Autopsy Guided Exercise

Video walkthrough available on the Tool Walkthrough Playlist at https://youtube.com/@hexordia

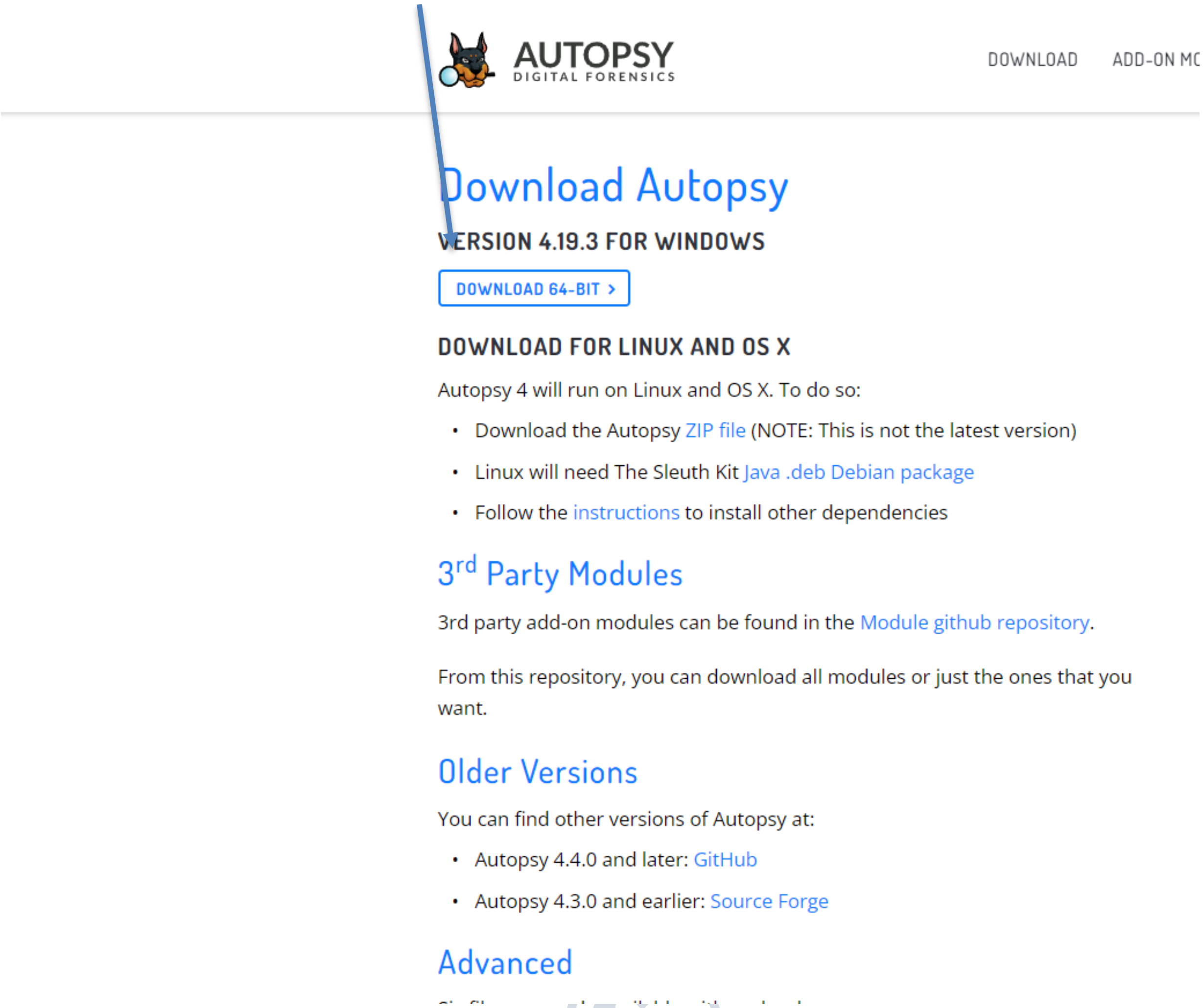
To get started, please download Autopsy from https://www.autopsy.com/download

Prior to installation, verify the hash value to the known good from the syllabus for students enrolled in the HMFA Virtual Live course. The MD5 hash value for the 64-bit 4.19.3 version is 1e49be55c6c5c568ad1a5a7ffdbb410c Please note, Windows Defender may flag this file, if the hash matches, you should be good to proceed and install using the Autopsy Setup Wizard.

**If you already have Autopsy Installed, please move on to Set Up and Use.

Installation

For the purposes of this course, DOWNLOAD 64-BIT will be utilized.



Download Autopsy

VERSION 4.19.3 FOR WINDOWS

DOWNLOAD FOR LINUX AND OS X

Autopsy 4 will run on Linux and OS X. To do so:

- Download the Autopsy ZIP file (NOTE: This is not the latest version)
- Linux will need The Sleuth Kit Java .deb Debian package
- Follow the instructions to install other dependencies

3rd Party Modules

3rd party add-on modules can be found in the Module github repository.

From this repository, you can download all modules or just the ones that you want.

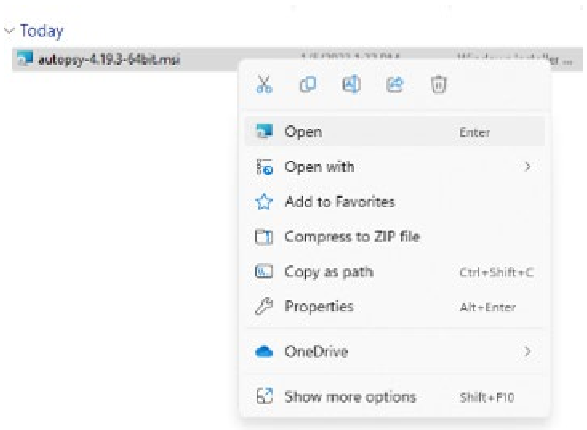
Older Versions

You can find other versions of Autopsy at:

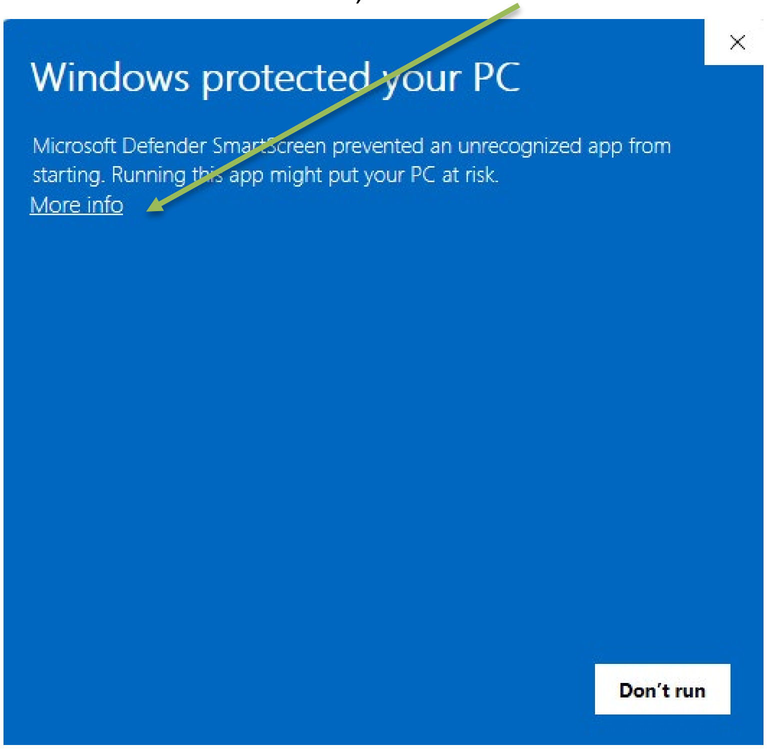
- Autopsy 4.4.0 and later: GitHub
- Autopsy 4.3.0 and earlier: Source Forge

Advanced

Double click the downloaded file or right click and select “Open.”

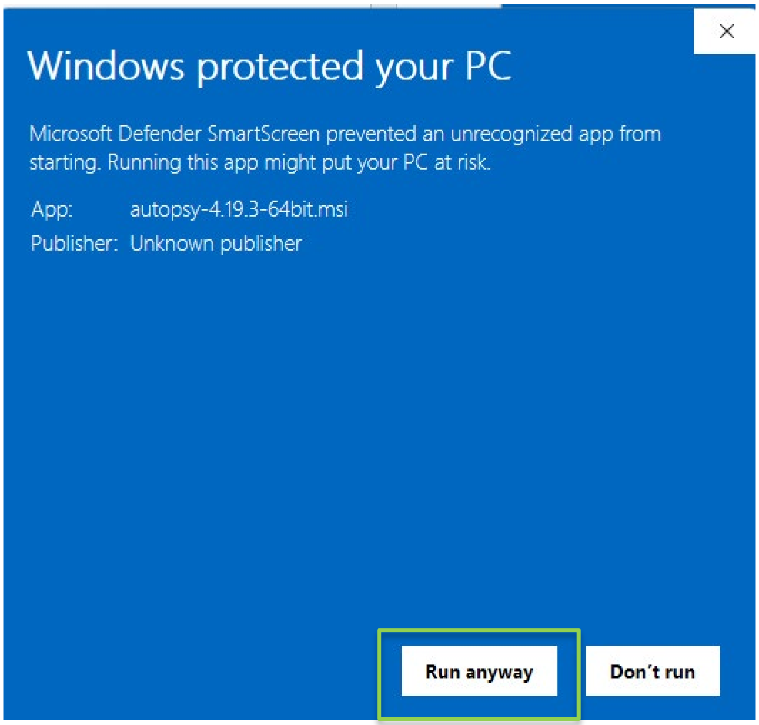


Windows Defender, select “More Info” and select “run anyway.”



Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.



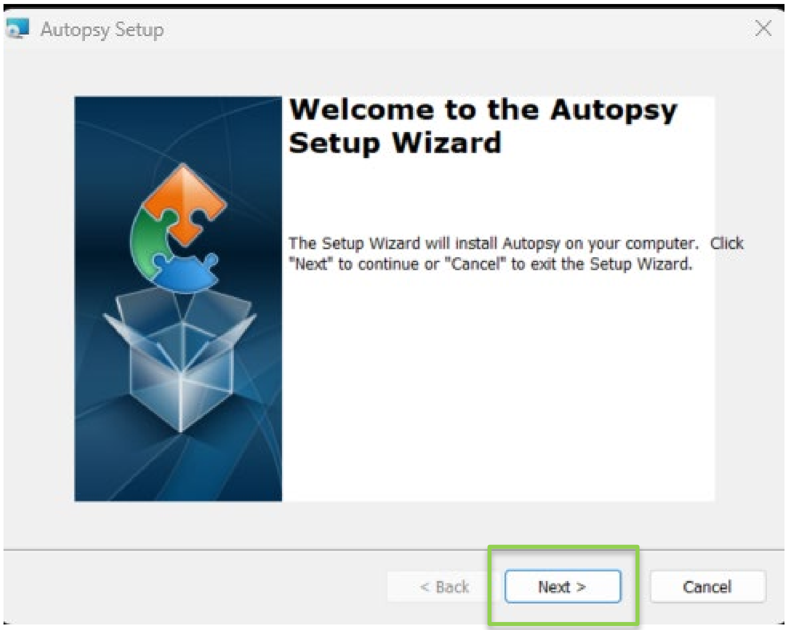
Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: autopsy-4.19.3-64bit.msi

Publisher: Unknown publisher

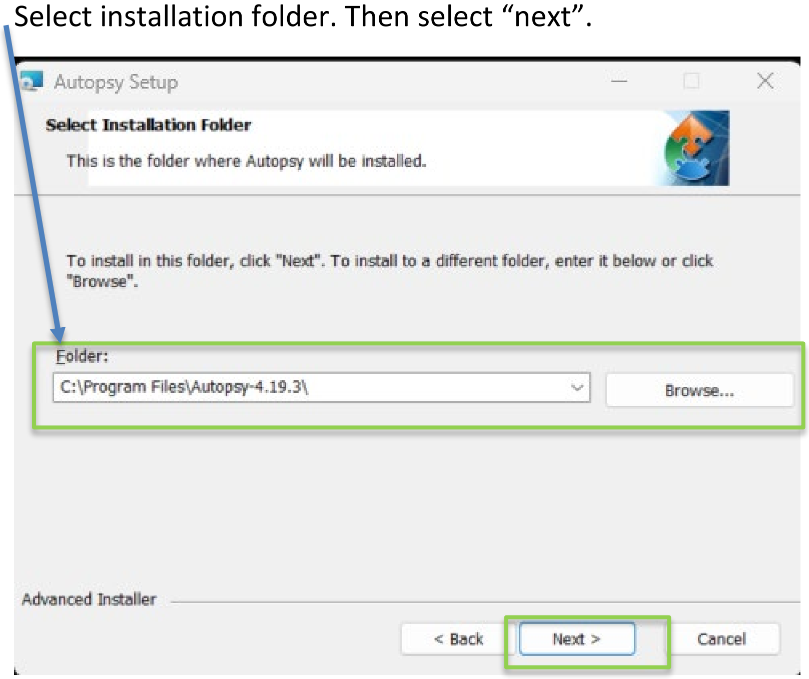
Select “next”.



Welcome to the Autopsy Setup Wizard

The Setup Wizard will install Autopsy on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Select installation folder. Then select “next”.



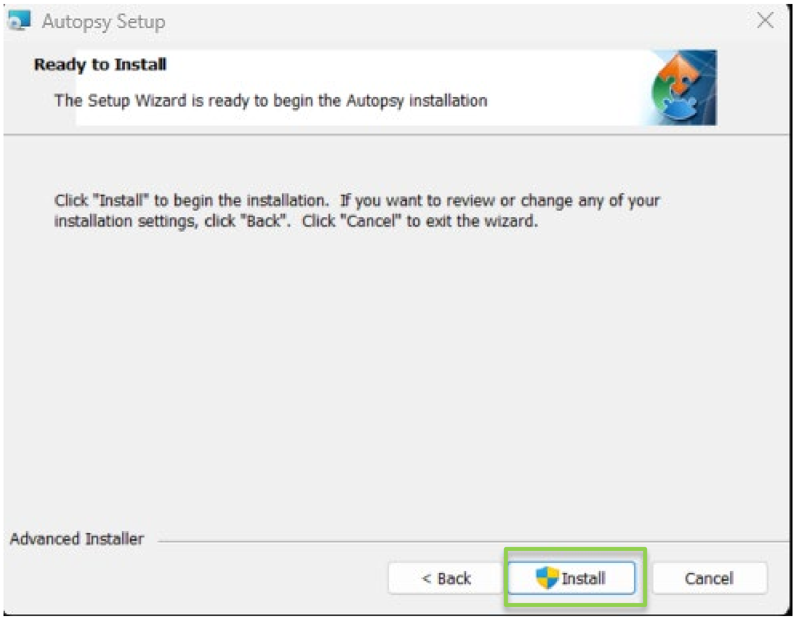
Select Installation Folder

This is the folder where Autopsy will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

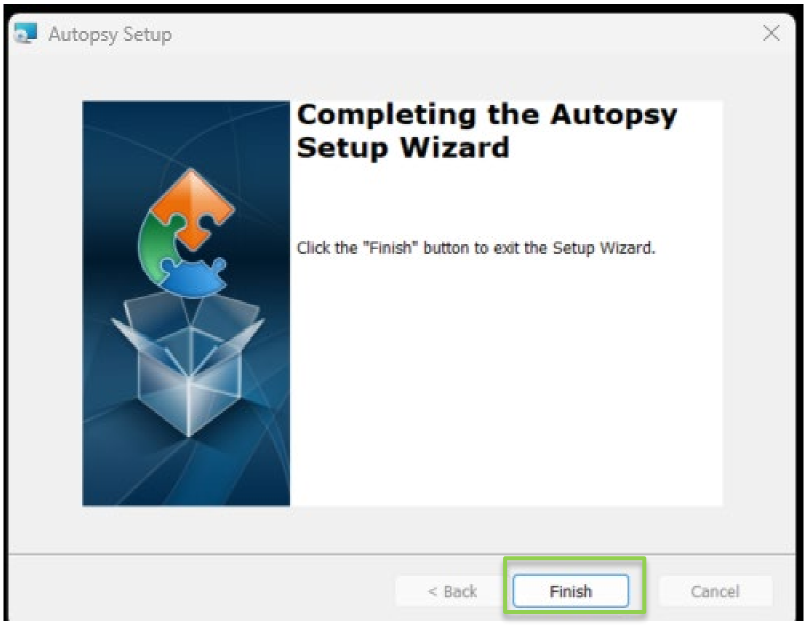
Folder: C:\Program Files\Autopsy-4.19.3\

Next select “Install.” If a pop-up occurs for User Controls, follow prompts. If “no” is selected, installation will stop. If “yes” is selected installation will continue.



Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

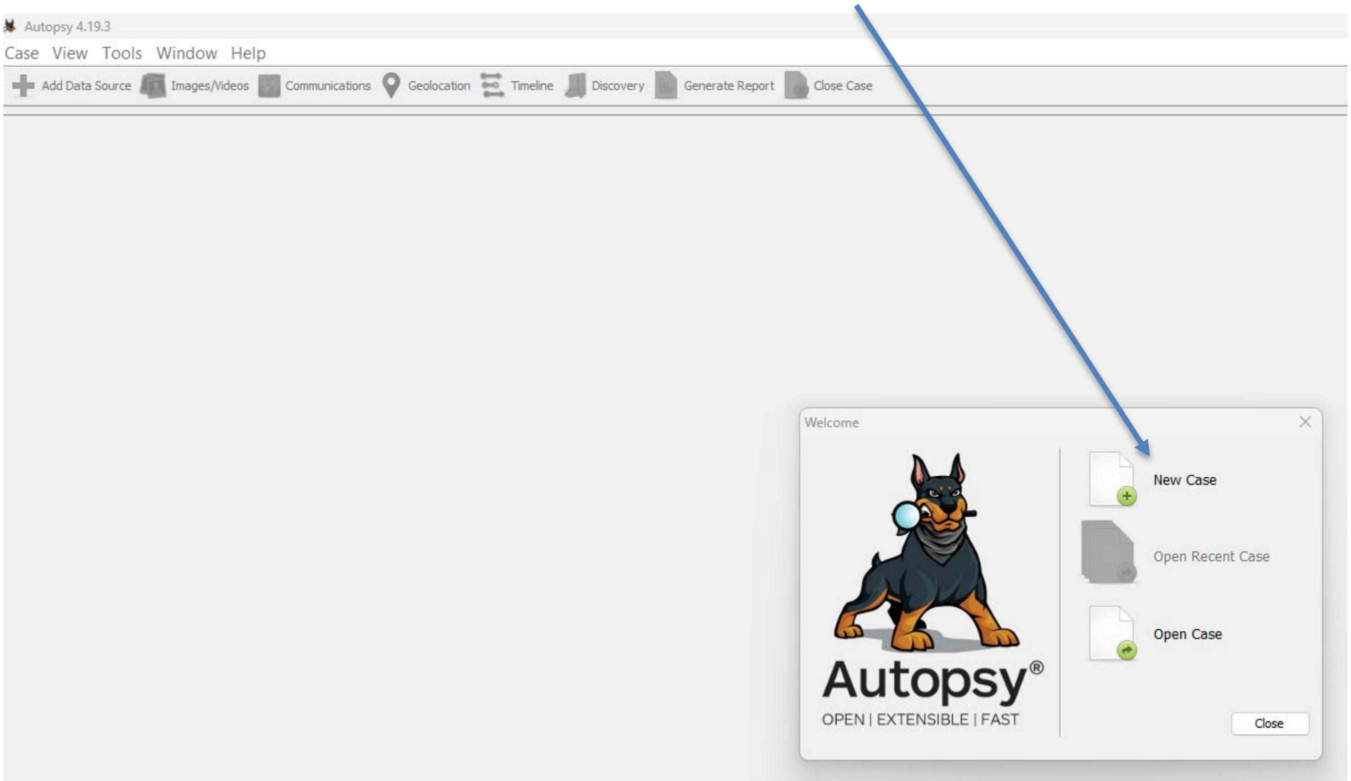
Select “Finish”.



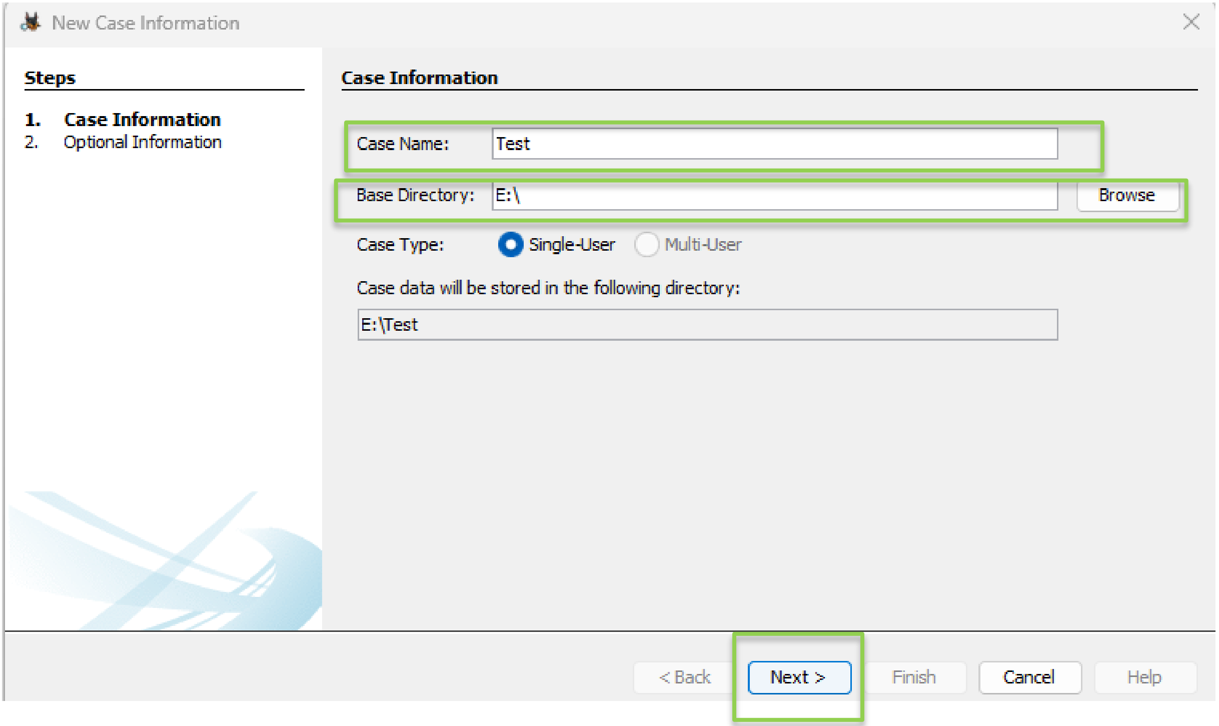
Click the "Finish" button to exit the Setup Wizard.

Set Up and Use

Once Autopsy is installed, Launch the application, and select “New Case”.



Enter a case name and select an output directory (base directory). Use “Single-User” for the Case Type. Select “Next”.



Case Name: Test

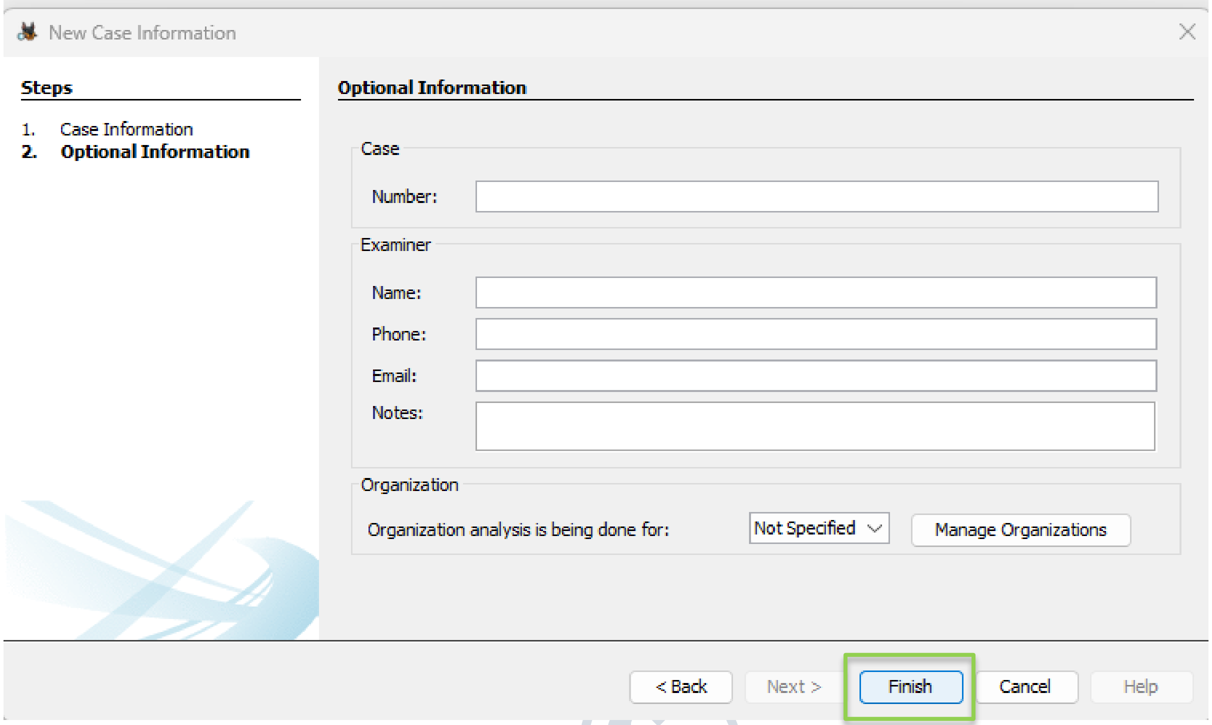
Base Directory: E:\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

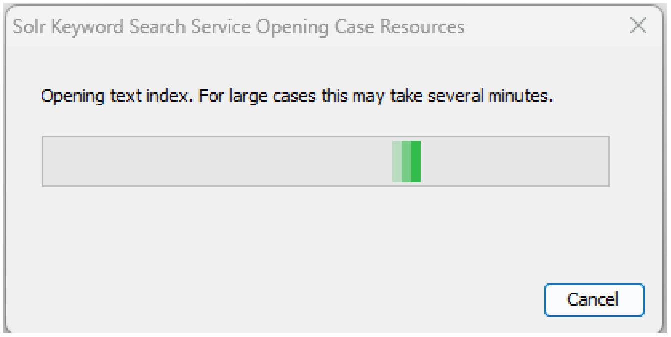
E:\Test

The next screen allows for the input of optional case. Select “Finish”.



Organization analysis is being done for: Not Specified

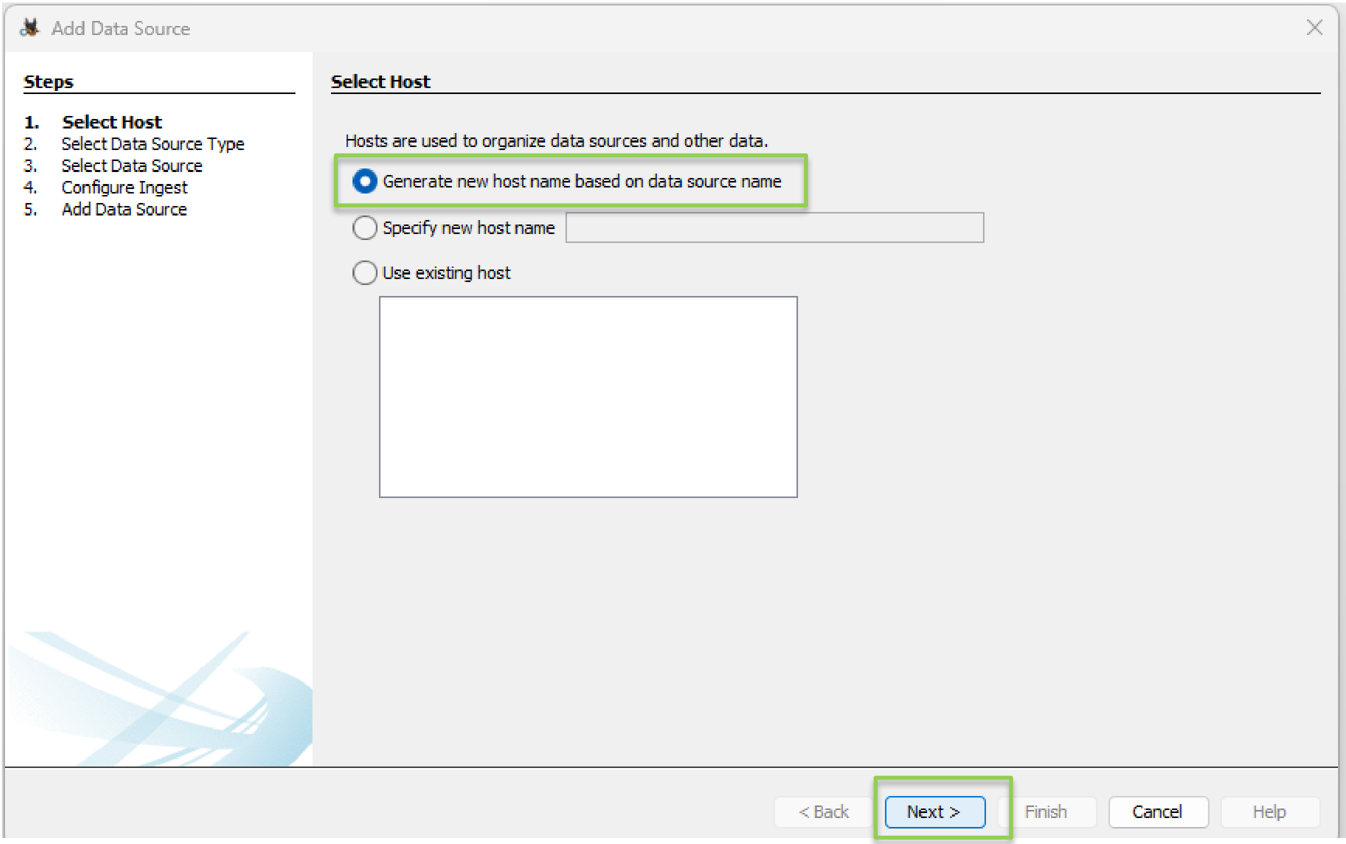
This next phase may take a bit to create.



Solr Keyword Search Service Opening Case Resources

Opening text index. For large cases this may take several minutes.

On the Select Host screen, select "Generate new host name based on data source name and select "Next".



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

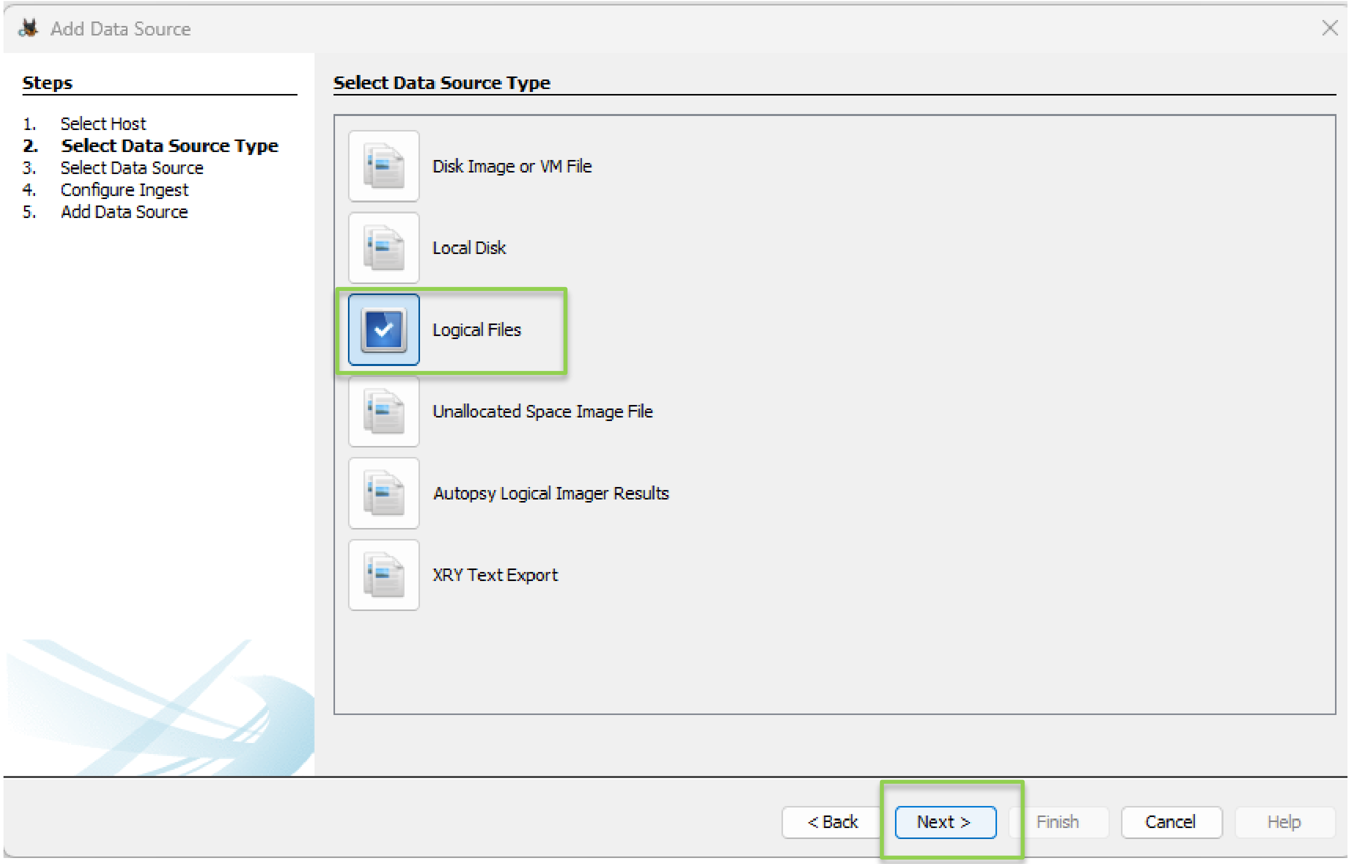
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

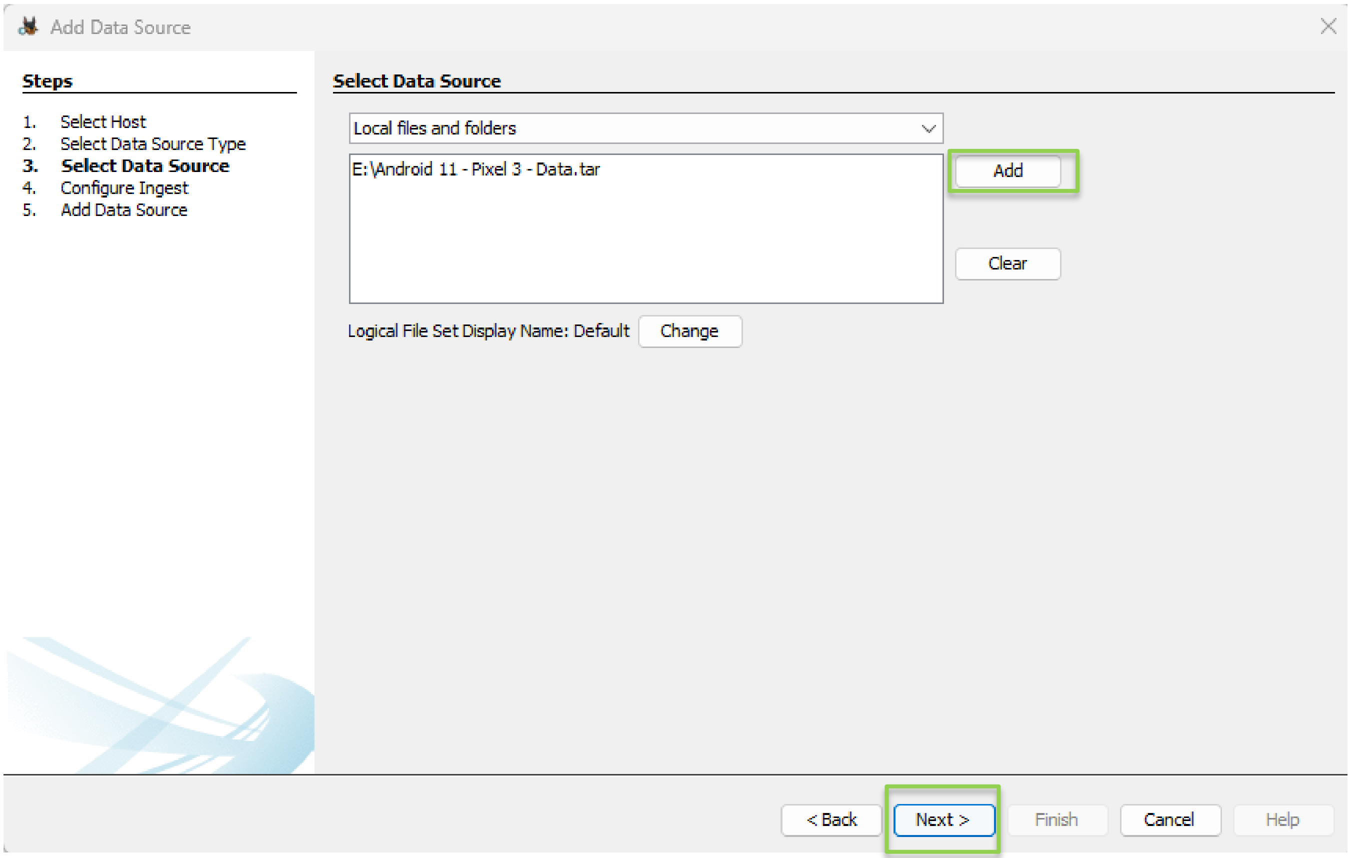
○ Specify new host name

○ Use existing host

The Data Source type will vary based on the image type. Android and iOS images should be loaded as logical files rather than as an image file. Select “Logical Files” and “Next”.



Select “Add” and navigate to the image file. In this instance we are loading a .tar of an Android image. Select “Next”.



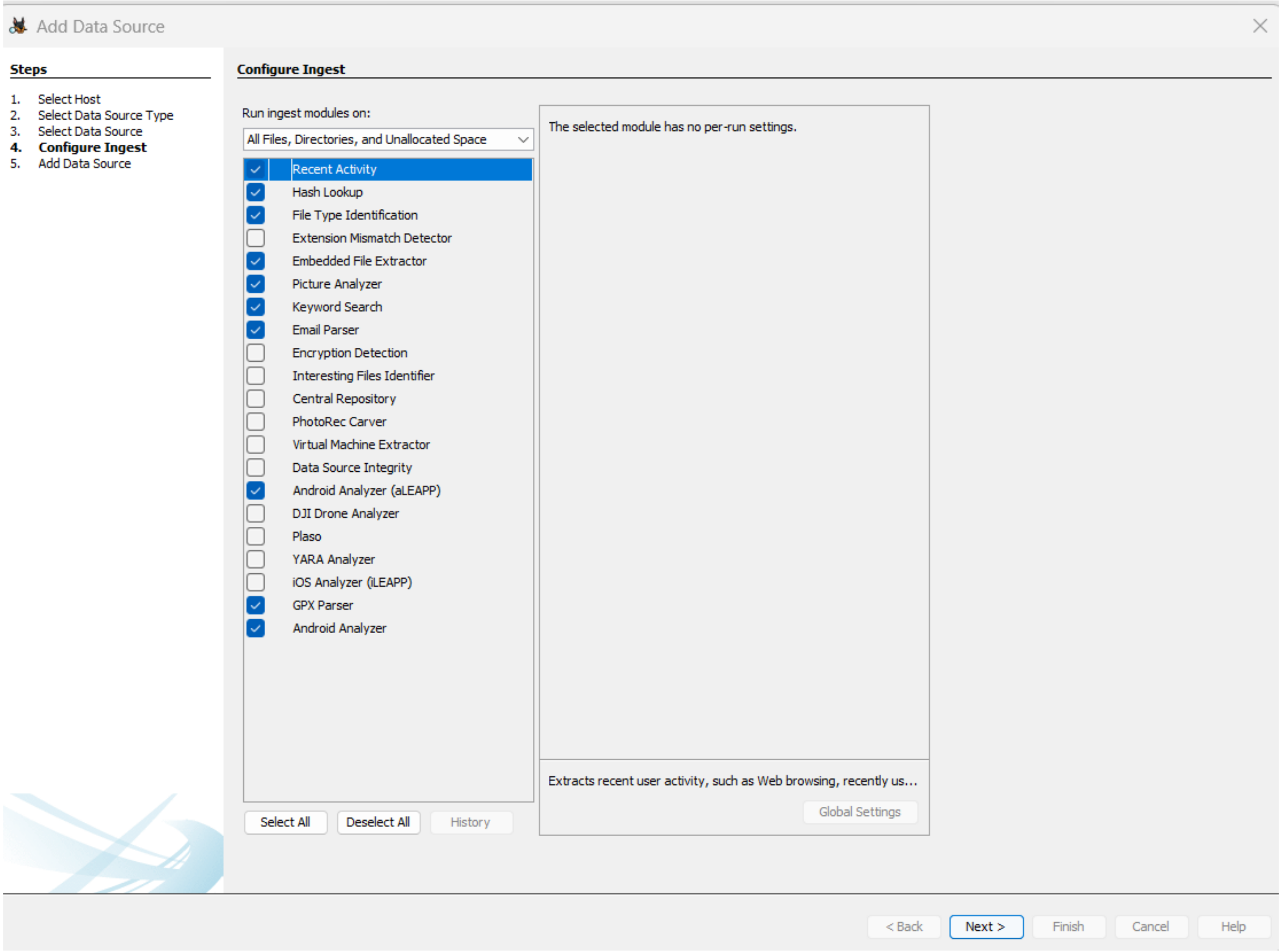
Local files and folders

E:\Android 11 - Pixel 3 - Data.tar

Logical File Set Display Name: Default

Here you will select your ingest options depending on the operating system. Once configured select "Next."

Android Image Selection example:



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

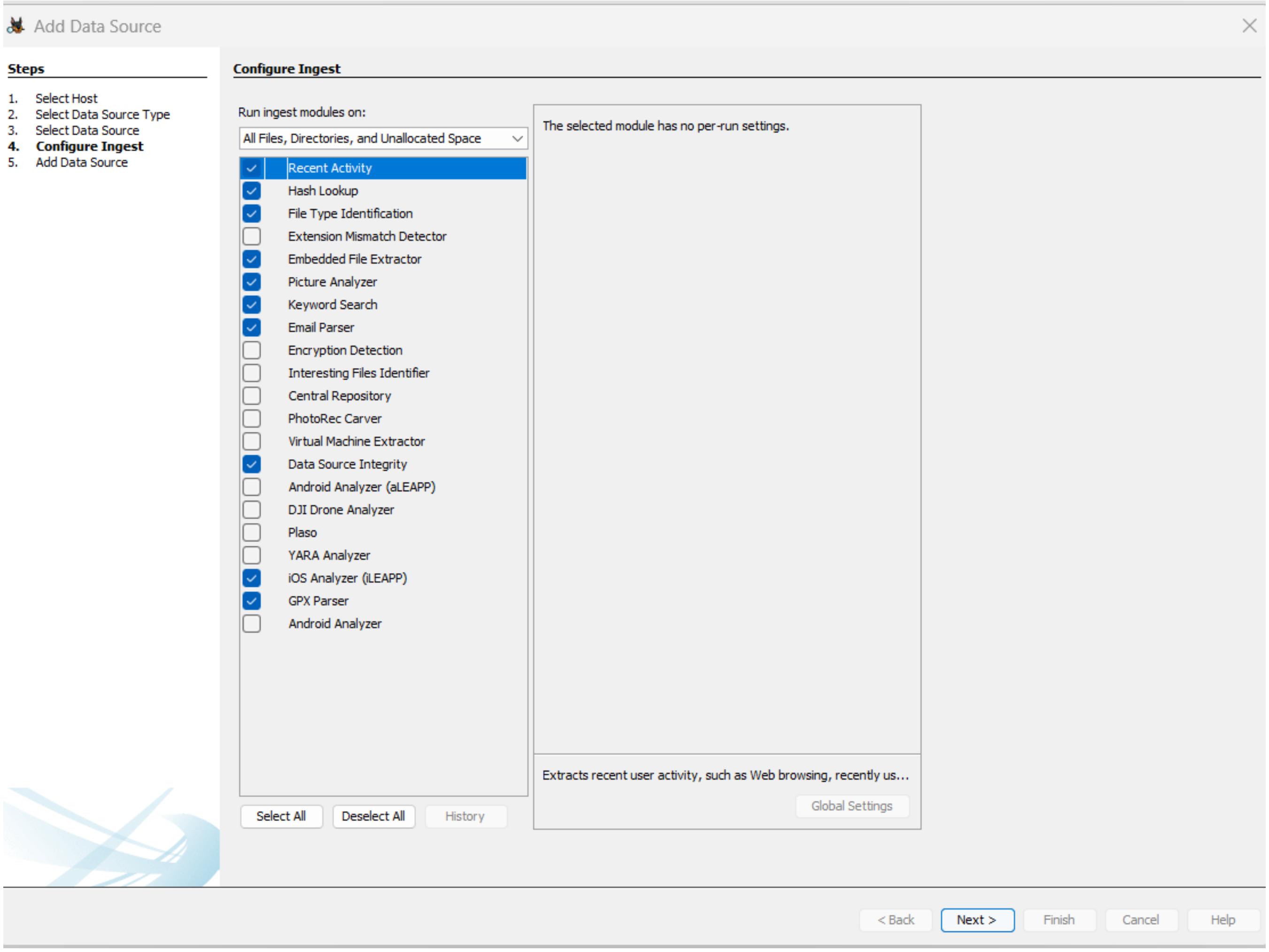
All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☐ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☐ Encryption Detection
- ☐ Interesting Files Identifier
- ☐ Central Repository
- ☐ PhotoRec Carver
- ☐ Virtual Machine Extractor
- ☐ Data Source Integrity
- ☑ Android Analyzer (aLEAPP)
- ☐ DJI Drone Analyzer
- ☐ Plaso
- ☐ YARA Analyzer
- ☐ iOS Analyzer (iLEAPP)
- ☑ GPX Parser
- ☑ Android Analyzer

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us…

iOS Image Selection example:



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

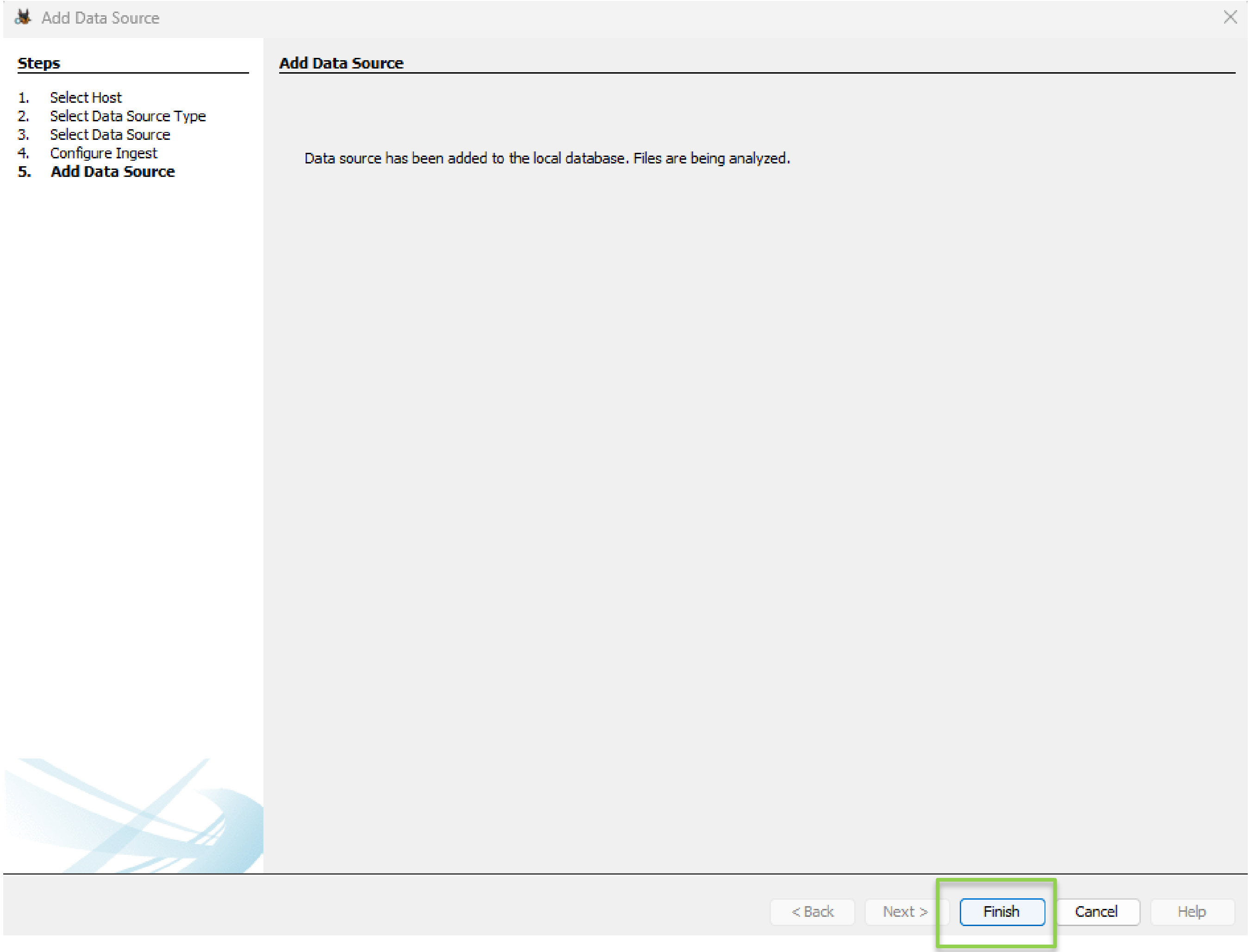
Run ingest modules on: All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☐ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☐ Encryption Detection
- ☐ Interesting Files Identifier
- ☐ Central Repository
- ☐ PhotoRec Carver
- ☐ Virtual Machine Extractor
- ☑ Data Source Integrity
- ☐ Android Analyzer (aLEAPP)
- ☐ DJI Drone Analyzer
- ☐ Plaso
- ☐ YARA Analyzer
- ☑ iOS Analyzer (iLEAPP)
- ☑ GPX Parser
- ☐ Android Analyzer

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Select “Finish”.



Add Data Source

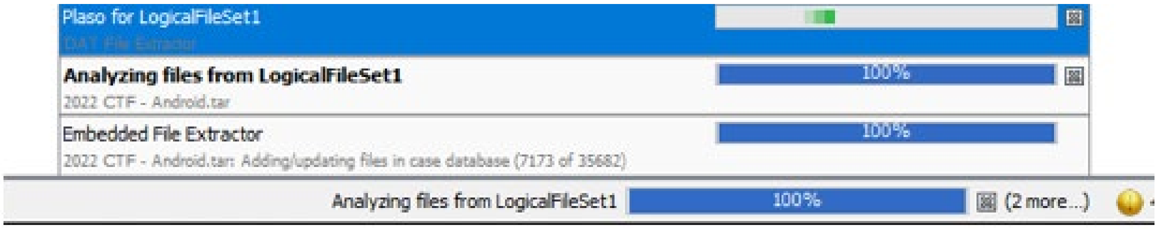
Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

The bottom right-hand corner of the screen contains a status bar.



Plaso for LogicalFileSet1
DAT File Extractor

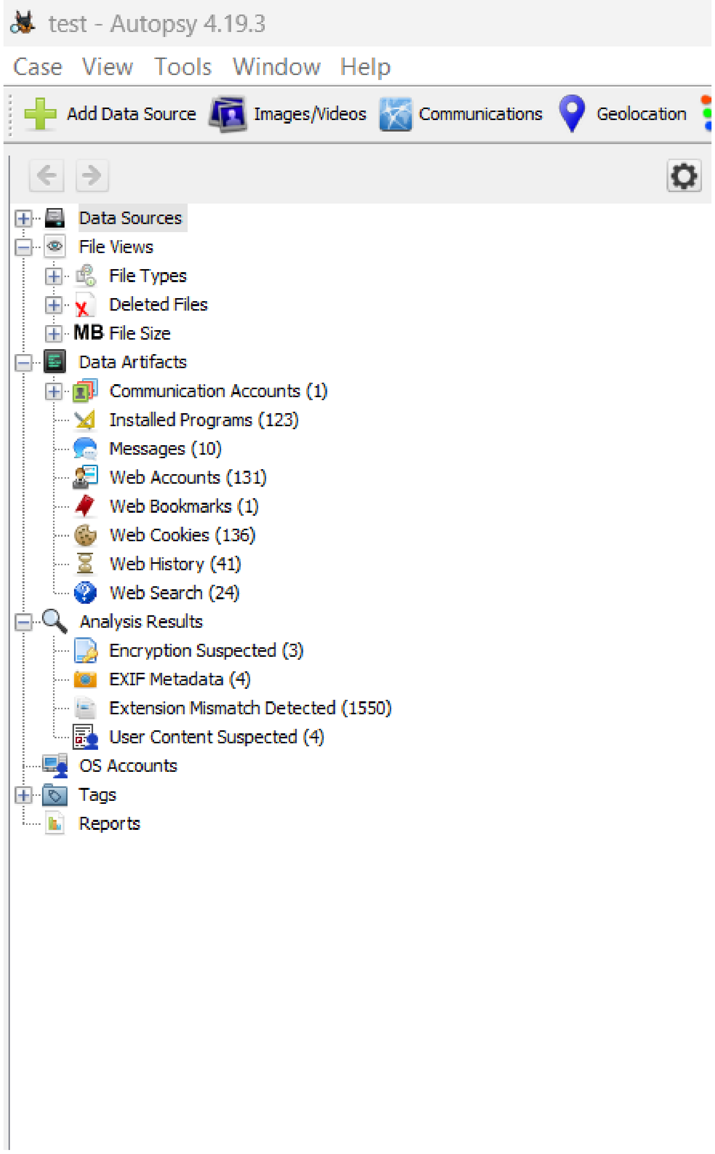
Analyzing files from LogicalFileSet1 100%
2022 CTF - Android.tar

Embedded File Extractor 100%
2022 CTF - Android.tar: Adding/updating files in case database (7173 of 35682)

Analyzing files from LogicalFileSet1 100% (2 more...)

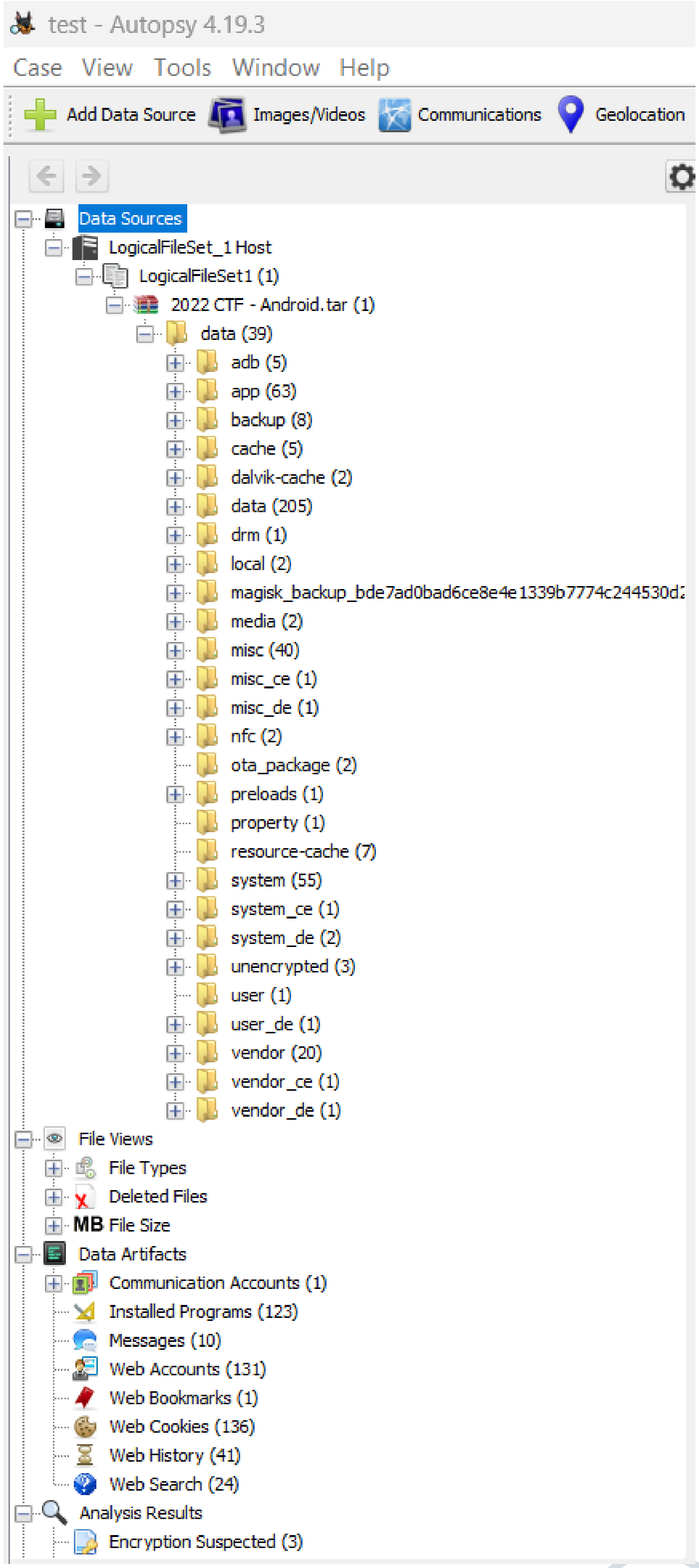
Navigating the Case

The left-hand pane allows the option to select a variety of different types of results that will be displayed in the top-right pane. Looking at the left-hand side we see Categories such as Data Sources, File Views, Data Artifacts, Analysis Results, and Tags. We can expand or collapse each of these categories by selecting the "+" or "-" to the left which will also show subcategories.



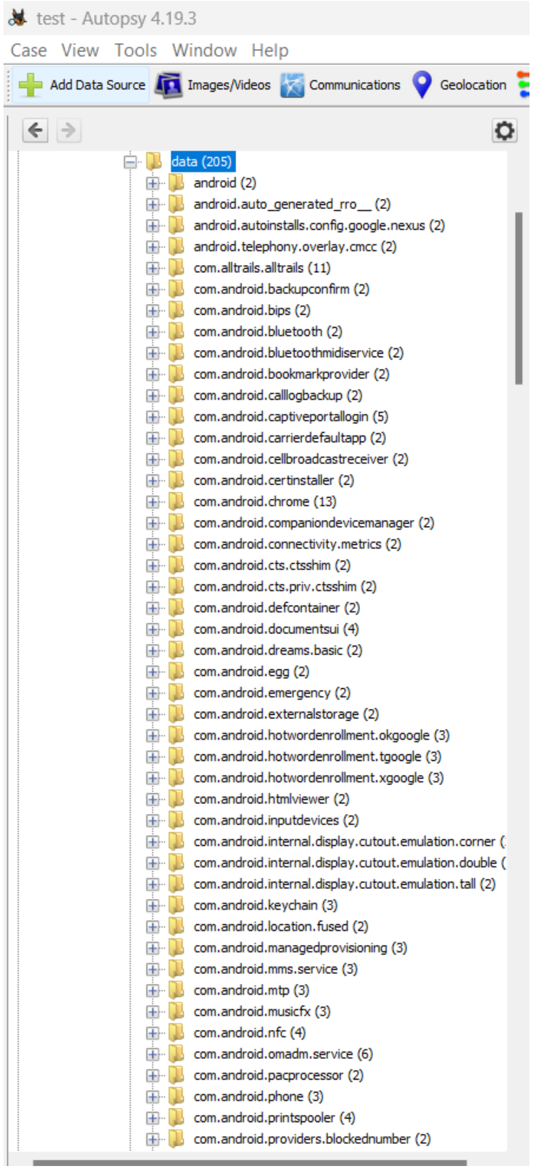
To view the file tree, click the "+" next to "Data Sources", and then again for "logitalfileset_1 Host", "LogicalFileSet1(1)", "2022 CTF-Android.Tar" and lastly "data". The display will vary based on the files processed and lastly data.

The file tree should look something like this:

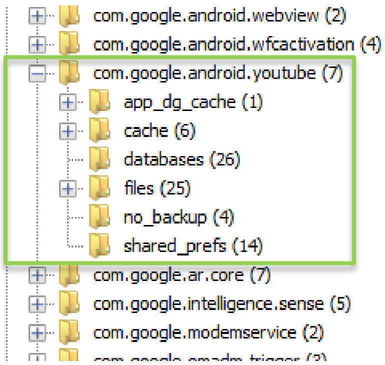


```
Data Sources
  LogicalFileSet_1 Host
    LogicalFileSet1 (1)
      2022 CTF - Android.tar (1)
        data (39)
          adb (5)
          app (63)
          backup (8)
          cache (5)
          dalvik-cache (2)
          data (205)
          drm (1)
          local (2)
          magisk_backup_bde7ad0bad6ce8e4e1339b7774c244530d2
          media (2)
          misc (40)
          misc_ce (1)
          misc_de (1)
          nfc (2)
          ota_package (2)
          preloads (1)
          property (1)
          resource-cache (7)
          system (55)
          system_ce (1)
          system_de (2)
          unencrypted (3)
          user (1)
          user_de (1)
          vendor (20)
          vendor_ce (1)
          vendor_de (1)
File Views
  File Types
  Deleted Files
  MB File Size
Data Artifacts
  Communication Accounts (1)
  Installed Programs (123)
  Messages (10)
  Web Accounts (131)
  Web Bookmarks (1)
  Web Cookies (136)
  Web History (41)
  Web Search (24)
Analysis Results
  Encryption Suspected (3)
```

Each of the “+” options allow you to navigate through the files and folders in the “data” directory.

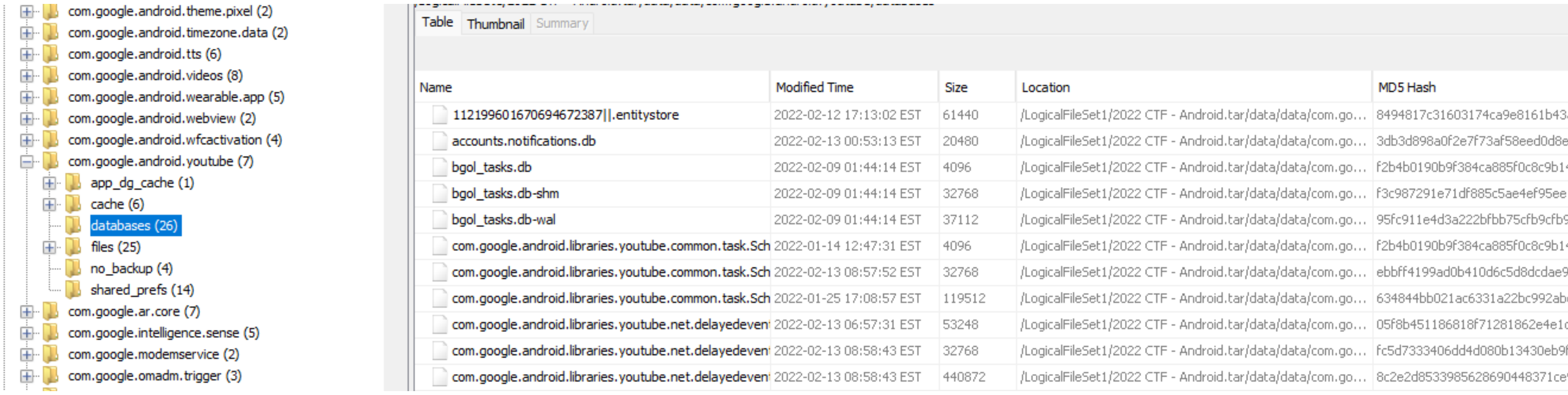


```
data (205)
    android (2)
    android.auto_generated_rro__ (2)
    android.autoinstalls.config.google.nexus (2)
    android.telephony.overlay.cmcc (2)
    com.alltrails.alltrails (11)
    com.android.backupconfirm (2)
    com.android.bips (2)
    com.android.bluetooth (2)
    com.android.bluetoothmidiservice (2)
    com.android.bookmarkprovider (2)
    com.android.calllogbackup (2)
    com.android.captiveportallogin (5)
    com.android.carrierdefaultapp (2)
    com.android.cellbroadcastreceiver (2)
    com.android.certinstaller (2)
    com.android.chrome (13)
    com.android.companiondevicemanager (2)
    com.android.connectivity.metrics (2)
    com.android.cts.ctsshim (2)
    com.android.cts.priv.ctsshim (2)
    com.android.defcontainer (2)
    com.android.documentsui (4)
    com.android.dreams.basic (2)
    com.android.egg (2)
    com.android.emergency (2)
    com.android.externalstorage (2)
    com.android.hotwordenrollment.okgoogle (3)
    com.android.hotwordenrollment.tgoogle (3)
    com.android.hotwordenrollment.xgoogle (3)
    com.android.htmlviewer (2)
    com.android.inputdevices (2)
    com.android.internal.display.cutout.emulation.corner (
    com.android.internal.display.cutout.emulation.double (
    com.android.internal.display.cutout.emulation.tall (2)
    com.android.keychain (3)
    com.android.location.fused (2)
    com.android.managedprovisioning (3)
    com.android.mms.service (3)
    com.android.mtp (3)
    com.android.musicfx (3)
    com.android.nfc (4)
    com.android.omadm.service (6)
    com.android.pacprocessor (2)
    com.android.phone (3)
    com.android.printspooler (4)
    com.android.providers.blockednumber (2)
```



```
com.google.android.webview (2)
com.google.android.wfcactivation (4)
com.google.android.youtube (7)
    app_dg_cache (1)
    cache (6)
    databases (26)
    files (25)
    no_backup (4)
    shared_prefs (14)
com.google.ar.core (7)
com.google.intelligence.sense (5)
com.google.modemservice (2)
com.google.omadm.trigger (2)
```

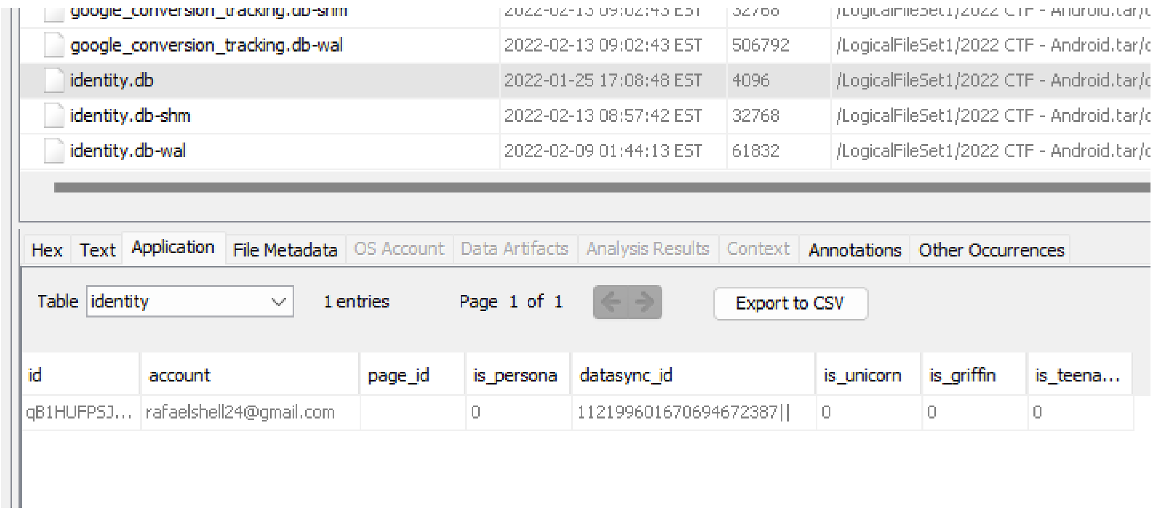
When the folder is selected from the tree that has terminal files, those files will be shown in the upper right-hand pane with columns of metadata to the right.



- com.google.android.theme.pixel (2)
- com.google.android.timezone.data (2)
- com.google.android.tts (6)
- com.google.android.videos (8)
- com.google.android.wearable.app (5)
- com.google.android.webview (2)
- com.google.android.wfcactivation (4)
- com.google.android.youtube (7)
  - app_dg_cache (1)
  - cache (6)
  - databases (26)
  - files (25)
  - no_backup (4)
  - shared_prefs (14)
- com.google.ar.core (7)
- com.google.intelligence.sense (5)
- com.google.modemservice (2)
- com.google.omadm.trigger (3)

Name	Modified Time	Size	Location	MD5 Hash
1121996016706946723 87||.entitystore	2022-02-12 17:13:02 EST	61440	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	8494817c31603174ca9e8161b43
accounts.notifications.db	2022-02-13 00:53:13 EST	20480	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	3db3d898a0f2e7f73af58eed0d8e
bgol_tasks.db	2022-02-09 01:44:14 EST	4096	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	f2b4b0190b9f384ca885f0c8c9b1
bgol_tasks.db-shm	2022-02-09 01:44:14 EST	32768	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	f3c987291e71df885c5ae4ef95ee
bgol_tasks.db-wal	2022-02-09 01:44:14 EST	37112	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	95fc911e4d3a222bfbb75cfb9cfb
com.google.android.libraries.youtube.common.task.Sch	2022-01-14 12:47:31 EST	4096	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	f2b4b0190b9f384ca885f0c8c9b1
com.google.android.libraries.youtube.common.task.Sch	2022-02-13 08:57:52 EST	32768	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	ebbff4199ad0b410d6c5d8dcdae
com.google.android.libraries.youtube.common.task.Sch	2022-01-25 17:08:57 EST	119512	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	634844bb021ac6331a22bc992ab
com.google.android.libraries.youtube.net.delayedevent	2022-02-13 06:57:31 EST	53248	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	05f8b451186818f71281862e4e1
com.google.android.libraries.youtube.net.delayedevent	2022-02-13 08:58:43 EST	32768	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	fc5d7333406dd4d080b13430eb9
com.google.android.libraries.youtube.net.delayedevent	2022-02-13 08:58:43 EST	440872	/LogicalFileSet1/2022 CTF - Android.tar/data/data/com.go...	8c2e2d8533985628690448371ce

When a file in the upper-right pane is selected, the bottom pane can be used to view the file in a variety of ways. Below we will use the “Application” tab of the bottom pane to see the data using the Autopsy native SQLite browsing utility.



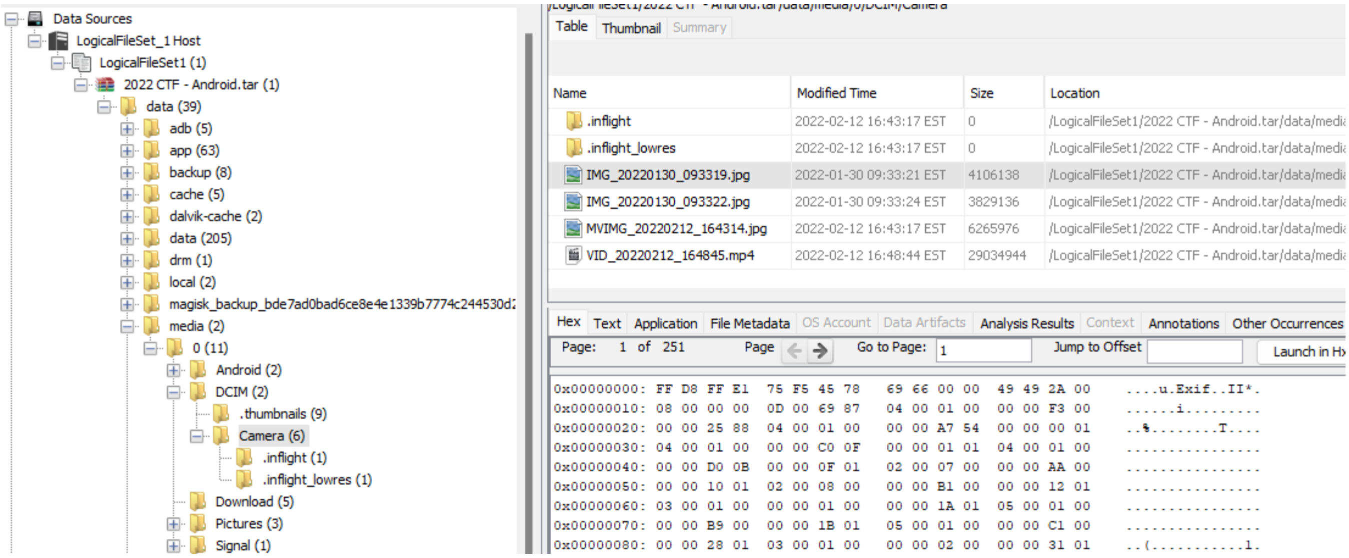
google_conversion_tracking.db-shm	2022-02-13 09:02:43 EST	32768	/LogicalFileSet1/2022 CTF - Android.tar/c
google_conversion_tracking.db-wal	2022-02-13 09:02:43 EST	506792	/LogicalFileSet1/2022 CTF - Android.tar/c
identity.db	2022-01-25 17:08:48 EST	4096	/LogicalFileSet1/2022 CTF - Android.tar/c
identity.db-shm	2022-02-13 08:57:42 EST	32768	/LogicalFileSet1/2022 CTF - Android.tar/c
identity.db-wal	2022-02-09 01:44:13 EST	61832	/LogicalFileSet1/2022 CTF - Android.tar/c

Table identity 1 entries Page 1 of 1

id	account	page_id	is_persona	datasync_id	is_unicorn	is_griffin	is_teena...
qB1HUFPSJ...	rafaelshell24@gmail.com		0	1121996016706946723 87||	0	0	0

Once a file is selected from the right panel hex and metadata tabs present additional data by selecting the “hex tab” and “File Metadata tab.”

Hex view:



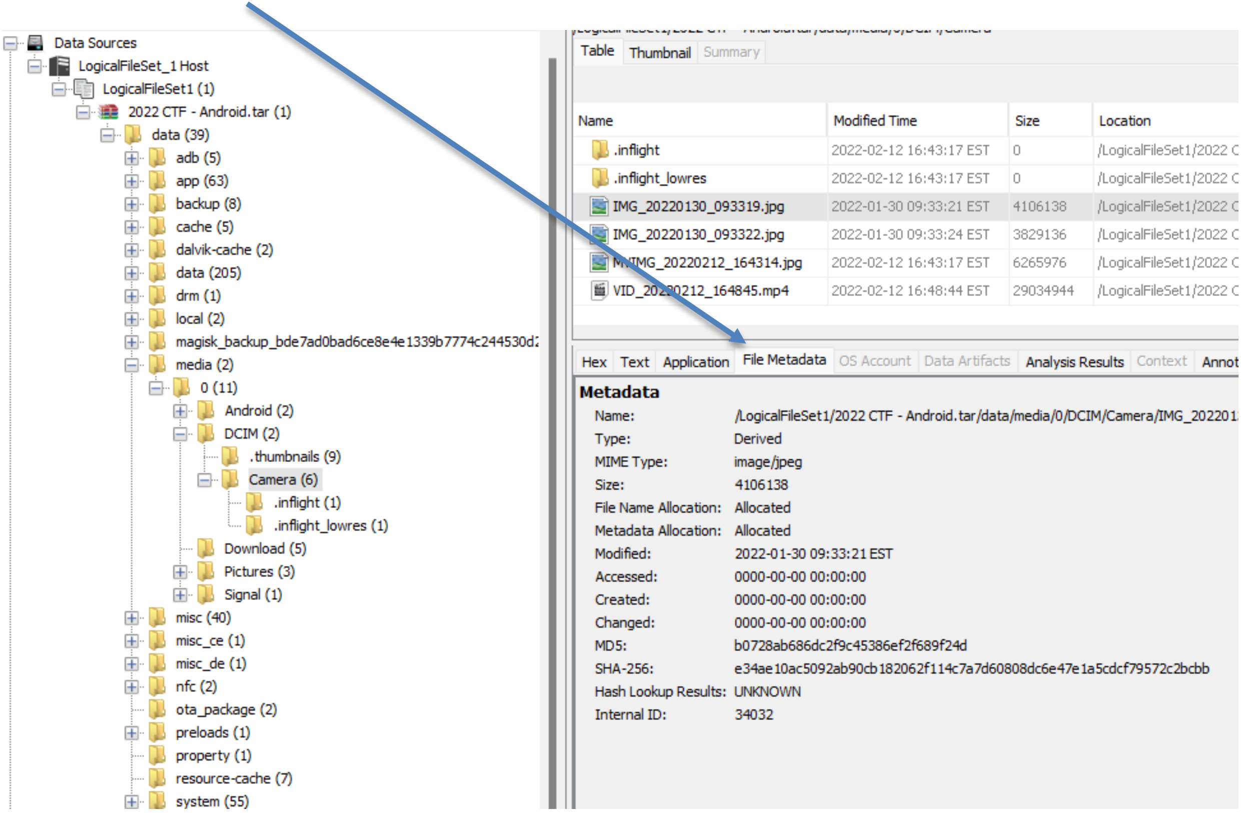
- Data Sources
  - LogicalFileSet_1 Host
    - LogicalFileSet1 (1)
      - 2022 CTF - Android.tar (1)
        - data (39)
          - adb (5)
          - app (63)
          - backup (8)
          - cache (5)
          - dalvik-cache (2)
          - data (205)
          - drm (1)
          - local (2)
          - magisk_backup_bde7ad0bad6ce8e4e1339b7774c244530d2
          - media (2)
            - 0 (11)
              - Android (2)
              - DCIM (2)
                - .thumbnails (9)
                - Camera (6)
                  - .inflight (1)
                  - .inflight_lowres (1)
              - Download (5)
              - Pictures (3)
              - Signal (1)

/LogicalFileSet1/2022 CTF - Android.tar/data/media/0/DCIM/Camera

Name	Modified Time	Size	Location
.inflight	2022-02-12 16:43:17 EST	0	/LogicalFileSet1/2022 CTF - Android.tar/data/media
.inflight_lowres	2022-02-12 16:43:17 EST	0	/LogicalFileSet1/2022 CTF - Android.tar/data/media
IMG_20220130_093319.jpg	2022-01-30 09:33:21 EST	4106138	/LogicalFileSet1/2022 CTF - Android.tar/data/media
IMG_20220130_093322.jpg	2022-01-30 09:33:24 EST	3829136	/LogicalFileSet1/2022 CTF - Android.tar/data/media
MVIMG_20220212_164314.jpg	2022-02-12 16:43:17 EST	6265976	/LogicalFileSet1/2022 CTF - Android.tar/data/media
VID_20220212_164845.mp4	2022-02-12 16:48:44 EST	29034944	/LogicalFileSet1/2022 CTF - Android.tar/data/media

```
0x00000000: FF D8 FF E1  75 F5 45 78   69 66 00 00  49 49 2A 00    ....u.Exif..II*.
0x00000010: 08 00 00 00  0D 00 69 87   04 00 01 00  00 00 F3 00    ......i.........
0x00000020: 00 00 25 88  04 00 01 00   00 00 A7 54  00 00 00 01    ..%........T....
0x00000030: 04 00 01 00  00 00 C0 0F   00 00 01 01  04 00 01 00    ................
0x00000040: 00 00 D0 0B  00 00 0F 01   02 00 07 00  00 00 AA 00    ................
0x00000050: 00 00 10 01  02 00 08 00   00 00 B1 00  00 00 12 01    ................
0x00000060: 03 00 01 00  00 00 01 00   00 00 1A 01  05 00 01 00    ................
0x00000070: 00 00 B9 00  00 00 1B 01   05 00 01 00  00 00 C1 00    ................
0x00000080: 00 00 28 01  03 00 01 00   00 00 02 00  00 00 31 01    ..(.........1.
```

File Metadata view:



- Data Sources
  - LogicalFileSet_1 Host
    - LogicalFileSet1 (1)
      - 2022 CTF - Android.tar (1)
        - data (39)
          - adb (5)
          - app (63)
          - backup (8)
          - cache (5)
          - dalvik-cache (2)
          - data (205)
          - drm (1)
          - local (2)
          - magisk_backup_bde7ad0bad6ce8e4e1339b7774c244530d2
          - media (2)
            - 0 (11)
              - Android (2)
              - DCIM (2)
                - .thumbnails (9)
                - Camera (6)
                  - .inflight (1)
                  - .inflight_lowres (1)
              - Download (5)
              - Pictures (3)
              - Signal (1)
          - misc (40)
          - misc_ce (1)
          - misc_de (1)
          - nfc (2)
          - ota_package (2)
          - preloads (1)
          - property (1)
          - resource-cache (7)
          - system (55)

Name	Modified Time	Size	Location
.inflight	2022-02-12 16:43:17 EST	0	/LogicalFileSet1/2022 C
.inflight_lowres	2022-02-12 16:43:17 EST	0	/LogicalFileSet1/2022 C
IMG_20220130_093319.jpg	2022-01-30 09:33:21 EST	4106138	/LogicalFileSet1/2022 C
IMG_20220130_093322.jpg	2022-01-30 09:33:24 EST	3829136	/LogicalFileSet1/2022 C
MVIMG_20220212_164314.jpg	2022-02-12 16:43:17 EST	6265976	/LogicalFileSet1/2022 C
VID_20220212_164845.mp4	2022-02-12 16:48:44 EST	29034944	/LogicalFileSet1/2022 C

Metadata

Name:	/LogicalFileSet1/2022 CTF - Android.tar/data/media/0/DCIM/Camera/IMG_202201
Type:	Derived
MIME Type:	image/jpeg
Size:	4106138
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-01-30 09:33:21 EST
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	b0728ab686dc2f9c45386ef2f689f24d
SHA-256:	e34ae10ac5092ab90cb182062f114c7a7d60808dc6e47e1a5cdcf79572c2bcbb
Hash Lookup Results:	UNKNOWN
Internal ID:	34032