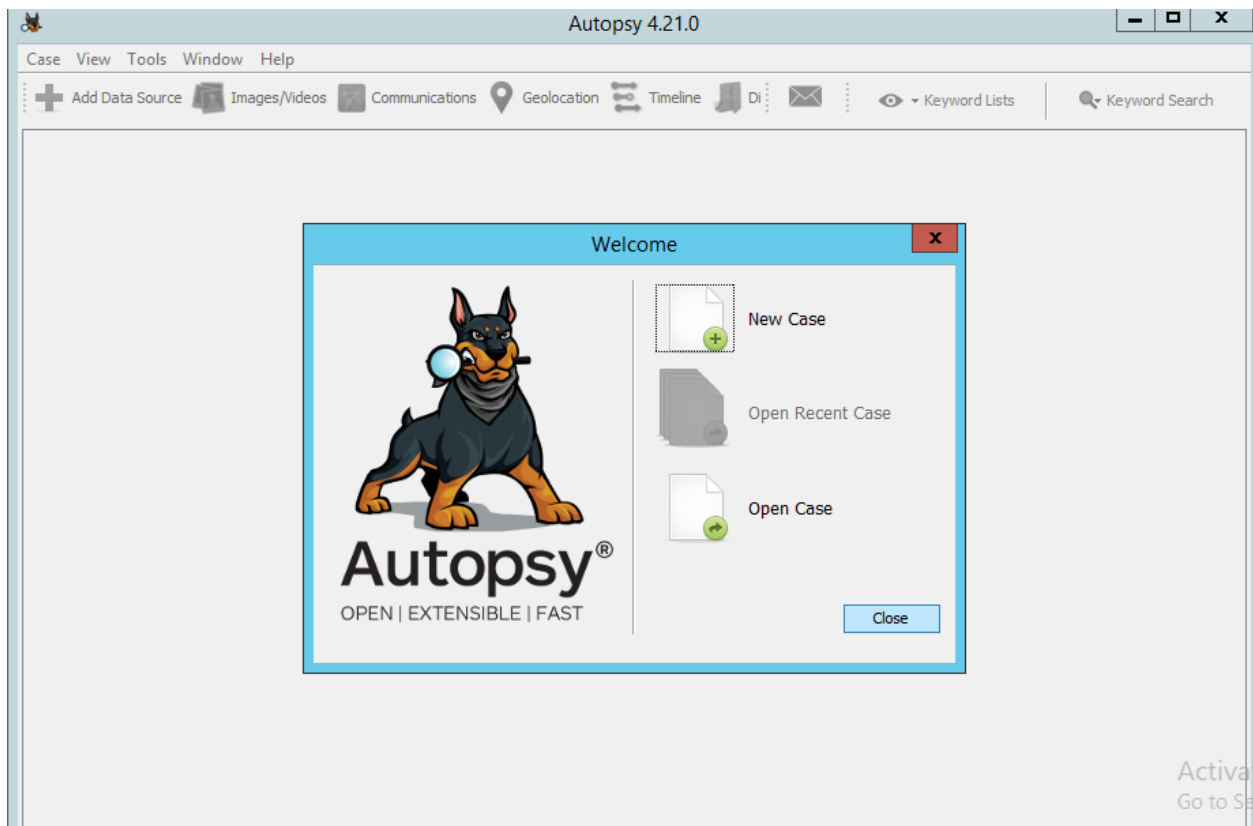
- The installation begins as shown below.



- 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”.



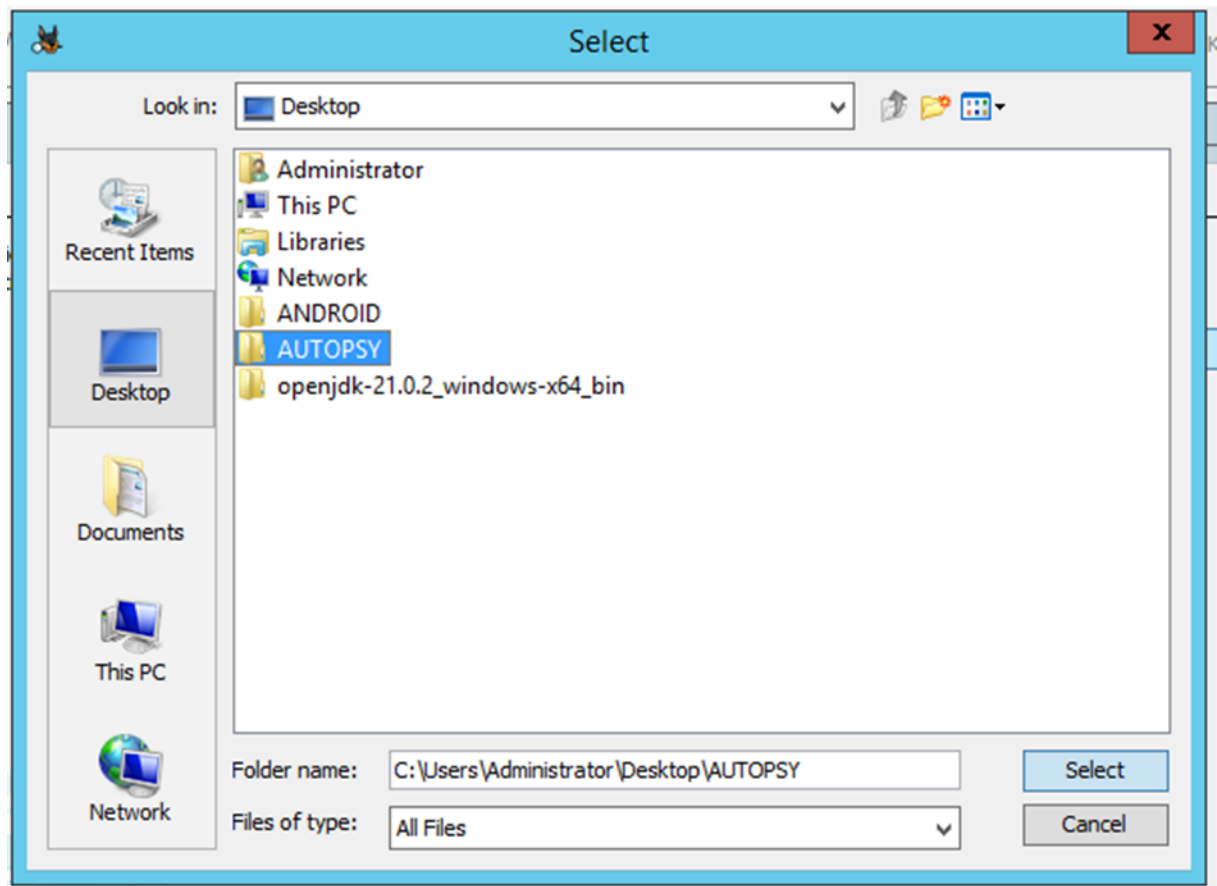
- The new case information window appears. under the Case Name enter a name.

The screenshot shows the 'New Case Information' dialog box. The title bar reads 'New Case Information'. On the left, under the 'Steps' section, there are two steps: '1. Case Information' and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields and controls:

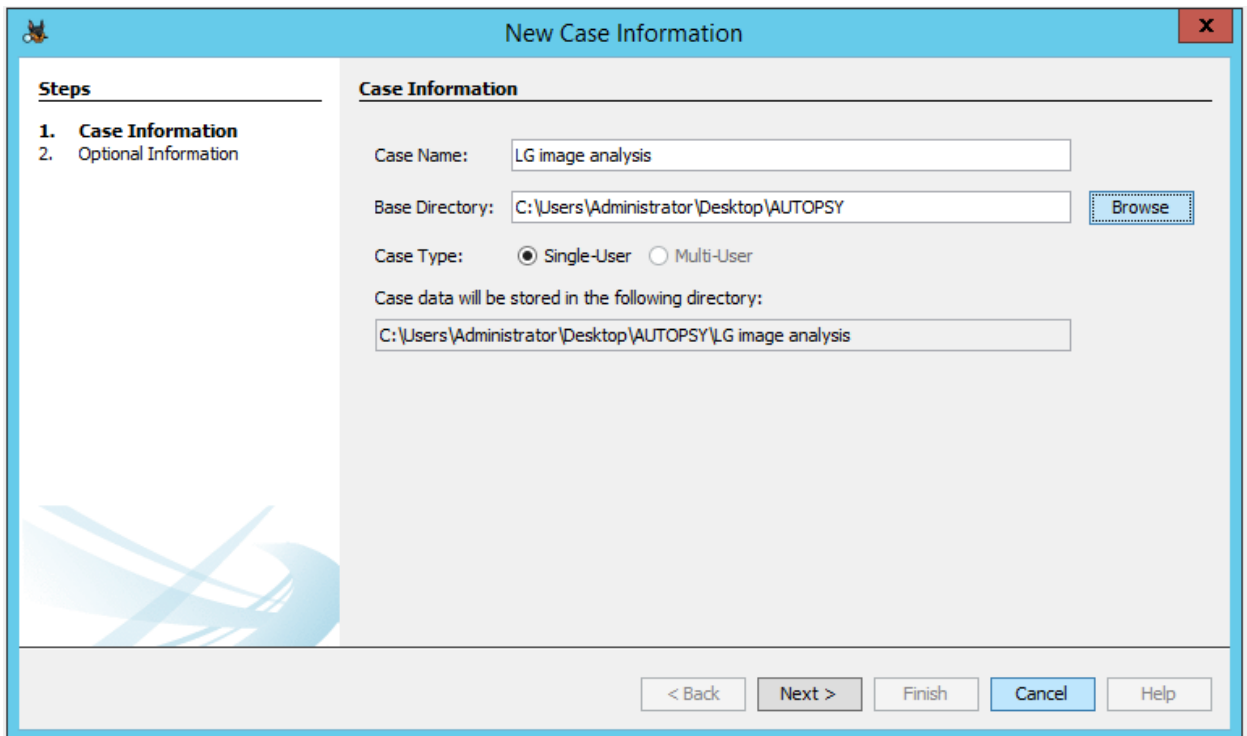
- 'Case Name:' followed by a text box containing 'LG image analysis'.
- 'Base Directory:' followed by a text box and a 'Browse' button.
- 'Case Type:' followed by two radio buttons: 'Single-User' (which is selected) and 'Multi-User'.
- 'Case data will be stored in the following directory:' followed by a text box containing '\\G image analysis'.

At the bottom of the dialog, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- 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”.

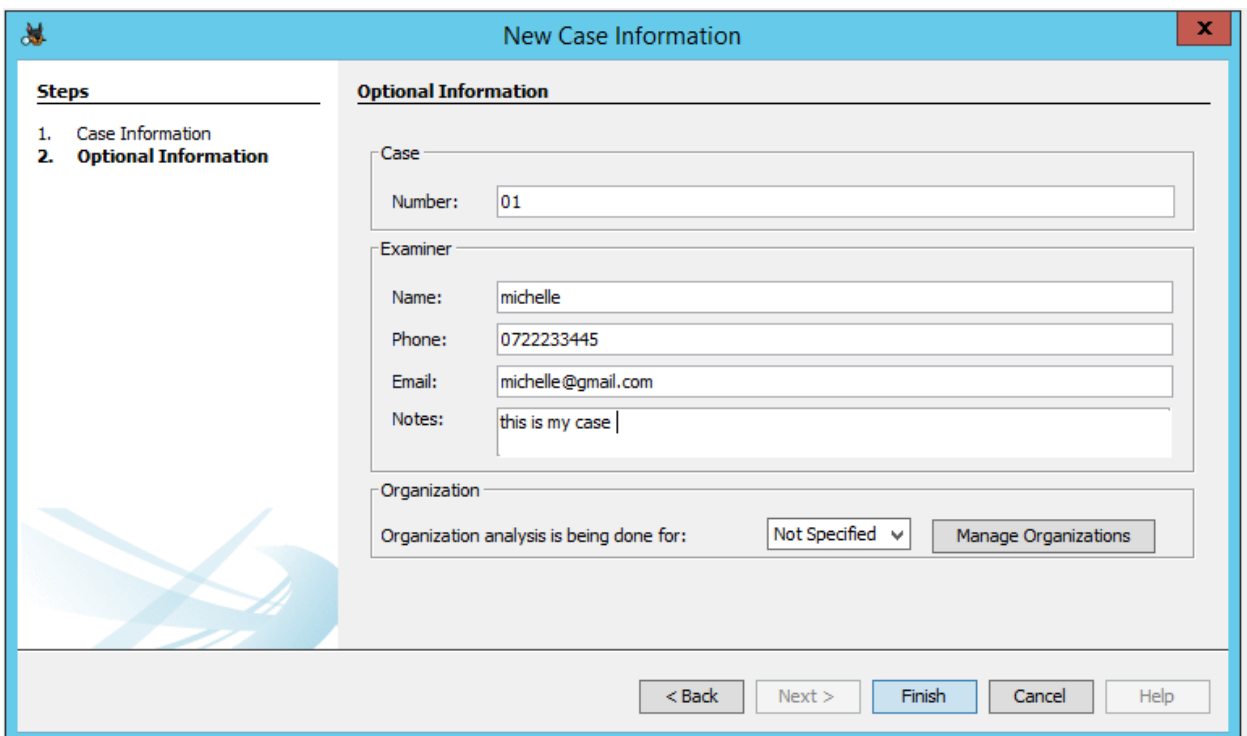


The dialog box is titled "New Case Information" and has a close button (X) in the top right corner. On the left, a "Steps" pane shows "1. Case Information" as the current step and "2. Optional Information" as the next step. The main area is titled "Case Information" and contains the following fields:

- Case Name:** A text box containing "LG image analysis".
- Base Directory:** A text box containing "C:\Users\Administrator\Desktop\AUTOPSY" with a "Browse" button to its right.
- Case Type:** Two radio buttons: "Single-User" (selected) and "Multi-User".
- Case data will be stored in the following directory:** A text box containing "C:\Users\Administrator\Desktop\AUTOPSY\LG image analysis".

At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

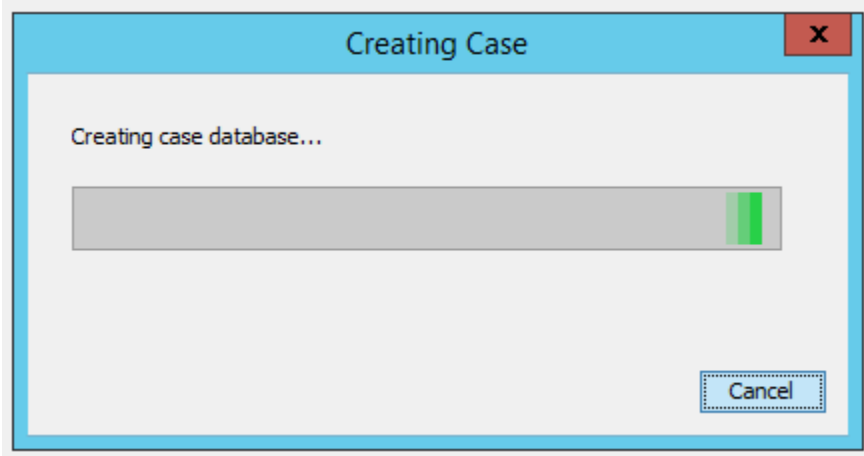
- Enter optional information as shown below and click and click “Finish”.



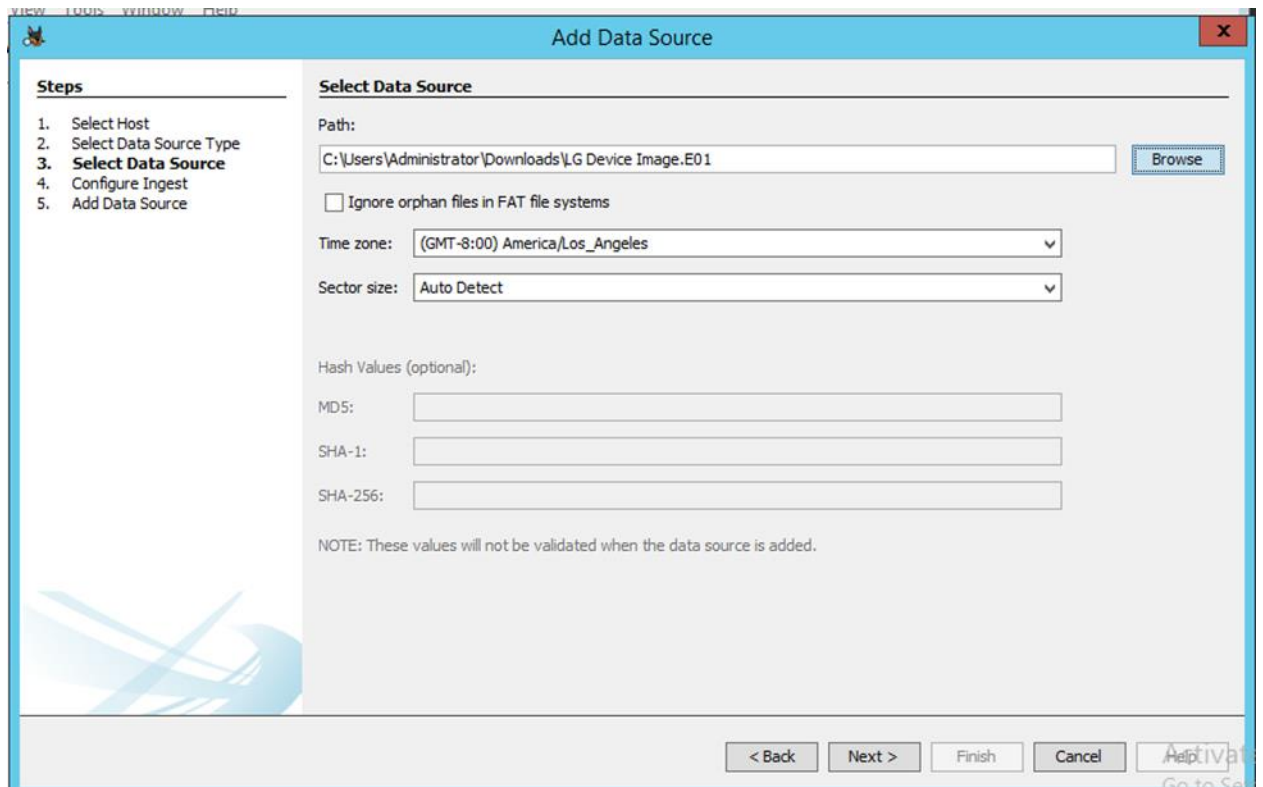
The dialog box is titled "New Case Information" and has a close button (X) in the top right corner. On the left, a "Steps" pane shows "1. Case Information" and "2. Optional Information" as the current step. The main area is titled "Optional Information" and contains the following fields:

- Case:** A text box containing "01".
- Examiner:** A group box containing four text boxes: "Name" (michelle), "Phone" (0722233445), "Email" (michelle@gmail.com), and "Notes" (this is my case |).
- Organization:** A group box containing a text box "Organization analysis is being done for:" followed by a dropdown menu showing "Not Specified" and a "Manage Organizations" button.

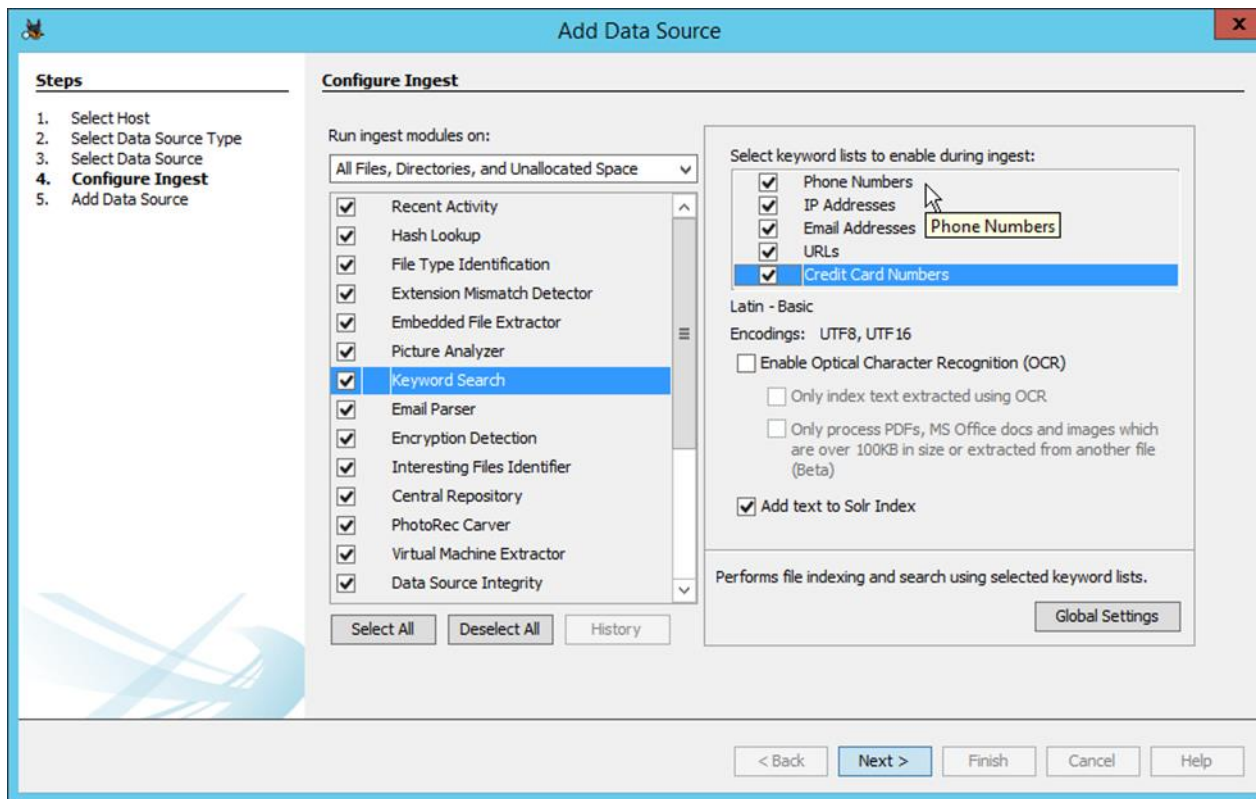
At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".



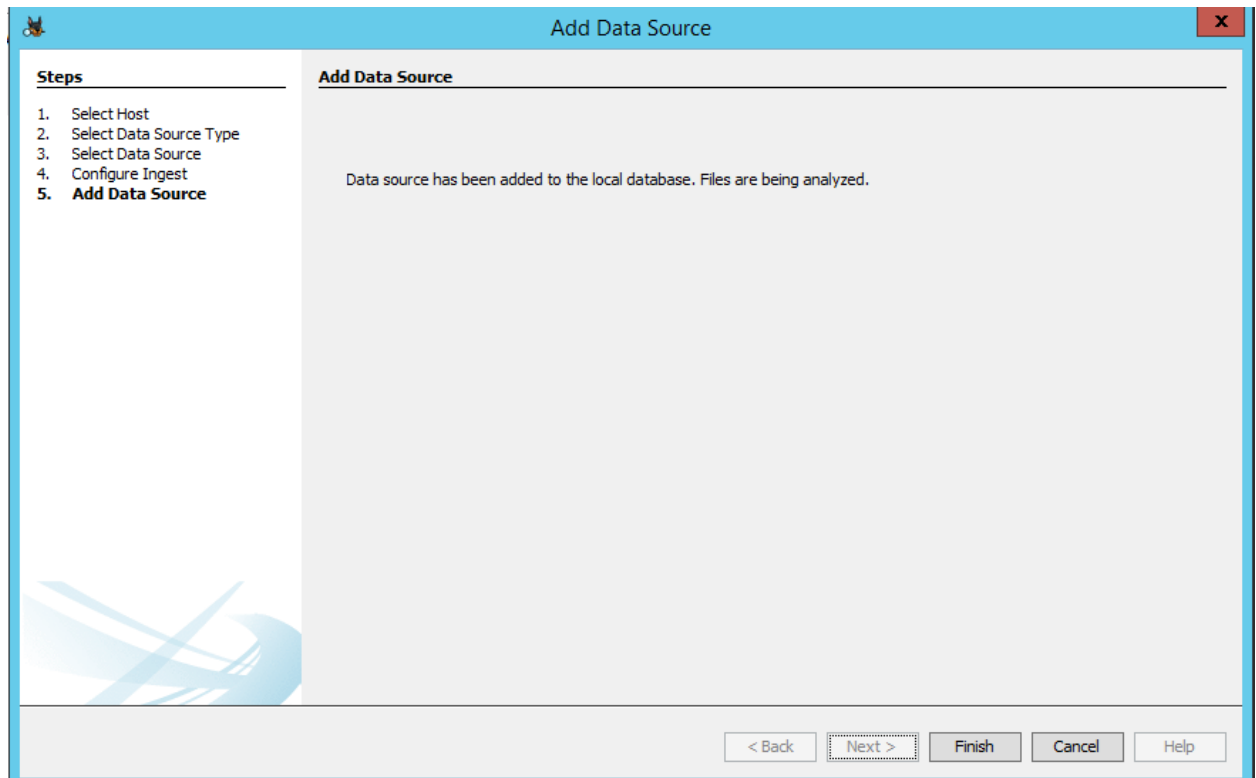
- The add data source window appears as below, under step 3 enter the path to the LG Device Image and then click next.



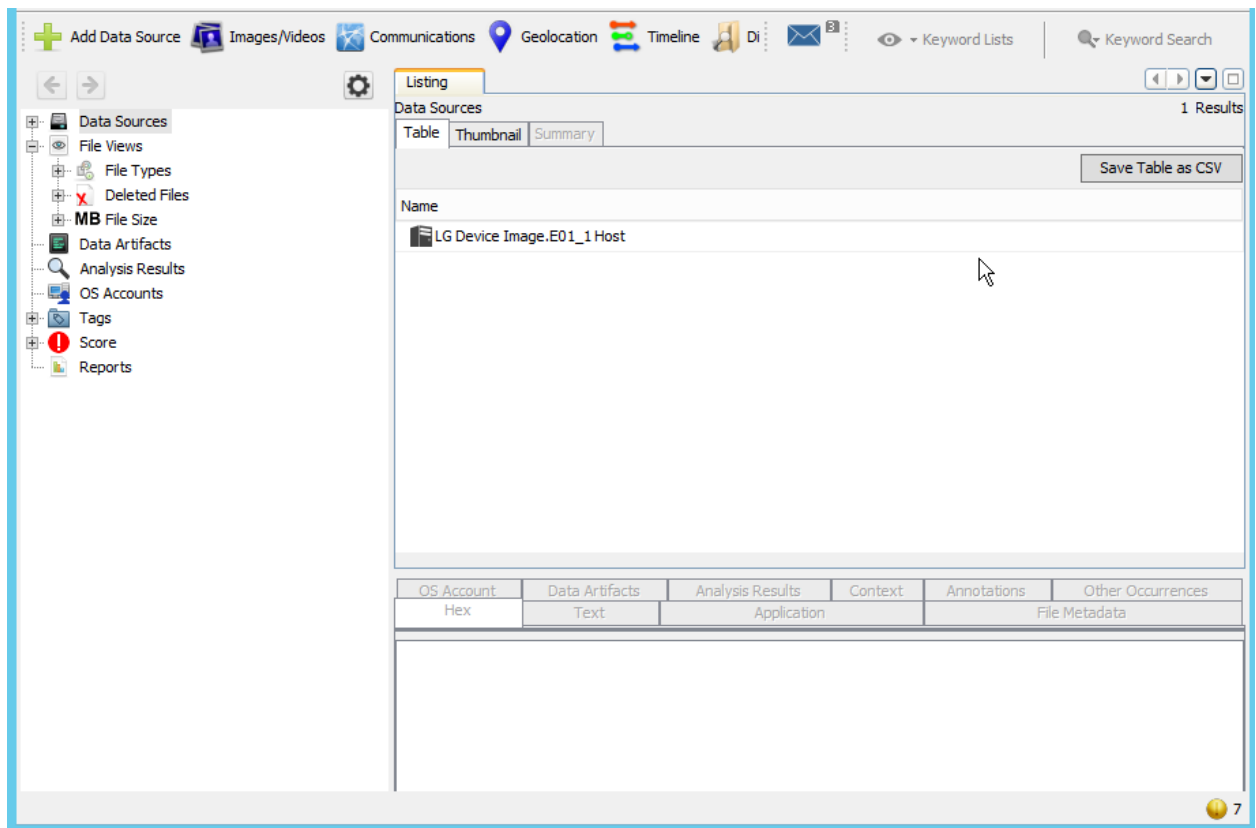
- Under the configure ingest module ensure to check all modules as shown below. Select each module on the left pane with their associated keywords to appear on the right pane. Ensure to check all the keywords for each selected module and click “Next”.



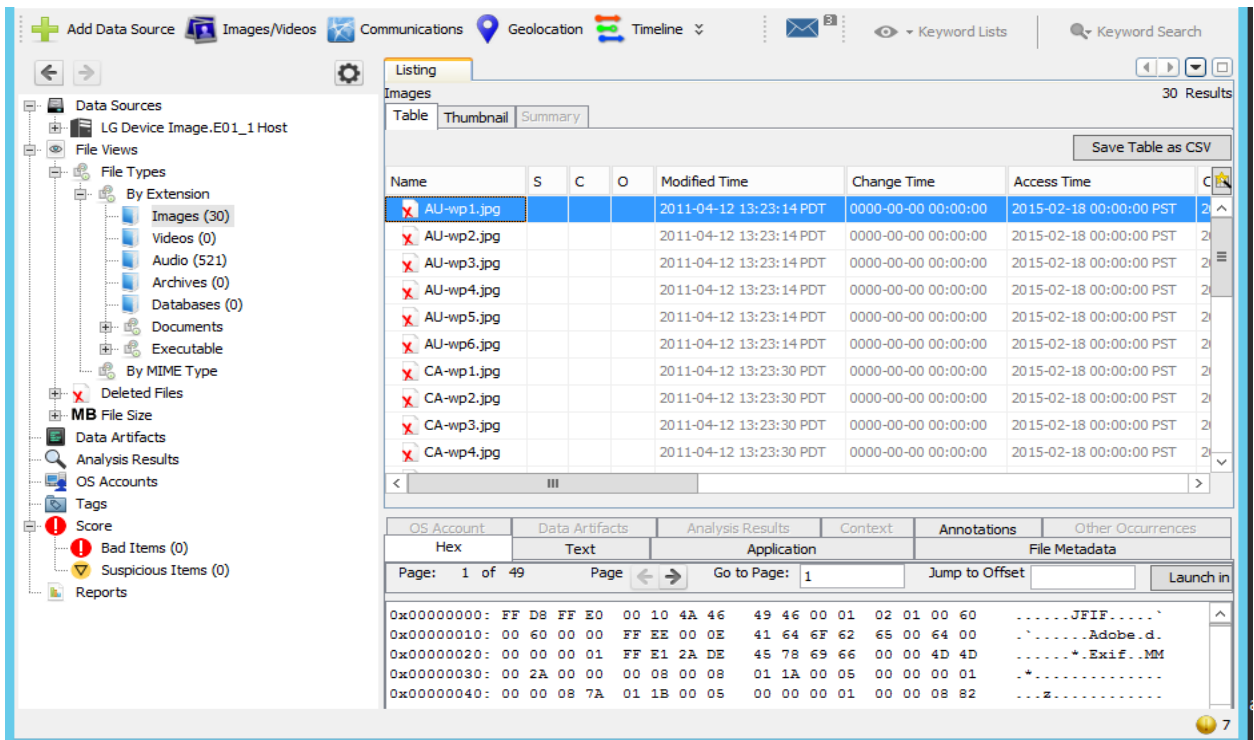
- Autopsy will analyze the files in the image file and a data source wizard appears as shown below, click on “Finish”.



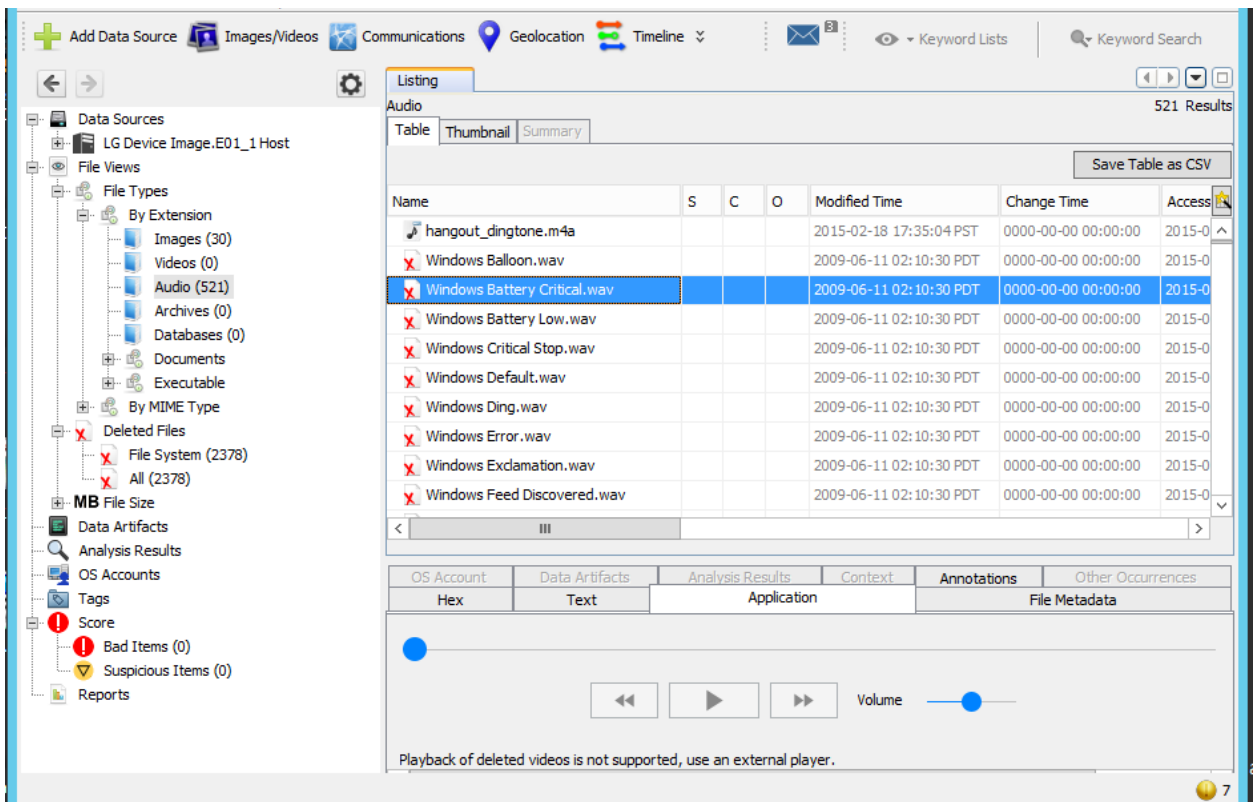
- The below appears, wait until autopsy completes analyzing the image file. observe the status at the lower right corner of the autopsy window.



- 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.

The screenshot shows the Autopsy software interface. On the left pane, under 'Data Sources', 'File Views', and 'Deleted Files', the 'All (2378)' view is selected. The main pane displays a table of deleted files. The first file, '1424261109999', is highlighted. Below the table, the 'File Metadata' tab is active, showing details for the selected file.

Name	S	C	O	Modified Time	Change Time	Access Time
1424261109999				2015-02-18 17:35:10 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache-201828170.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache109770822.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache585536646.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache-27967639.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache848258848.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache1910165812.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache-1648484034.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
DiskCache1074722708.tmp				2015-02-18 17:36:14 PST	0000-00-00 00:00:00	2015-02-18 00:00:00
smaller.fon				2009-06-11 02:14:06 PDT	0000-00-00 00:00:00	2015-02-18 00:00:00

Metadata

Name: /img_LG Device Image.E01/Android/data/com.android.providers.media/albumthumbs/1424261109999
Type: File System
MIME Type: application/octet-stream
Size: 0
File Name Allocation: Unallocated
Metadata Allocation: Unallocated

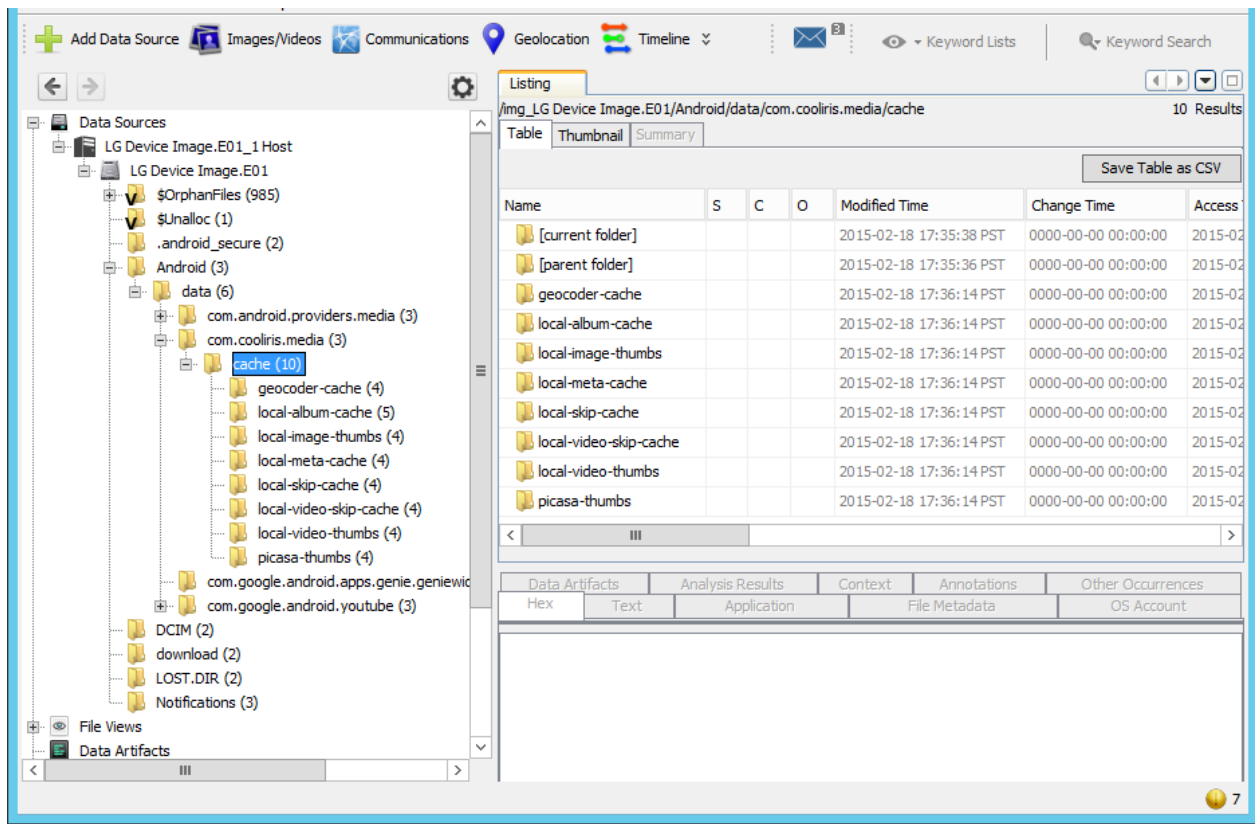
- Autopsy classifies files based on sizes in three sections as shown in the below screenshot.

The screenshot shows a forensic analysis tool interface. On the left is a sidebar with a tree view containing categories like 'Data Sources', 'File Views', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', 'Bad Items (0)', 'Suspicious Items (0)', and 'Reports'. The 'Data Sources' section is expanded, showing 'LG Device Image.E01_1 Host'. Under 'File Views', 'By Extension' and 'By MIME Type' are visible. The 'MB File Size' section shows a list of file sizes: 'MB 50 - 200MB (5)', 'MB 200MB - 1GB (3)', and 'MB 1GB+ (1)'. The 'By Extension' view is selected, showing a list of files with their names, sizes, and modification times. The main pane displays a table of files. The first file is 'l2057.ngr' with a size of 50 - 200MB. Below the table is a hex view of the selected file, showing the first 100 bytes of the file in hexadecimal and ASCII.

Name	S	C	O	Modified Time	Change Time	Access Time	Created
l2057.ngr				2011-04-12 13:14:54 PDT	0000-00-00 00:00:00	2015-02-18 00:00:00 PST	2015-02-18 00:00:00 PST
111111~1.SNO				2011-04-05 17:11:52 PDT	0000-00-00 00:00:00	2015-02-18 00:00:00 PST	2015-02-18 00:00:00 PST
PINTLGT.IMG				2009-06-11 02:32:18 PDT	0000-00-00 00:00:00	2015-02-18 00:00:00 PST	2015-02-18 00:00:00 PST
_HAKIR~1.MP4				2011-09-23 17:09:00 PDT	0000-00-00 00:00:00	2015-02-18 00:00:00 PST	2015-02-18 00:00:00 PST
JANETD~1.FLV				2011-09-23 16:40:44 PDT	0000-00-00 00:00:00	2015-02-18 00:00:00 PST	2015-02-18 00:00:00 PST

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
0x00000000:	53 0B CE FE 6B DD 31 7F	10 47 84 9B F9 D2 01 00	S...k.1..G.....						
0x00000010:	C7 EB 71 00 84 54 08 00	53 84 54 00 FF FF FF FF	..q..T..S.T.....						
0x00000020:	00 00 00 00 00 00 00 00	00 00 00 00 E7 06 01 00						
0x00000030:	00 26 2D 00 BE BB 01 00	00 84 80 00 82 82 02 00	..6-.....						
0x00000040:	00 23 A8 00 ED 3B 03 00	02 8B D0 00 F9 D5 03 00	..\$.....						
0x00000050:	00 8D F2 00 4C 80 04 00	03 5F 43 01 36 25 05 00L.....C.64..						

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



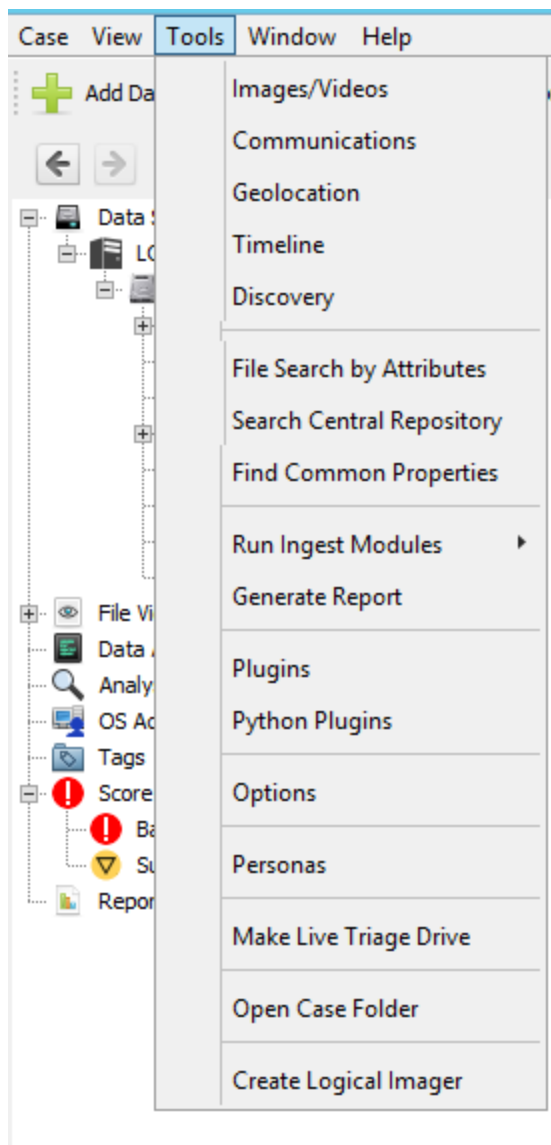
- Autopsy displays directory named OrphanFiles that contain broken files as shown below.

The screenshot displays a forensic analysis tool interface. On the left, a tree view shows the data sources, including 'LG Device Image.E01' and its subfolders like '\$OrphanFiles (985)', '\$Unalloc (1)', '.android_secure (2)', 'Android (3)', 'DCIM (2)', 'download (2)', 'LOST.DIR (2)', and 'Notifications (3)'. The main pane shows a 'Listing' of files under the path '/img_LG Device Image.E01/\$OrphanFiles'. The listing table has columns for Name, S, C, O, Modified Time, Change Time, and Access Time. Below the listing, there is a 'Hex' view showing memory addresses and their corresponding hexadecimal and ASCII representations.

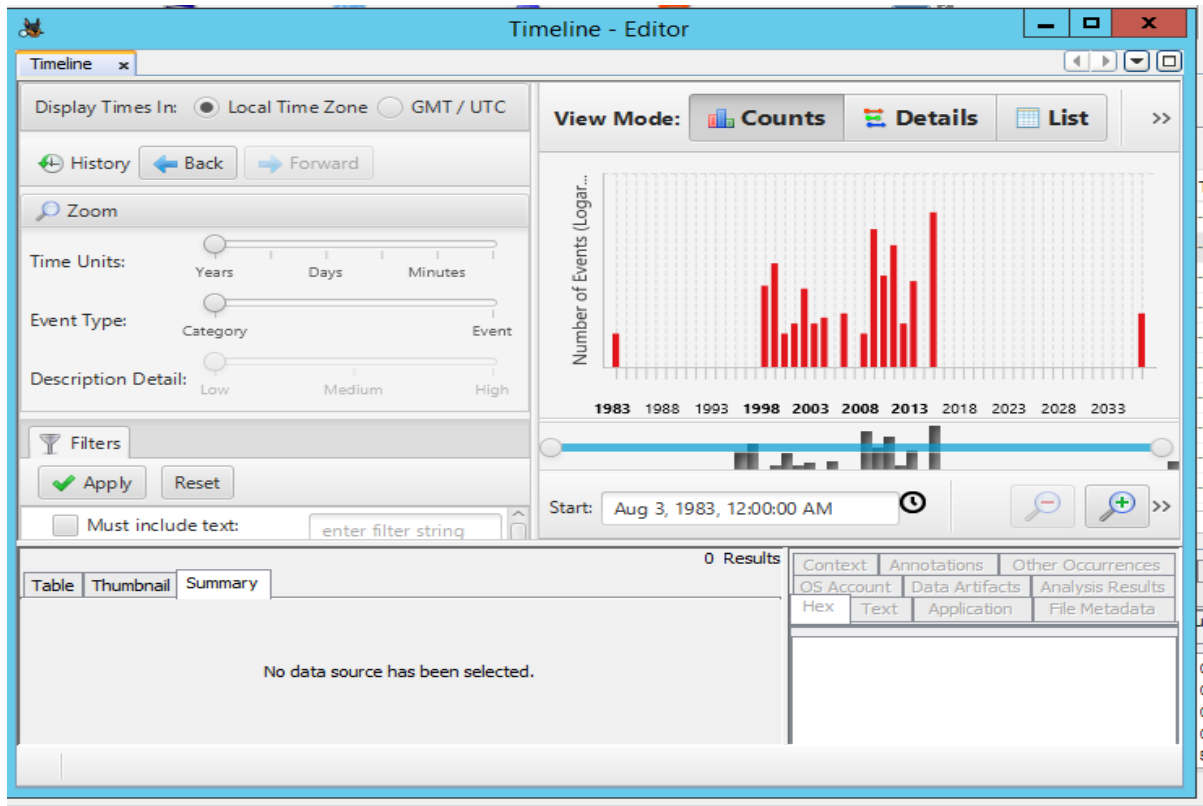
Name	S	C	O	Modified Time	Change Time	Access Time
aparaji.ttf				2010-11-21 08:56:54 PST	0000-00-00 00:00:00	2015-02-1
app775.fon				2009-06-11 02:13:14 PDT	0000-00-00 00:00:00	2015-02-1
app850.fon				2009-06-11 02:13:14 PDT	0000-00-00 00:00:00	2015-02-1
app852.fon				2009-06-11 02:13:14 PDT	0000-00-00 00:00:00	2015-02-1
app855.fon				2009-06-11 02:13:14 PDT	0000-00-00 00:00:00	2015-02-1
app857.fon				2009-06-11 02:13:14 PDT	0000-00-00 00:00:00	2015-02-1
app866.fon				2009-06-11 02:13:14 PDT	0000-00-00 00:00:00	2015-02-1
app932.fon				2009-06-11 02:13:48 PDT	0000-00-00 00:00:00	2015-02-1
app936.fon				2009-06-11 02:13:16 PDT	0000-00-00 00:00:00	2015-02-1
app949.fon				2009-06-11 02:13:52 PDT	0000-00-00 00:00:00	2015-02-1

Hex	Text	Application	File Metadata	OS Account
0x00000000: 5D AC D4 E9 19 05 FD C5 F9 09 8A 0A 76 3B 77 75	J.....			
0x00000010: 95 03 46 A9 D8 66 85 1D DE BF 85 2F EB EF 60 6B	..F..f...			
0x00000020: 4F D0 96 9A 5E 83 15 58 8F 54 07 FB 3E 53 26 03	O...^..X..			
0x00000030: 17 F3 04 B2 9B 6C 4B 01 92 50 81 30 99 68 C1 D5lK..			
0x00000040: CF 69 A2 3D E6 A1 12 B9 29 9C 0D 03 C9 5B 06 E3	..i.=.....			

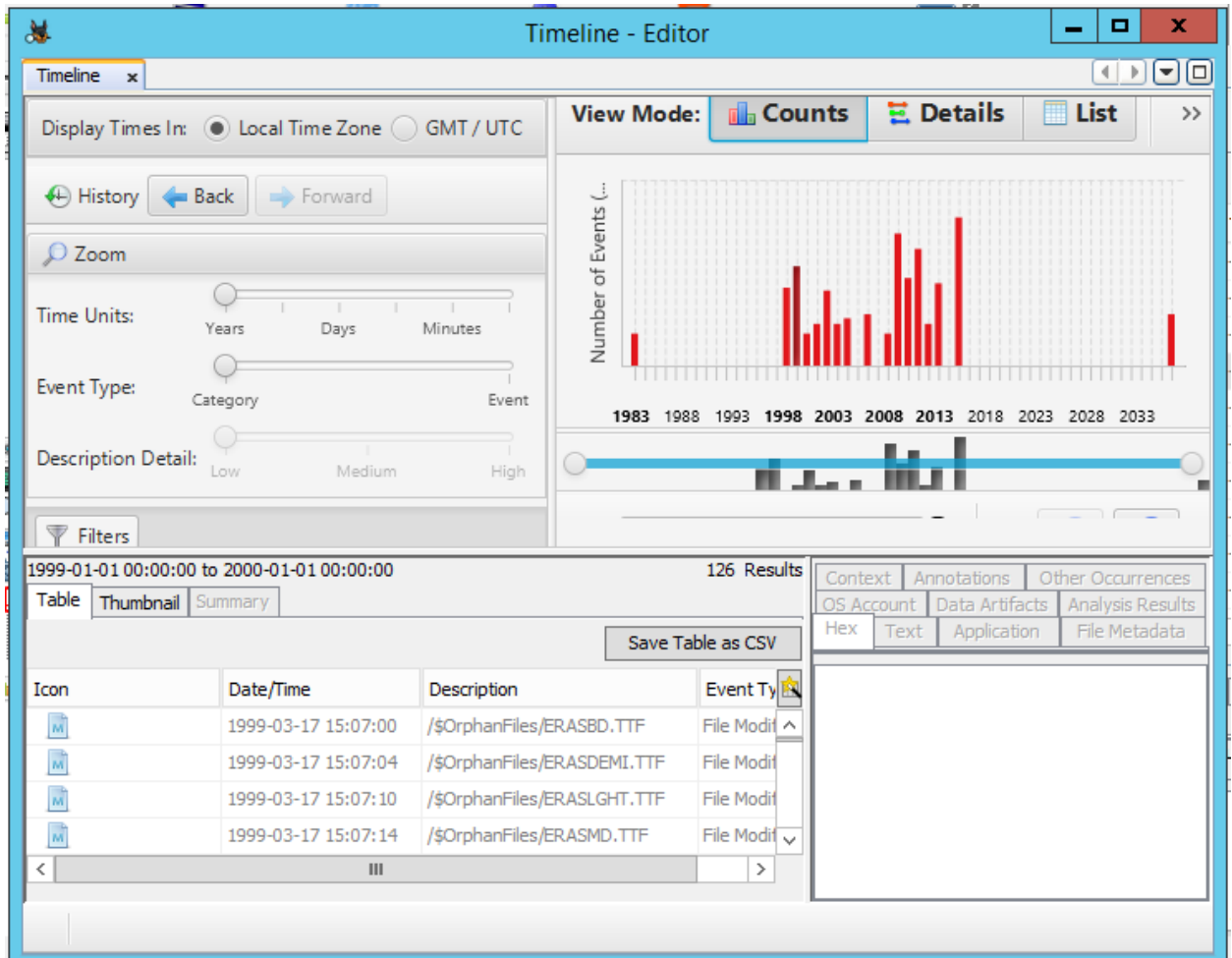
- Timeline helps to determine filesystem events on the device during a selected period.



- The red color bars represent filesystem activities.

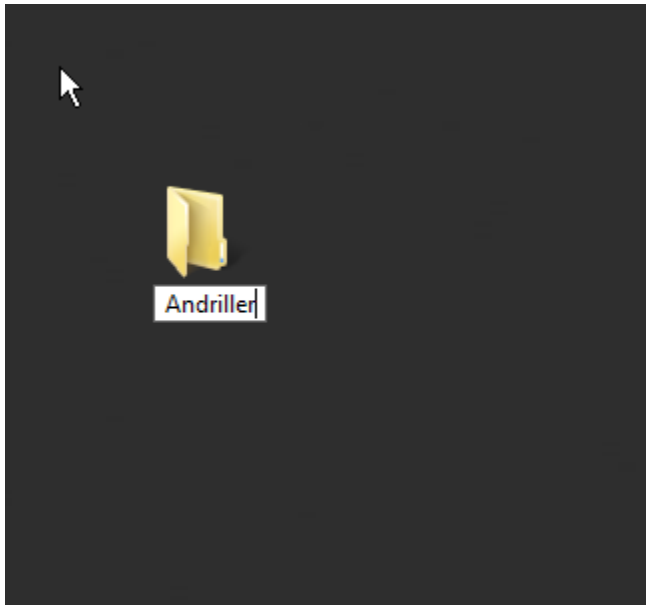


- Choose a time interval and select a bar from the graph autopsy displays all the filesystem events that occurred during the time interval associated with the selected bar.

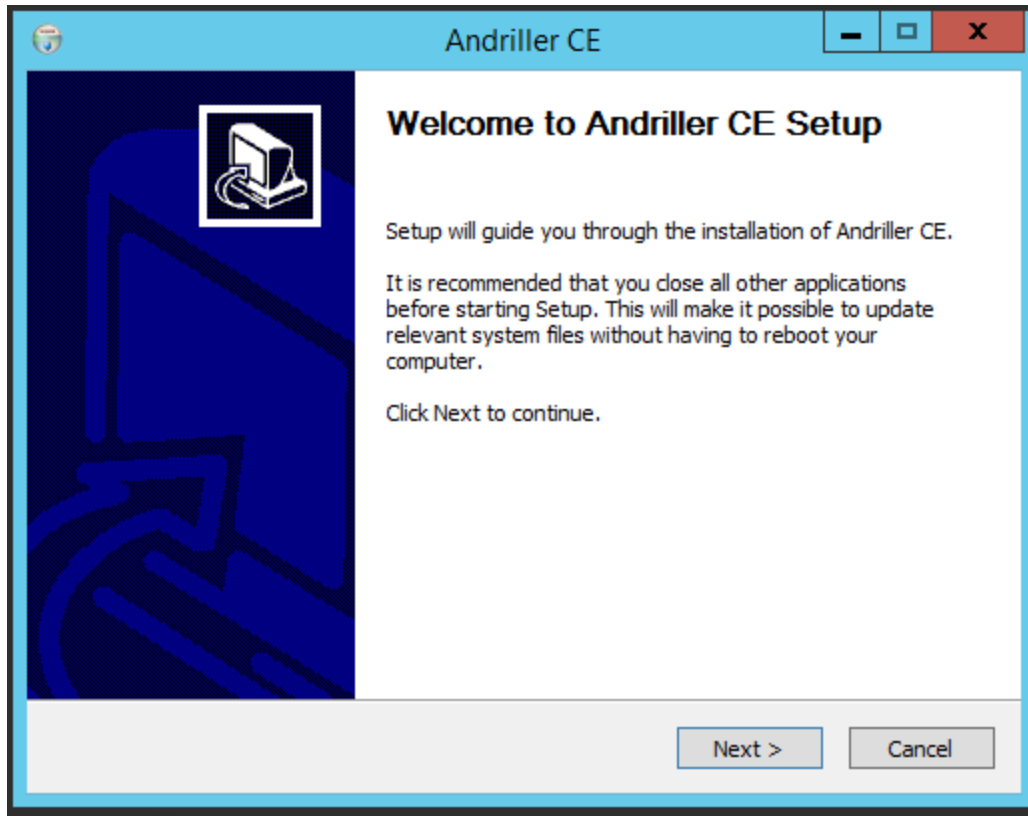


LAB 2: ANALYZING AN ANDROID DEVICE USING ANDRILLER

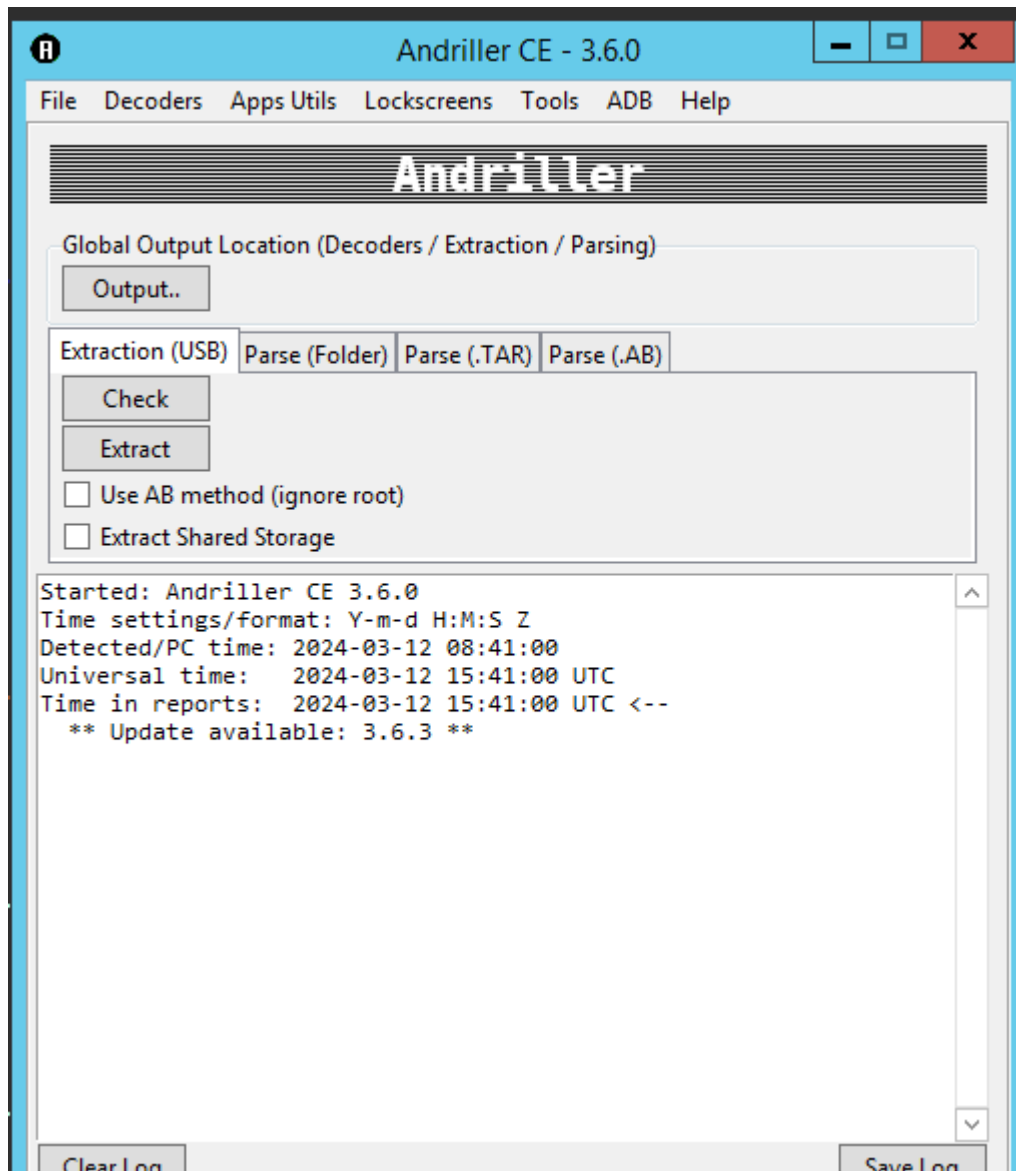
- Log on to window server 2012 virtual machine and create a folder named Andriller on the Desktop.



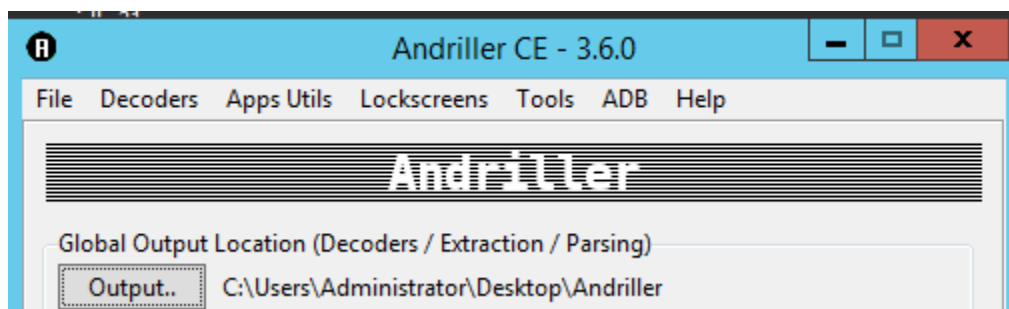
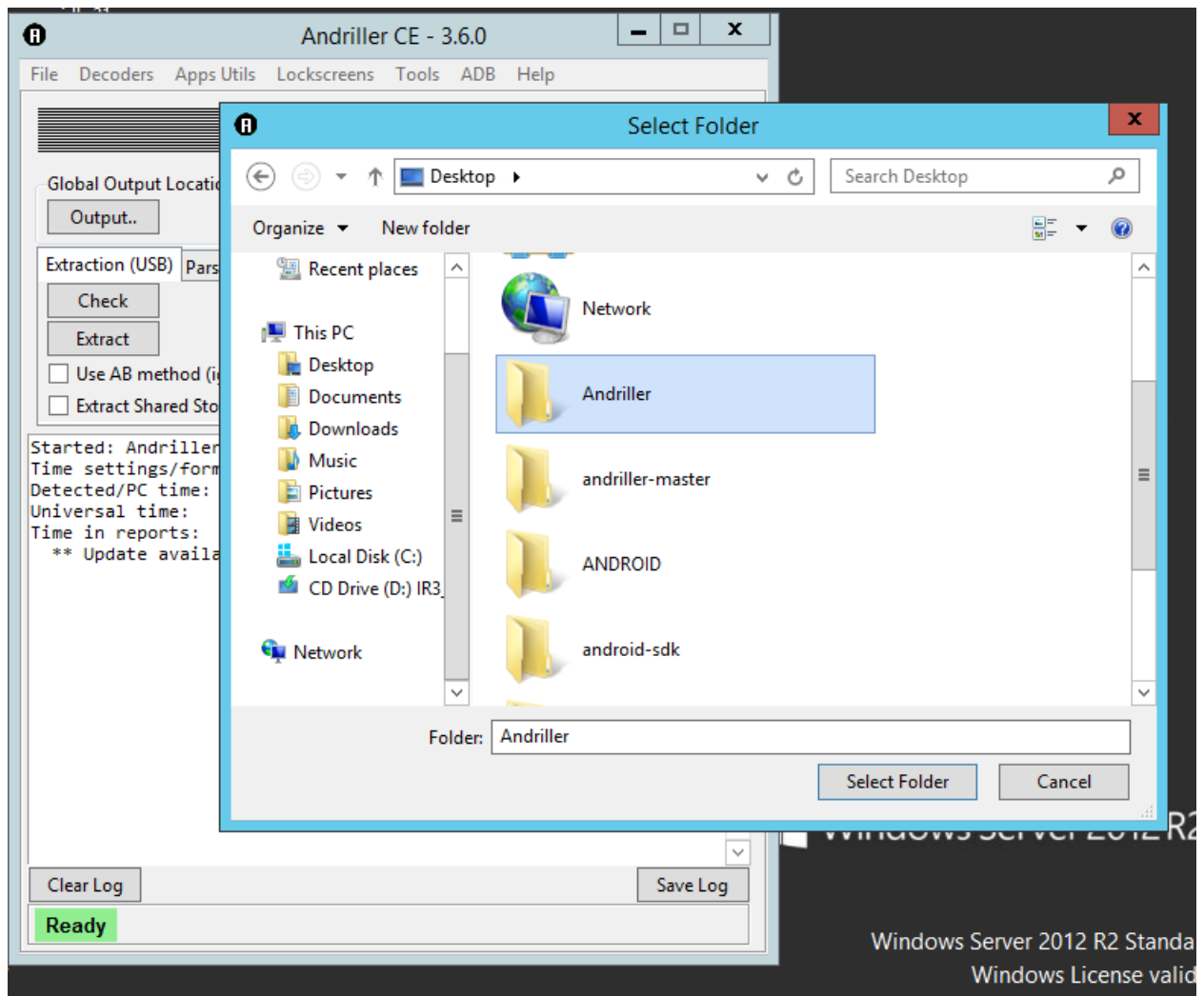
- Double the Andriller exe file and follow the wizard.



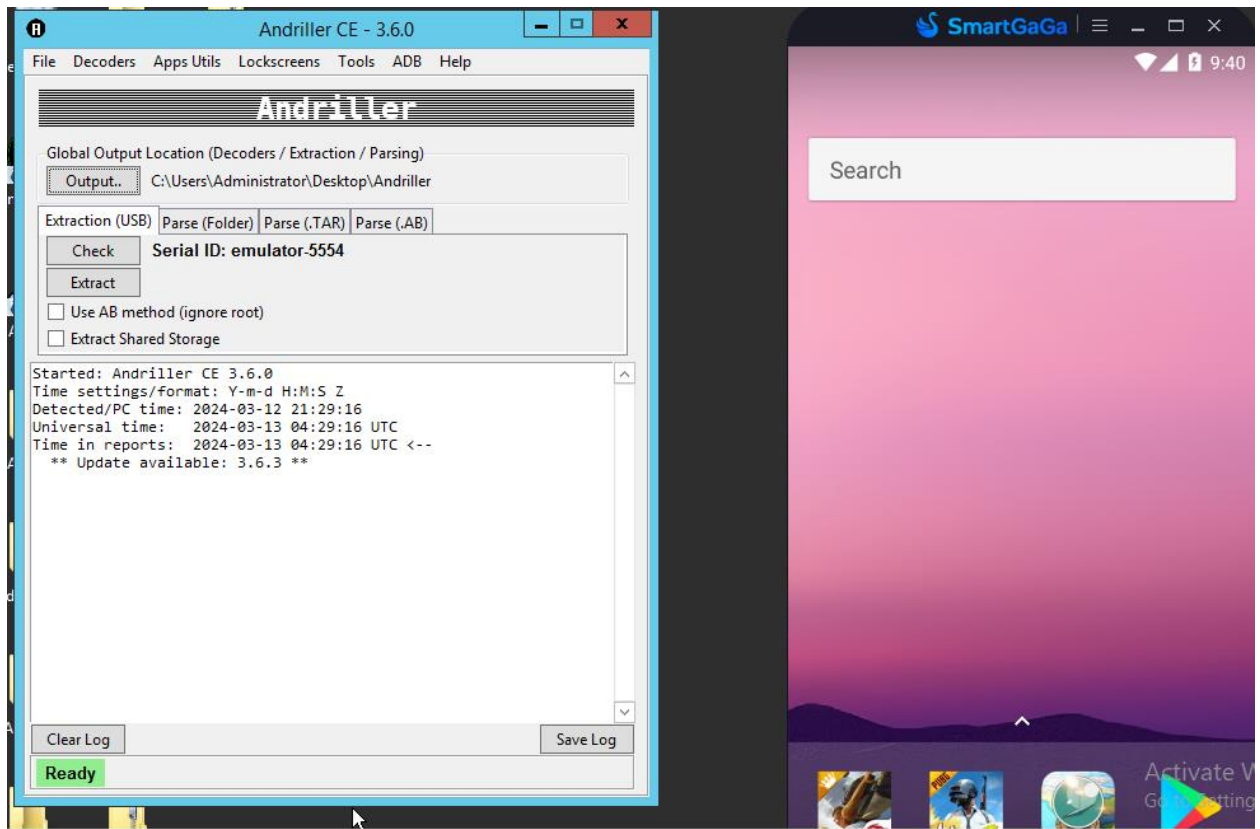
- Andriller main window appears as shown in the screenshot below.



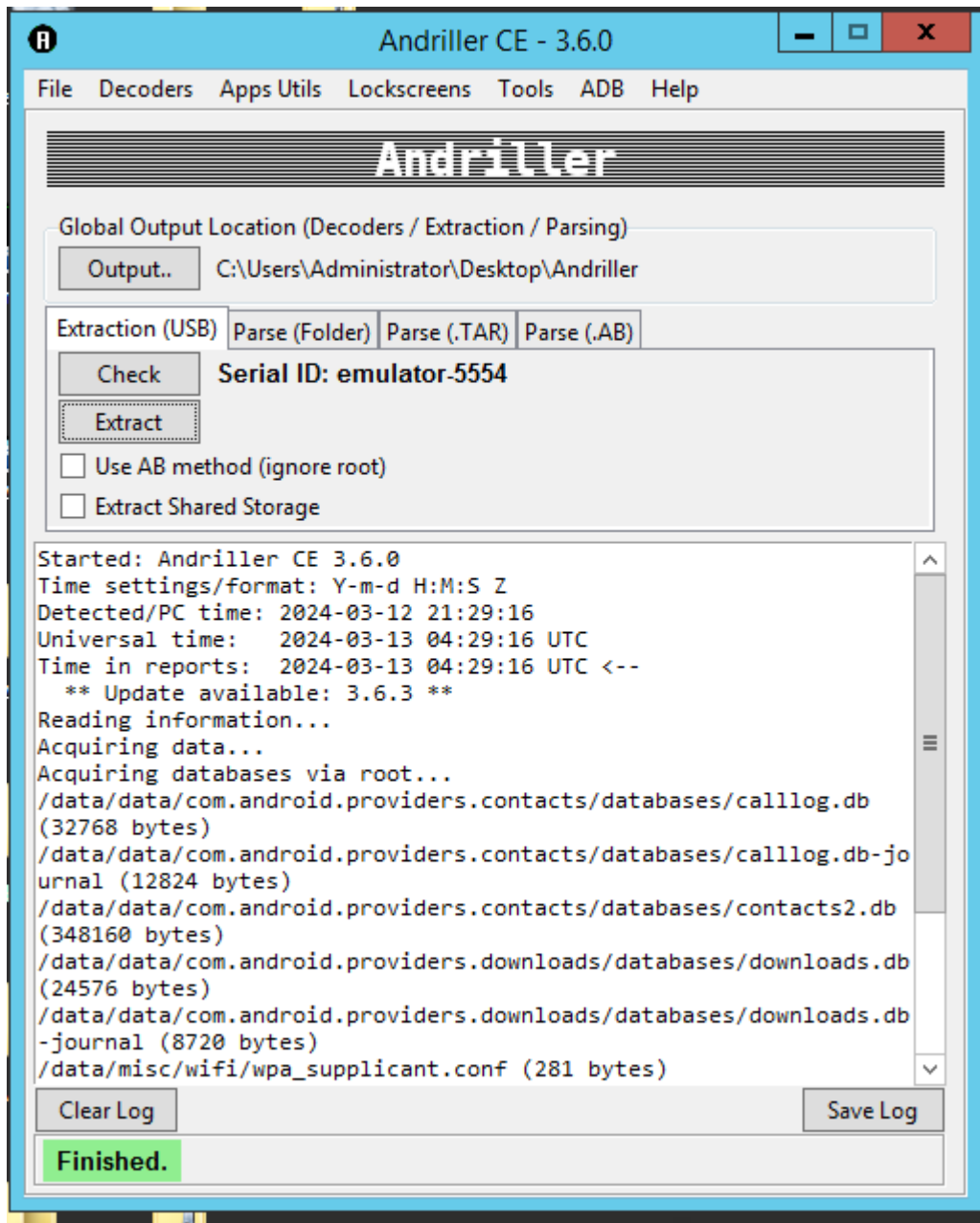
- To specify output location to store all the logs and data for andriller, click the “output” in the andriller window and navigate to Desktop and select the Andriller folder which we created earlier as shown on the screenshot below and click on select folder.



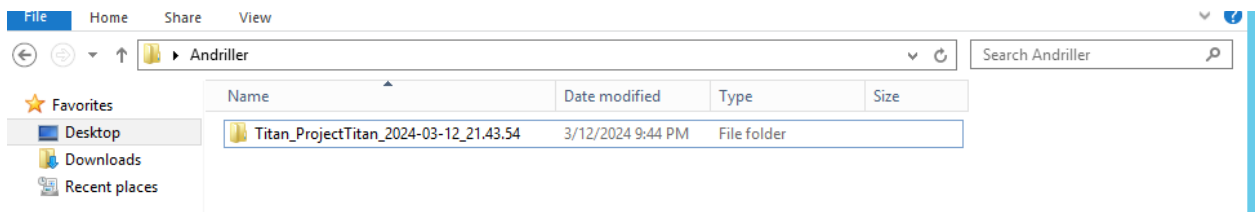
- Next, we click on “check” to see if android emulator is connected to andriller. The serial id of the emulator displayed as shown below rendering a success in the connection between andriller and the android emulator.



- 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.

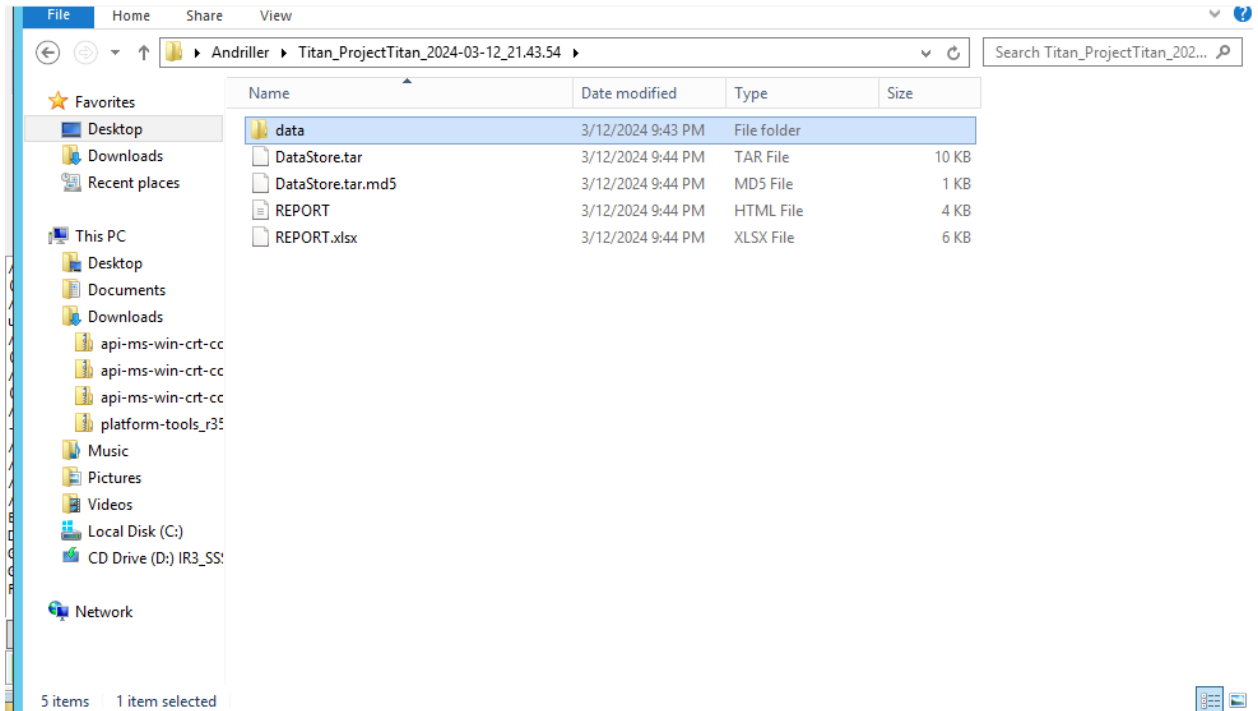


- Andriller creates a directory inside the Andriller folder with the name of the device followed by the timestamp as shown below.



- Navigate to the Andriiller 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

dli...

File | C:/Users/Administrator/Desktop/An... A

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
Permission	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)