

AUTOPSY

Arkansas Strike Team

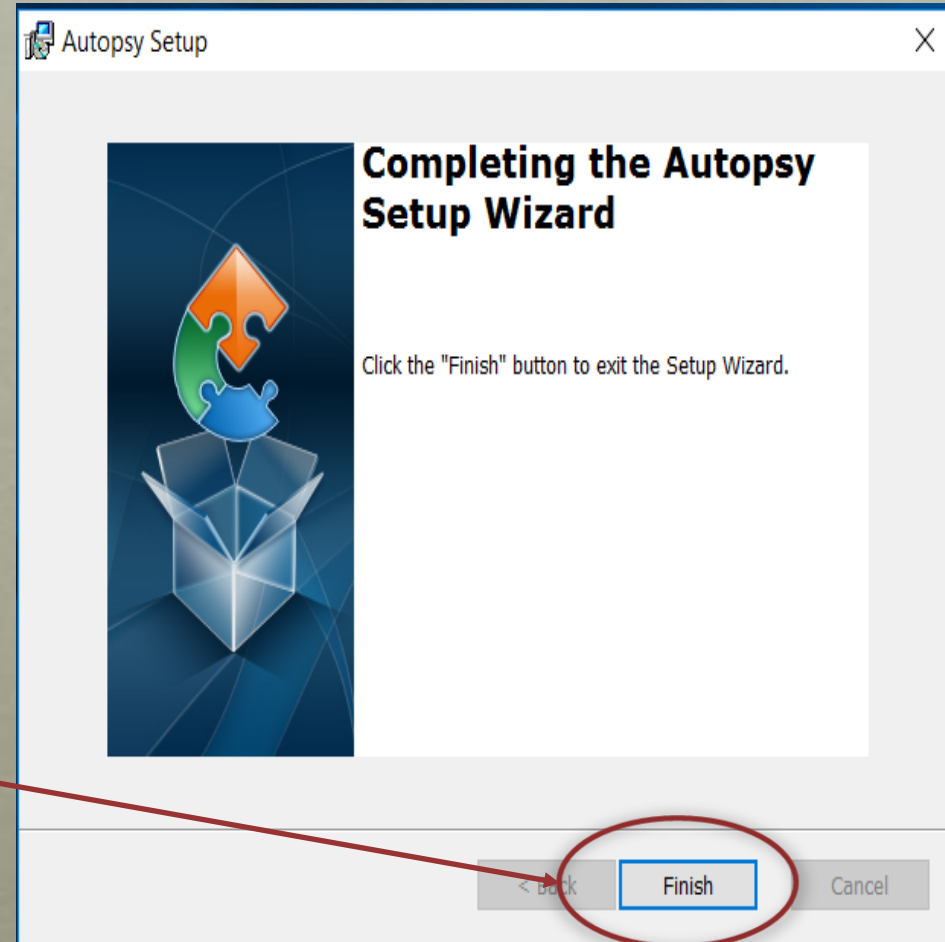
September 2021

AUTOPSY

- **Autopsy** is a FREE forensic tool. It is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer.
- Download Autopsy from the website:
<http://sleuthkit.org/autopsy/download.php>

INSTALLATION

- Run Autopsy msi file (autopsy-4.3.0-64bit.exe)
- Click through the dialog boxes until you click a button that says *Finish*

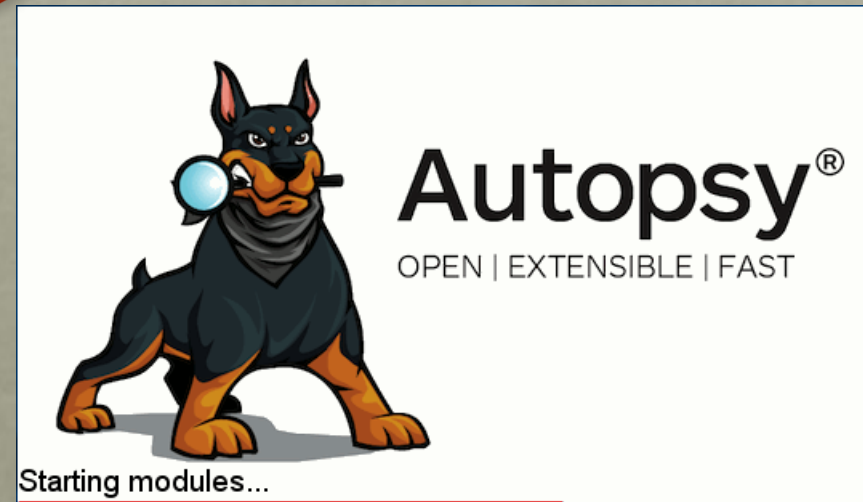


AUTOPSY WORKFLOW

- 1. Create a Case**
- 2. Adding a Data Source**
- 3. Analyze with Ingest Modules**
- 4. Manual Analysis**
- 5. Report Generation**

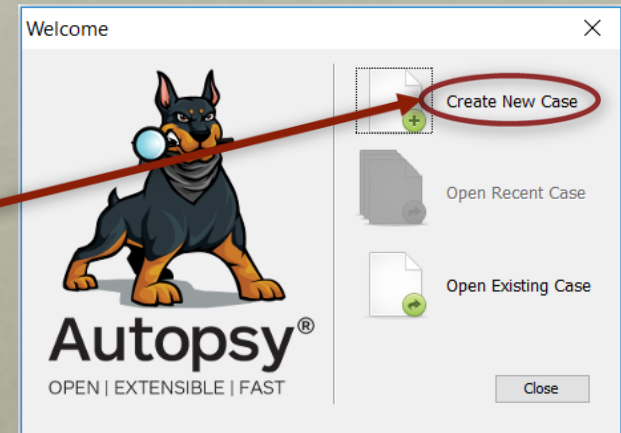
LAUNCH AUTOPSY

- Autopsy should now be fully installed
- Double click on the icon



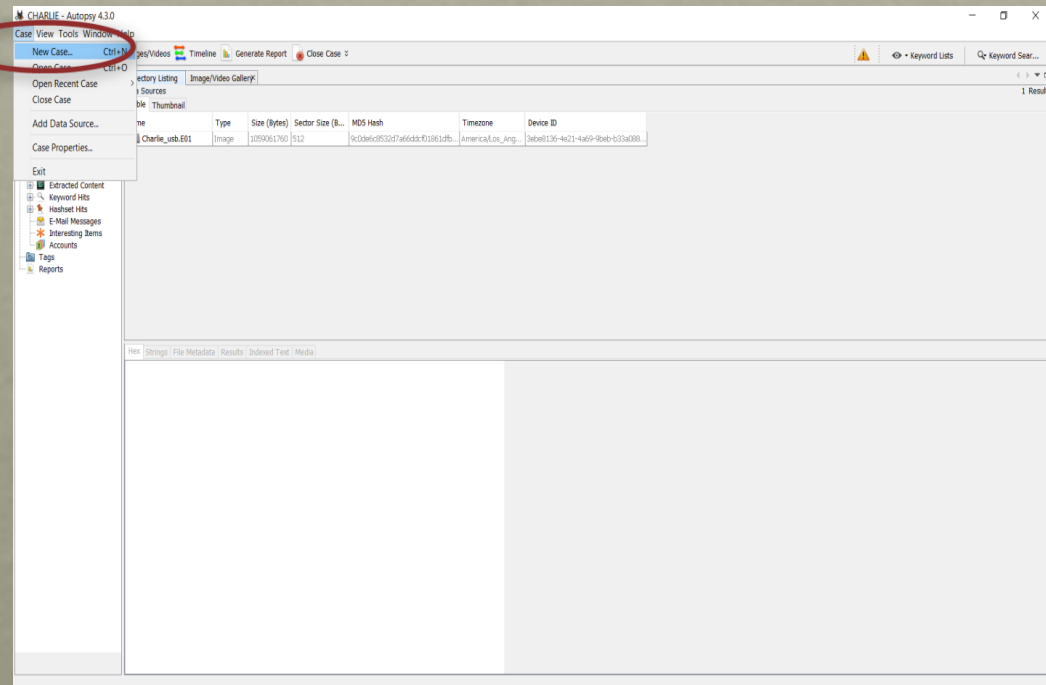
CREATE NEW CASE

- Click **Create New Case**



or

- Click **CASE**
→ New Case



NEW CASE INFORMATION

New Case Information

Steps

1. Case Info
2. Additional Information

Case Info

Enter New Case Information:

Case Name:

Base Directory:

Case Type: Single-user Multi-user

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

New Case Information

Steps

1. Case Info
2. Additional Information

Additional Information

Optional: Set Case Number and Examiner

Case Number:

Examiner:

< Back Next > **Finish** Cancel Help

ADDING A DATA SOURCE

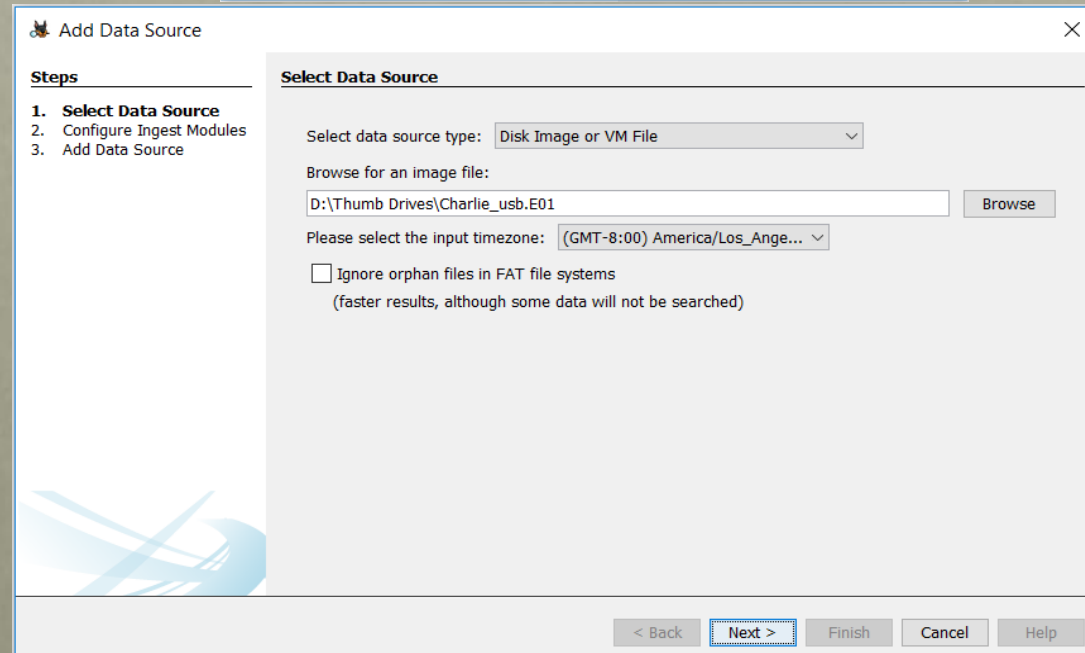
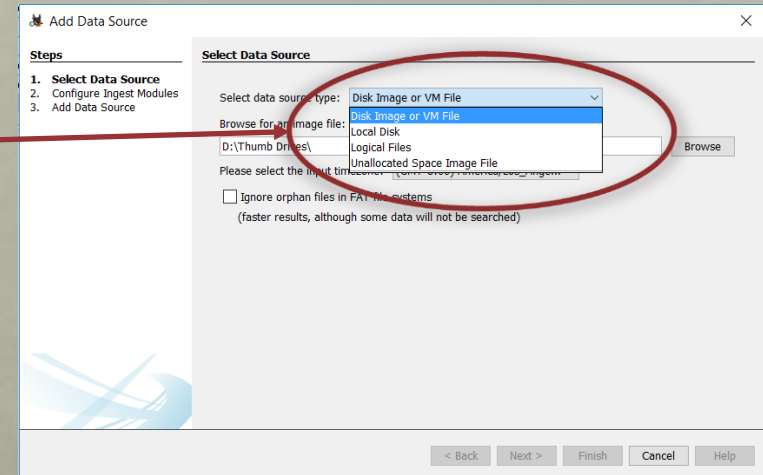
- There are four options.

1. Disk Image or VM File

2. Local Disk

3. Logical Files

4. Unallocated Space Image File



THREE TYPES OF DATA SOURCES

1. Disk Image: A file (or set of files) that is a byte-for-byte copy of a hard drive or flash drive

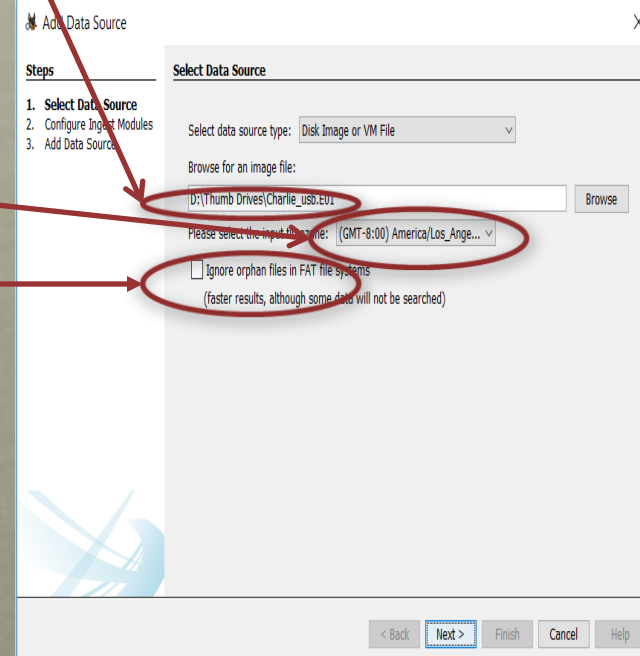
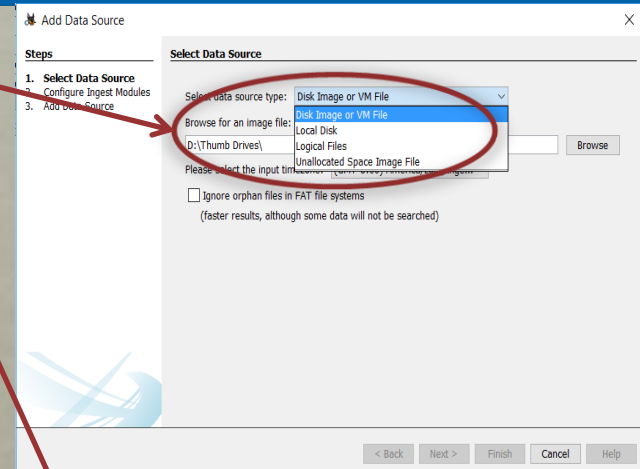
- Raw Single (For example: *.img, *.dd, *.raw, *.bin)
- Raw Split (For example: *.001, *.002, *.aa, *.ab, etc)
- EnCase (For example: *.e01, *.e02, etc)
- Virtual Machines (For example: *.vmdk, *.vhd)

THREE TYPES OF DATA SOURCES (CONT)

- 2. Local Drive:** Local storage device (USB attached flash drive)
- 3. Logical Files:** Local files or folders

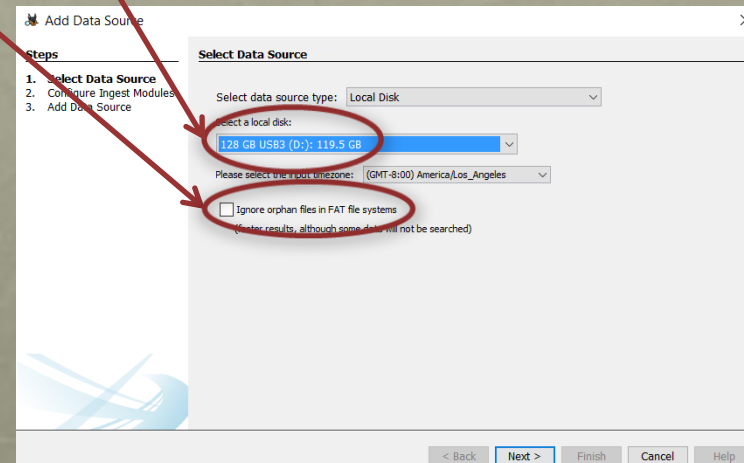
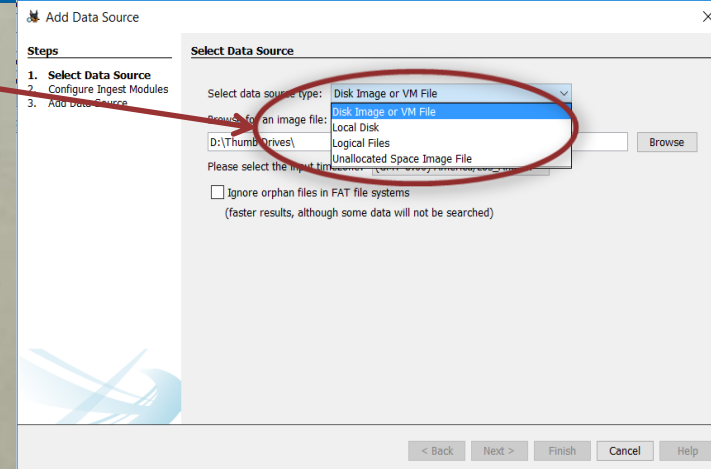
ADDING A DISK IMAGE

1. Select "**Disk Image**" from the pull down.
2. Browse to the first file in the disk image and only the first file and Autopsy will find the rest.
3. Select **Timezone** that the disk image came from. Autopsy will not know how to normalize to UTC.
4. Choose to perform orphan file finding on FAT file systems. This can be a time intensive process because it will require that Autopsy look at each sector in the device.



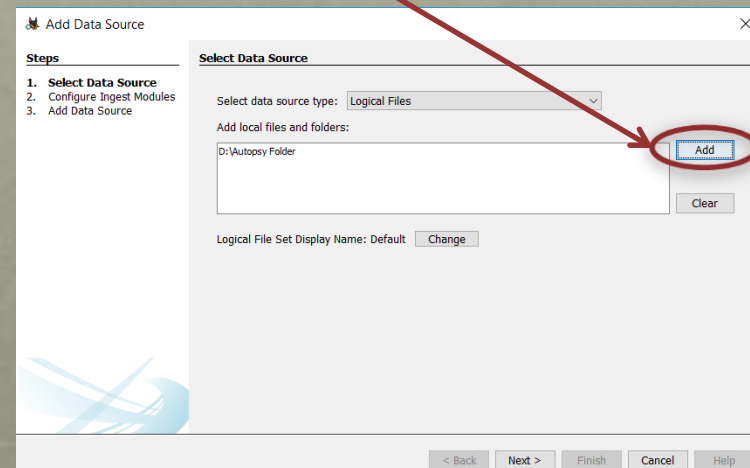
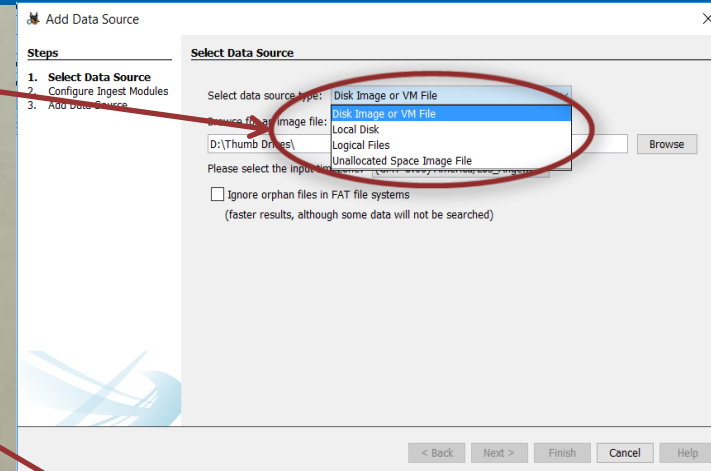
ADDING A LOCAL DRIVE

1. Select “**Local Drive**” from the pull down of the Data Source Type.
2. Select a local disk from the drop down list
3. Choose to perform orphan file finding on FAT file systems. This can be a time intensive process because it will require that Autopsy look at each sector in the device.



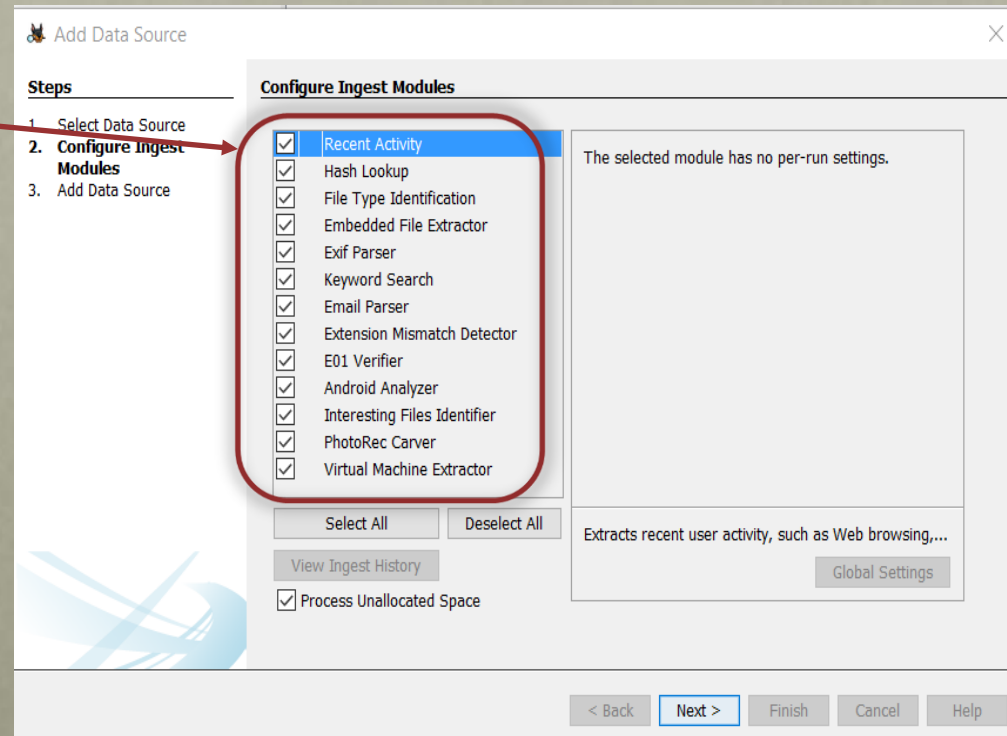
ADDING A LOCAL FILES

1. Select “**Local Files**” from the full down of Data Source Type.
2. Press the “**Add**” button and navigate to a folder (including sub-folders) or file to add.
3. Continue to press “Add” until all files and folders have been selected.



INGEST MODULES

- List of Ingest Modules to enable
- After you configure the ingest modules, you may need to wait for Autopsy to finish its basic examination of the data source



VIEWING INGEST MODULES RESULTS

Click **Yellow Triangle** on the top right



Module	Num	New?	Subject	Timestamp
Hash Lookup	1		No known bad hash database set.	12:53:40
Hash Lookup	1		No known hash database set.	12:53:40
Recent Activity	1		Started Charlie_usb.E01	12:53:40
Recent Activity	1		Finished Charlie_usb.E01 - No errors reported	12:53:40
Recent Activity	1		Charlie_usb.E01 - Browser Results	12:53:40
Embedded File Extrac...	1		Encrypted files in archive detected.	12:53:46
Embedded File Extrac...	1		Encrypted files in archive detected.	12:53:47
Embedded File Extrac...	1		Encrypted files in archive detected.	12:53:49
Embedded File Extrac...	1		Encrypted files in archive detected.	12:53:51
Embedded File Extrac...	1		Encrypted files in archive detected.	12:53:53
File Type Identification	1		File Type Id Results	12:54:37
Keyword Search	1		• Keyword Indexing Results	12:55:24
Extension Mismatch D...	1		• File Extension Mismatch Results	12:55:24
PhotoRec Carver	1		• PhotoRec Results	12:55:24
E01 Verifier	1		• Starting Charlie_usb.E01	12:55:24
E01 Verifier	1		• Charlie_usb.E01 verified	12:55:29

Sort by: Time Total: 16 Unique: 16

INGEST MODULES (CONT)

- **Recent Activity Module** extracts user activity as saved by web browsers and the OS. Also runs Regripper on the registry hive
- **File Type Identification Module** determines file types based on signatures and reports them based on MIME type. It stores the results in the Blackboard and many modules depend on this. It uses the Tika open source library. You can define your own custom file types in Tools, Options, File Types

INGEST MODULES (CONT)

- **Hash Database Lookup Module** uses hash databases to ignore known files from the NIST NSRL. Use the "Advanced" button to add and configure the hash databases to use during this process. You will get updates on known bad file hits as the ingest occurs. You can later add hash databases via the Tools -> Options menu in the main UI. NIST NSRL can be downloaded from

<http://sourceforge.net/projects/autopsy/files/NSRL/>

INGEST MODULES (CONT)

- **Hash Embedded File Extraction Module** opens ZIP, RAR, other archive formats, Doc, Docx, PPT, PPTX, XLS, and XLSX and sends the derived files from those files back through the ingest pipeline for analysis.
- **EXIF Parser Module** extracts EXIF information from JPEG files and posts the results into the tree in the main UI.

INGEST MODULES (CONT)

- **Keyword Search Module** uses keyword lists to identify files with specific words in them. You can select the keyword lists to search for automatically and you can create new lists using the "Advanced" button. You do not need to wait for all files to be indexed before performing a keyword search, however you will only get results from files that have already been indexed when you perform your search

INGEST MODULES (CONT)

- **Extension Mismatch Detector Module** uses the results from the File Type Identification and flags files that have an extension not traditionally associated with the file's detected type. Ignores 'known' (NSRL) files. You can customize the MIME types and file extensions per MIME type in Tools, Options, File Extension Mismatch

INGEST MODULES (CONT)

- **Email Parser Module** identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails from them, adding the results to the Blackboard
- **E01 Verifier Module** computes a checksum on E01 files and compares with the E01 file's internal checksum to ensure they match

INGEST MODULES (CONT)

- **Extension Mismatch Detector Module** uses the results from the File Type Identification and flags files that have an extension not traditionally associated with the file's detected type. Ignores 'known' (NSRL) files. You can customize the MIME types and file extensions per MIME type in Tools, Options, File Extension Mismatch

INGEST MODULES (CONT)

- **Android Analyzer Module** allows you to parse common items from Android devices. Places artifacts into the BlackBoard
- **PhotoRec Carver Module** carves files from unallocated space and sends them through the file processing chain

INGEST MODULES (CONT)

- **Interesting Files Identifier Module** searches for files and directories based on user-specified rules in Tools, Options, Interesting Files. It works as a "File Alerting Module". It generates messages in the inbox when specified files are found

USER INTERFACE (UI) LAYOUT

- Tree Viewer
- Result Viewer
- Content Viewer
- Keyword Search
- Status Area

The screenshot shows the CHARLIE - Autopsy 4.3.0 interface. The main window is titled "CHARLIE - Autopsy 4.3.0" and contains a menu bar (Case, View, Tools, Window, Help) and a toolbar with buttons for "Add Data Source", "View Images/Videos", "Timeline", "Generate Report", and "Close Case".

Key UI components are highlighted with red boxes and labels:

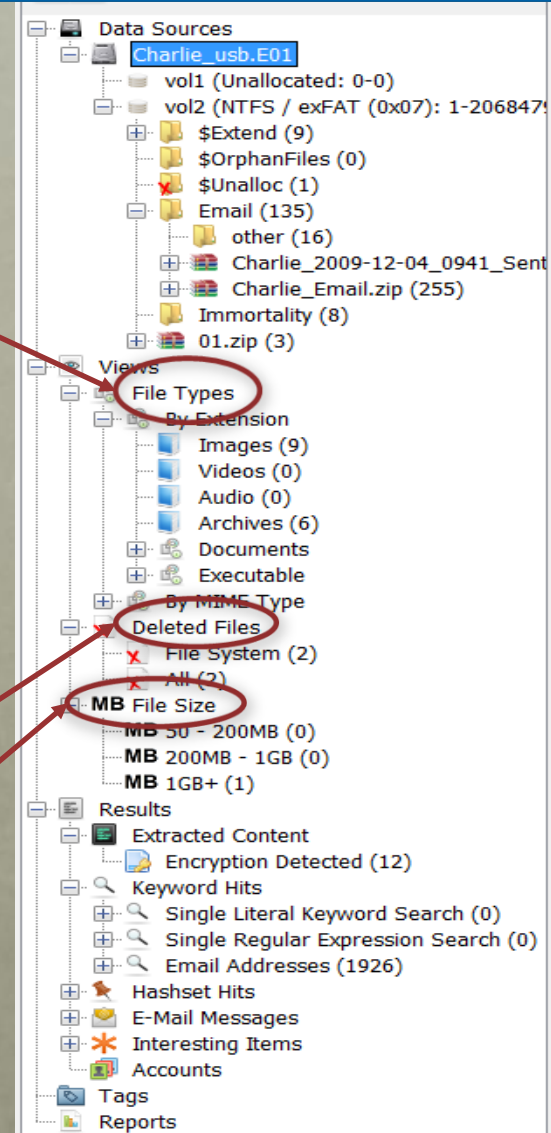
- Keyword Search:** A red box highlights the search bar at the top right, containing the text "Keyword Search".
- Tree Viewer:** A red box highlights the left sidebar, which contains a file tree structure under "Data Sources" and "Views".
- Result Viewer:** A red box highlights the central table displaying search results. The table has columns for Name, Location, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), MD5 Hash, and Flags. The selected row is "Charlie_2009-12-03_1216_Sent_astronaut1.jpg".
- Content Viewer:** A red box highlights the bottom right area, which displays a large image of an astronaut on the moon's surface.
- Status Area:** A red box highlights the bottom right corner, which contains the text "Status Area".

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	MD5 Hash	Flags
astronaut.jpg	/img_Charlie_usb.E01/vol2/astronaut.jpg	2009-11-24 13:33:33	2009-11-24 13:40:19	2009-12-10 14:26:04	2009-11-24 13:40:19	713418	Allocated	40b386b30ed026c60ec1ac72e87360a3	Allocated
astronaut1.jpg	/img_Charlie_usb.E01/vol2/astronaut1.jpg	2009-11-24 13:43:42	2009-11-24 13:44:00	2009-12-10 14:26:04	2009-11-24 13:47:38	722717	Allocated	45eade24b3a89b21fed303310ccbd54	Allocated
Charlie_2009-12-07_1144_Sent_microscope1.jpg	/img_Charlie_usb.E01/vol2/Email/other/C...	29:38	2009-12-10 14:29:37	2009-12-10 14:29:37	2009-12-10 14:29:37	136274	Allocated	4be2c4abb48c4389ca79866c21736ea1	Allocated
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol2/Email/Charlie...	26:05	2009-12-04 13:50:23	2009-12-04 13:50:23	2009-12-04 13:50:23	722717	Allocated	45eade24b3a89b21fed303310ccbd54	Allocated
microscope.jpg	/img_Charlie_usb.E01/vol2/microscope.jp...	09:36	2009-11-24 13:40:20	2009-11-24 13:40:20	2009-11-24 13:40:20	136274	Allocated	689e8ffccab52dc0ccc68078e42c094da	Allocated
microscope1.jpg	/img_Charlie_usb.E01/vol2/microscope1.jp...	2009-11-24 14:19:21	2009-11-24 14:19:21	2009-11-24 14:19:24	2009-11-24 14:19:24	136274	Allocated	4be2c4abb48c4389ca79866c21736ea1	Allocated
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol2/Email/Charlie_Em...	2009-12-04 12:50:26	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	722717	Allocated	45eade24b3a89b21fed303310ccbd54	Allocated
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol2/Email/Charlie_Em...	2009-12-04 12:50:26	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	722717	Allocated	45eade24b3a89b21fed303310ccbd54	Allocated

TREE VIEWER

Views filter all the files in the case by some external property of the file

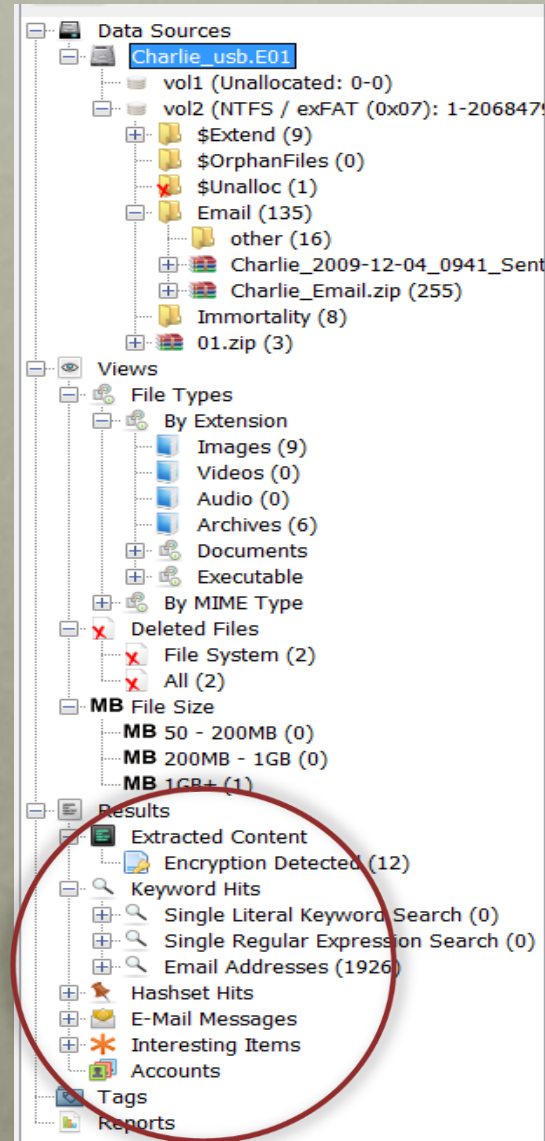
- **File Type** Sorts files by file extension.
- **Recent Files** Displays files that are accessed within the last seven days the user had the device.
- **Deleted Files** Displays files that have been deleted but the names have been recovered.
- **File Size** Sorts files by size.



TREE VIEWER

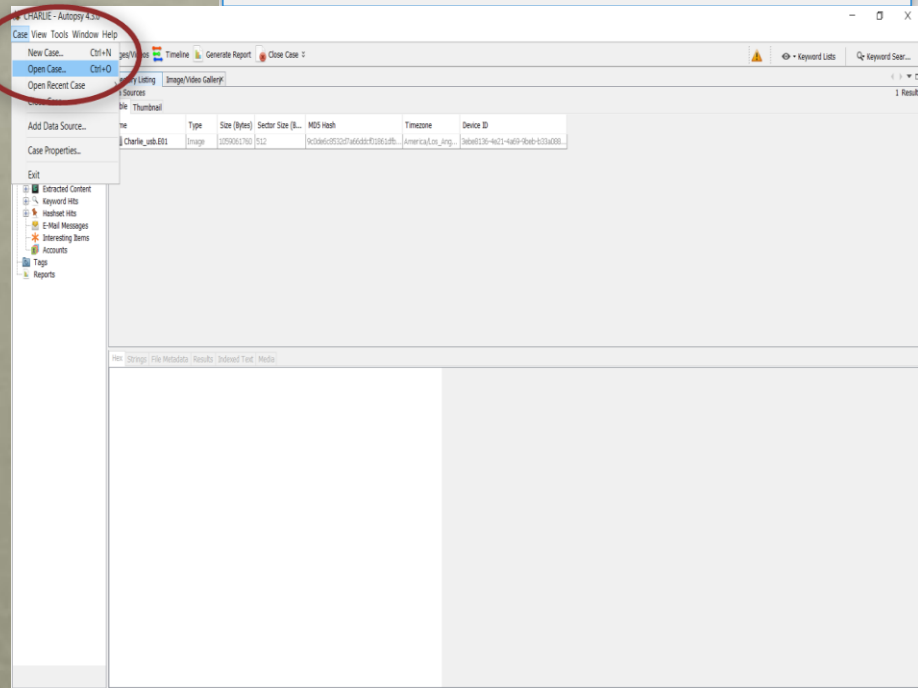
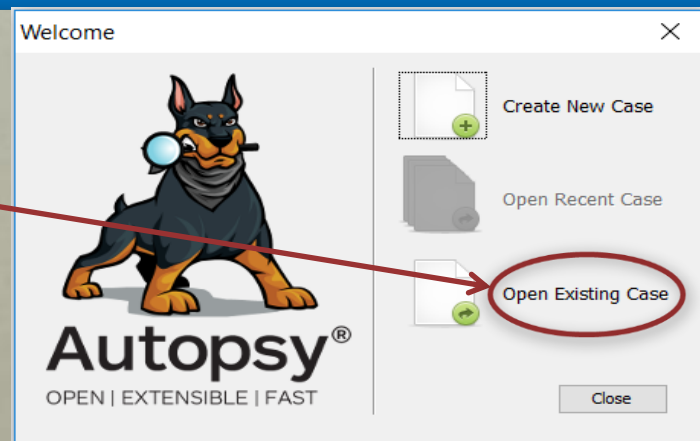
RESULTS

- **Extracted Content:** Many ingest modules will place results here; EXIF data, GPS locations, or Web History for example
- **Keyword Hits:** Keyword search hits show up here
- **Hashset Hits:** Hashset hits show up here
- **E-Mail Messages:** Email messages show up here
- **Interesting Items:** Things deemed interesting show up here
- **Tags:** Any item you tag shows up here so you can find it again easily



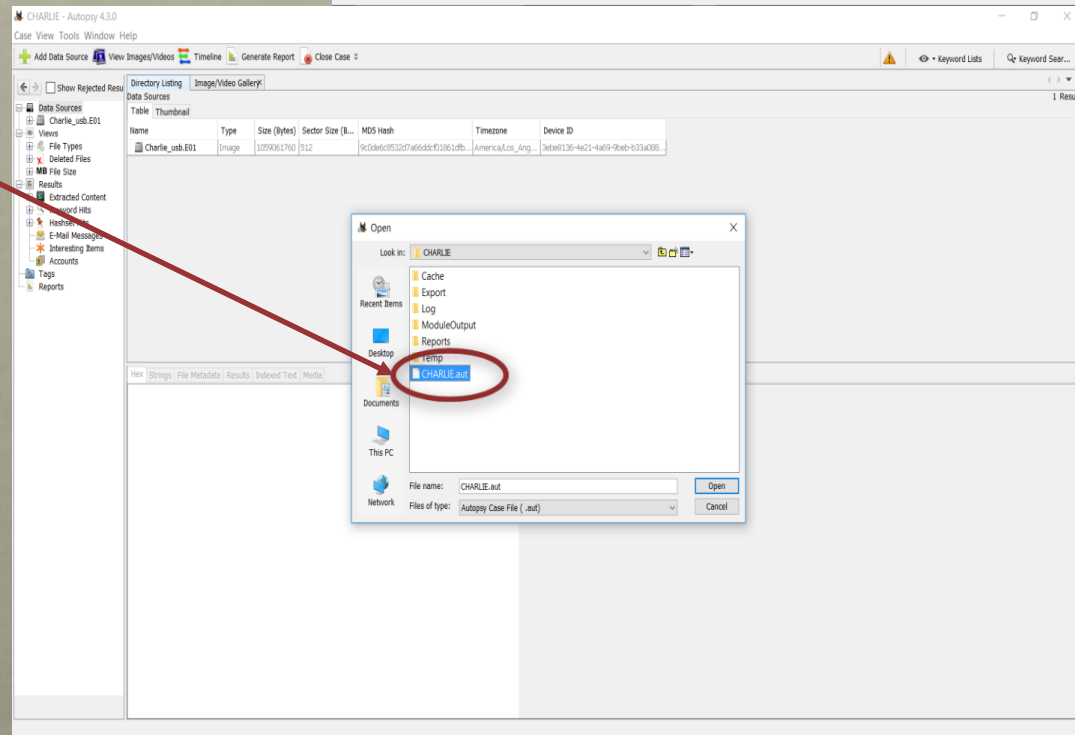
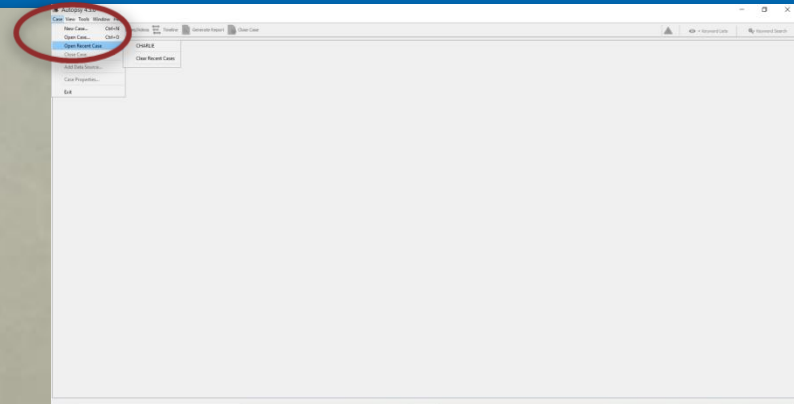
OPENING A CASE

- Click "Open Existing Case" or "Open Recent Case" from the opening splash screen.
- Choose the "Case", "Open Case" menu item or "Case", "Open Recent Case"



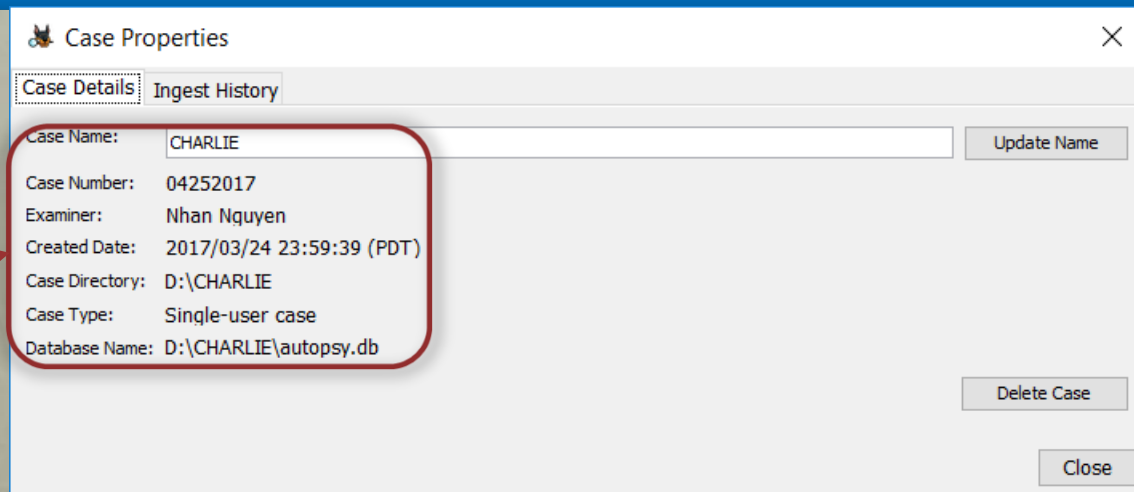
OPENING A CASE (CONT)

- Navigate to a folder containing the Autopsy case file.



CASE PROPERTIES

- Go to Case → Case Properties
- It shows the processing Start/End time



Case Properties

Case Details | Ingest History

Case Name: CHARLIE

Case Number: 04252017

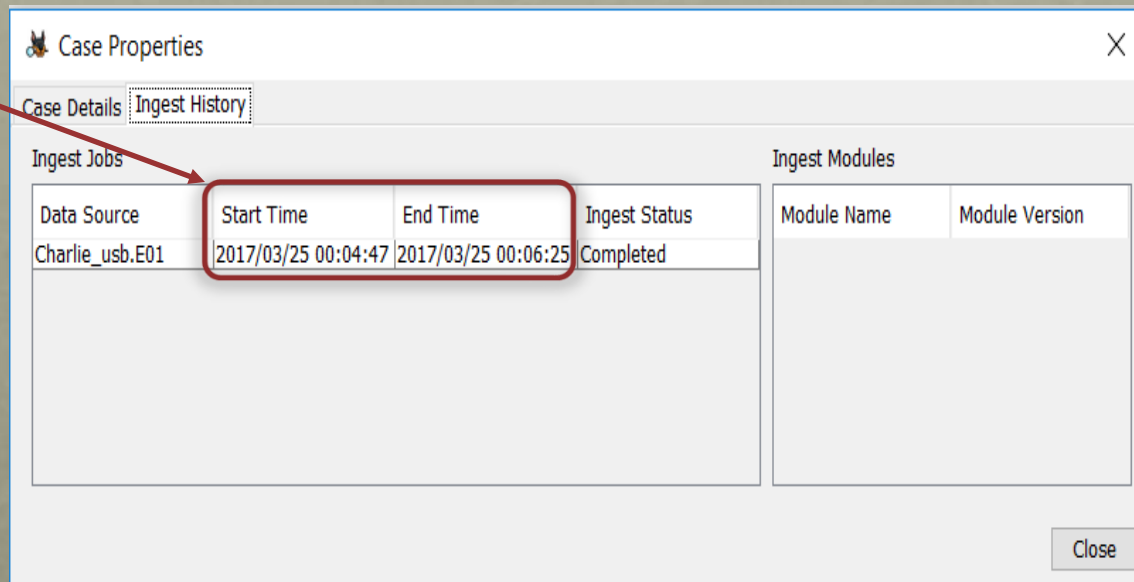
Examiner: Nhan Nguyen

Created Date: 2017/03/24 23:59:39 (PDT)

Case Directory: D:\CHARLIE

Case Type: Single-user case

Database Name: D:\CHARLIE\autopsy.db



Case Properties

Case Details | Ingest History

Ingest Jobs

Data Source	Start Time	End Time	Ingest Status
Charlie_usb.E01	2017/03/25 00:04:47	2017/03/25 00:06:25	Completed

Ingest Modules

Module Name	Module Version
-------------	----------------

SHOW SCREEN EDITER

- Go to **View** → **Show Screen Editor**
- Only shows **Result Viewer**

CHARLIE - Autopsy 4.3.0

Case View Tools Window Help

Images 9 Results

Table Thumbnail

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	MDS Hash	Flags(Meta)	Mode	UserID	GroupID	Meta Ad
astronaut.jpg	/img_Charlie_usb.E01/vol_vol2/astronaut.jpg	2009-11-24 13:33:33 ...	2009-11-24 13:40:19 ...	2009-12-10 14:26:04 ...	2009-11-24 13:40:19 ...	713418	Allocated	40c366b30ed026c0eac1ac72e87...	Allocated	rwxrwxrwx	0	0	37
astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2/astronaut1.jpg	2009-11-24 13:43:42 ...	2009-11-24 13:44:00 ...	2009-12-10 14:26:04 ...	2009-11-24 13:47:38 ...	722717	Allocated	45eade24b3a89ac21fed303310ccb...	Allocated	rwxrwxrwx	0	0	40
Charlie_2009-12-07_1144_Sent_microscope1.jpg	/img_Charlie_usb.E01/vol_vol2>Email/other/Charl...	2009-12-10 14:29:38 ...	2009-12-10 14:37:59 ...	2009-12-10 14:29:38 ...	2009-12-10 14:29:37 ...	136274	Allocated	4be2c4ab048c4389ca79866c2173...	Allocated	rwxrwxrwx	0	0	141
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2>Email/Charlie_20...	2009-12-04 13:50:24 ...	2009-12-04 13:50:24 ...	2009-12-10 14:26:05 ...	2009-12-04 13:50:23 ...	722717	Allocated	45eade24b3a89ac21fed303310ccb...	Allocated	rwxrwxrwx	0	0	126
microscope.jpg	/img_Charlie_usb.E01/vol_vol2/microscope.jpg	2009-11-24 13:27:51 ...	2009-11-24 13:56:35 ...	2009-11-24 14:09:36 ...	2009-11-24 13:40:20 ...	136274	Allocated	689a6ffcb9dcd1d2c68078e42c09...	Allocated	rwxrwxrwx	0	0	38
microscope1.jpg	/img_Charlie_usb.E01/vol_vol2/microscope1.jpg	2009-11-24 14:19:21 ...	2009-11-24 14:19:21 ...	2009-11-24 14:19:24 ...	2009-11-24 14:09:13 ...	136274	Allocated	4be2c4ab048c4389ca79866c2173...	Allocated	rwxrwxrwx	0	0	42
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2>Email/Charlie_Em...	2009-12-04 12:50:26 ...	0000-00-00 00:00:00 ...	0000-00-00 00:00:00 ...	0000-00-00 00:00:00 ...	722717	Allocated	45eade24b3a89ac21fed303310ccb...	Allocated	r-----	0	0	0
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2>Email/Charlie_Em...	2009-12-04 12:50:26 ...	0000-00-00 00:00:00 ...	0000-00-00 00:00:00 ...	0000-00-00 00:00:00 ...	722717	Allocated	45eade24b3a89ac21fed303310ccb...	Allocated	r-----	0	0	0
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2>Email/Charlie_Em...	2009-12-04 12:50:26 ...	0000-00-00 00:00:00 ...	0000-00-00 00:00:00 ...	0000-00-00 00:00:00 ...	722717	Allocated		Allocated	r-----	0	0	0

CHARLIE - Autopsy 4.3.0

Case View Tools Window Help

Images

Table Thumbnail

Page: 1 of 1

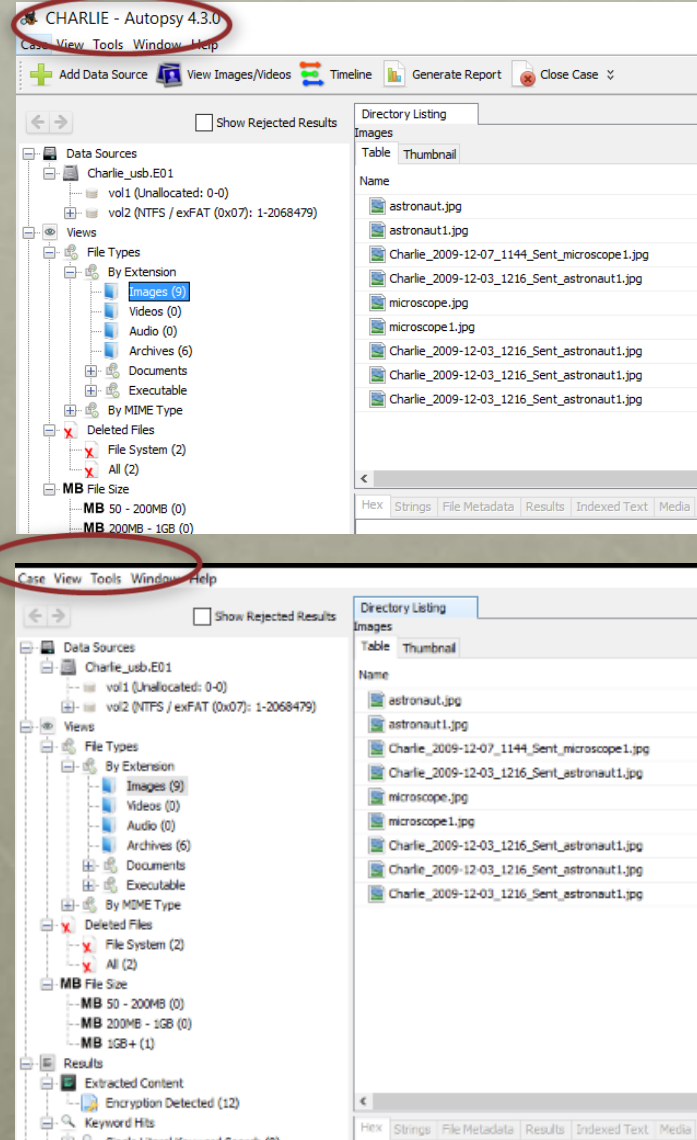
Pages: < > Go to Page: Images: 1-9

Small Thumbnails



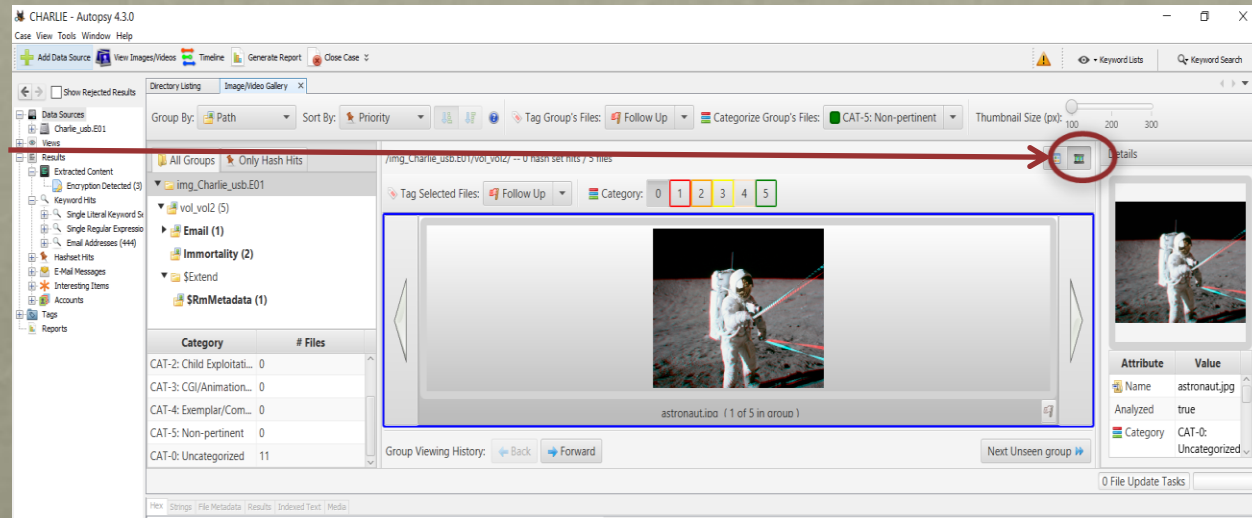
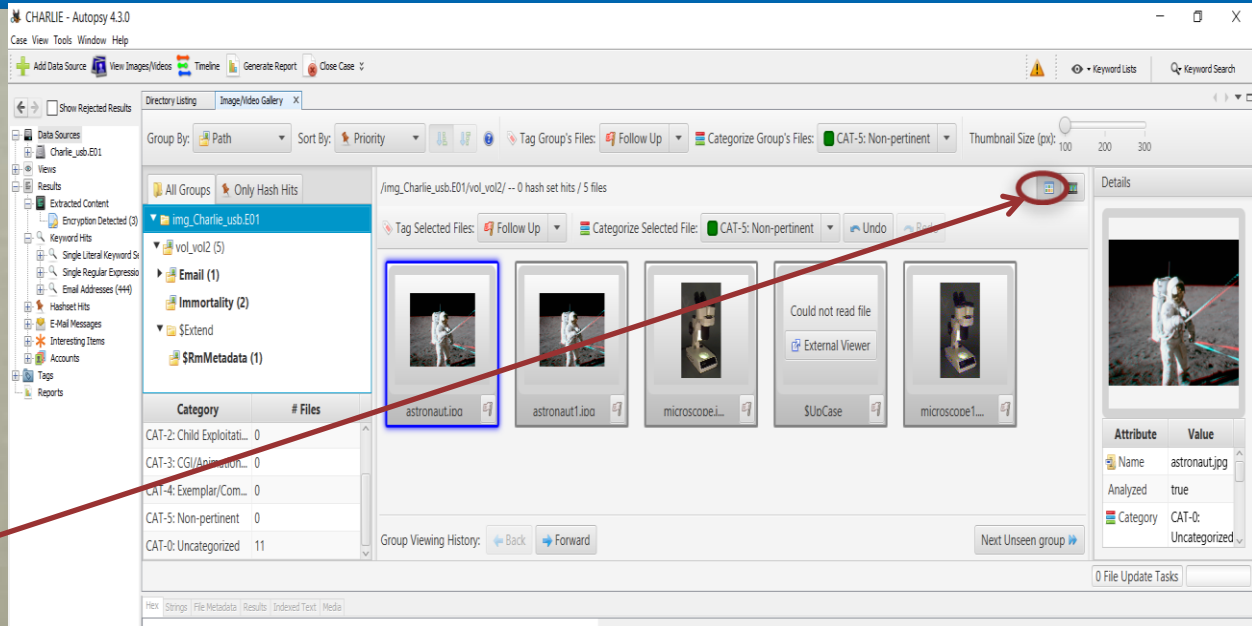
FULL SCREEN

- Go to **View** → **Full Screen**
- Full screen does not show the case name and version



VIEW IMAGES/VIDEOS

- Go to **Tools** → **View Images/Videos**
- Click **Photo Gallery**
- Click **Filmstrip**



VIEW IMAGES/VIDEOS IN HEX VIEW

- The header for the .JPG image is JFIF
- The .JPG image is viewed in HEX view

The screenshot shows the CHARLIE - Autopsy 4.3.0 interface. The left sidebar displays a tree view of data sources and file types. The main window shows a directory listing of images, with the file 'Charlie_2009-12-07_1144_Sent_microscope1.jpg' selected. The bottom pane shows the hex view of the selected file, with the 'JFIF' header circled in red. A red arrow points from the text 'The header for the .JPG image is JFIF' to the 'JFIF' header in the hex view. Another red arrow points from the text 'The .JPG image is viewed in HEX view' to the hex view pane.

Name	Location
astronaut.jpg	/img_Charlie_usb.E01/vol2/astronaut.jpg
astronaut1.jpg	/img_Charlie_usb.E01/vol2/astronaut1.jpg
Charlie_2009-12-07_1144_Sent_microscope1.jpg	/img_Charlie_usb.E01/vol2/Email/other/Charlie_2009-1
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol2/Email/Charlie_2009-12-03_
microscope.jpg	/img_Charlie_usb.E01/vol2/microscope.jpg
microscope1.jpg	/img_Charlie_usb.E01/vol2/microscope1.jpg
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol2/Email/Charlie_Email.zip/Cha
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol2/Email/Charlie_Email.zip/Cha
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol2/Email/Charlie_Email.zip/Cha

```
0x00000000: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 90 .....JFIF.....
0x00000010: 00 90 00 00 FF DB 00 43 0E 01 01 01 01 01 01 01 .....C.....
0x00000020: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
0x00000030: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
0x00000040: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
0x00000050: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....C.....
0x00000060: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
0x00000070: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
0x00000080: 70 61 73 78 77 6F 72 64 3D 69 6D 6F 72 74 61 .....password=immorta
0x00000090: 6C 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....1.....
0x000000a0: 00 11 08 02 65 01 73 03 01 22 00 02 11 01 09 11 .....e.s.....
0x000000b0: 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 01 .....
0x000000c0: 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 .....
0x000000d0: 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 .....
0x000000e0: 05 04 04 00 00 01 7D 01 02 03 04 00 11 05 12 21 .....}.....!
0x000000f0: 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 .....1A.Qa."q.2...#
0x00000100: 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 11 .....B...R..$3br...
0x00000110: 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A .....%*( )+456789:
0x00000120: 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A .....CDEF GHIJSTUVWXYZ
0x00000130: 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A .....cdefghijstuvwxyz
0x00000140: 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 .....
0x00000150: 9A A2 A3 A4 A5 A6 A7 A9 A9 A8 B2 B3 B4 B5 B6 B7 .....
0x00000160: B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 .....
0x00000170: D6 D7 D8 D9 DA DB DC E2 E3 E4 E5 E6 E7 E8 E9 EA F .....
0x00000180: F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 00 .....
0x00000190: 02 03 04 05 06 07 08 09 0A 0B FF C4 00 B5 11 00 .....
0x000001a0: 02 01 02 04 04 06 07 08 09 0A 0B FF C4 00 B5 11 00 .....
0x000001b0: 01 02 03 11 04 05 21 31 06 12 41 51 07 61 71 13 .....11.AQ.aq.....
0x000001c0: 22 32 41 08 14 02 91 A1 B1 C1 09 23 33 52 10 15 .....*2..B...$3R...
0x000001d0: 62 72 01 0A 16 24 34 A1 25 F1 17 18 19 1E 1D 26 27 .....br...$4...$*
0x000001e0: 28 29 2A 35 36 37 38 39 3A 43 44 45 46 47 48 49 .....()*+56789:CDEF GHI
0x000001f0: 4A 53 54 55 56 57 58 59 5A 63 64 65 66 67 68 69 .....JSTUVWXYZcdefghi
0x00000200: 6A 73 74 75 76 77 78 79 7A 82 83 84 85 86 87 88 .....jstuvwxyz.....
0x00000210: 89 9A 92 93 94 95 96 97 98 99 9A 9B A2 A3 A4 A5 A6 .....
0x00000220: A7 A8 A9 AA AB B2 B3 B4 B5 B6 B7 B8 B9 BA CB C3 C4 .....
0x00000230: C5 C6 C7 C8 C9 CA D2 D3 D4 D5 D6 D7 D8 D9 DA DB .....
0x00000240: E3 E4 E5 E6 E7 E8 E9 EA EB EC ED E4 F4 F5 F6 F7 F8 F9 .....
0x00000250: FA FF DA 00 00 00 00 00 02 11 03 11 00 3F 00 FE .....?.....
```


VIEW IMAGES/VIDEOS IN FILE METADATA VIEW

- The **.JPG** image is viewed in File Metadata view
- The Date/Time and MD5 of this **.JPG** image is shown here

The screenshot shows the Autopsy 4.3.0 interface. The left pane displays the file tree with 'Data Sources' expanded to 'Charlie_usb.E01' and 'Views' expanded to 'File Types' and 'Images (9)'. The 'Results' pane shows 'Extracted Content' with 'Encryption Detected (12)' and 'Keyword Hits' with 'Single Literal Keyword Search (6)'. The 'File Metadata' view is active, showing a table of files. The file 'Charlie_2009-12-07_1144_Sent_microscope1.jpg' is selected and highlighted with a red box. The 'File Metadata' view shows the following details for this file:

Name	Location	Modified Time
astronaut.jpg	/img_Charlie_usb.E01/vol_vol2/astronaut.jpg	2009-11-24 13:33:33 PST
astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2/astronaut1.jpg	2009-11-24 13:43:42 PST
Charlie_2009-12-07_1144_Sent_microscope1.jpg	/img_Charlie_usb.E01/vol_vol2/Email/other/Charlie_2009-1...	2009-12-10 14:29:38 PST
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-12-03_...	2009-12-04 12:50:24 PST
microscope.jpg	/img_Charlie_usb.E01/vol_vol2/microscope.jpg	2009-11-24 13:27:51 PST
microscope1.jpg	/img_Charlie_usb.E01/vol_vol2/microscope1.jpg	2009-11-24 14:19:21 PST
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Cha...	2009-12-04 12:50:26 PST
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Cha...	2009-12-04 12:50:26 PST
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Cha...	2009-12-04 12:50:26 PST

The 'File Metadata' view shows the following details for the selected file:

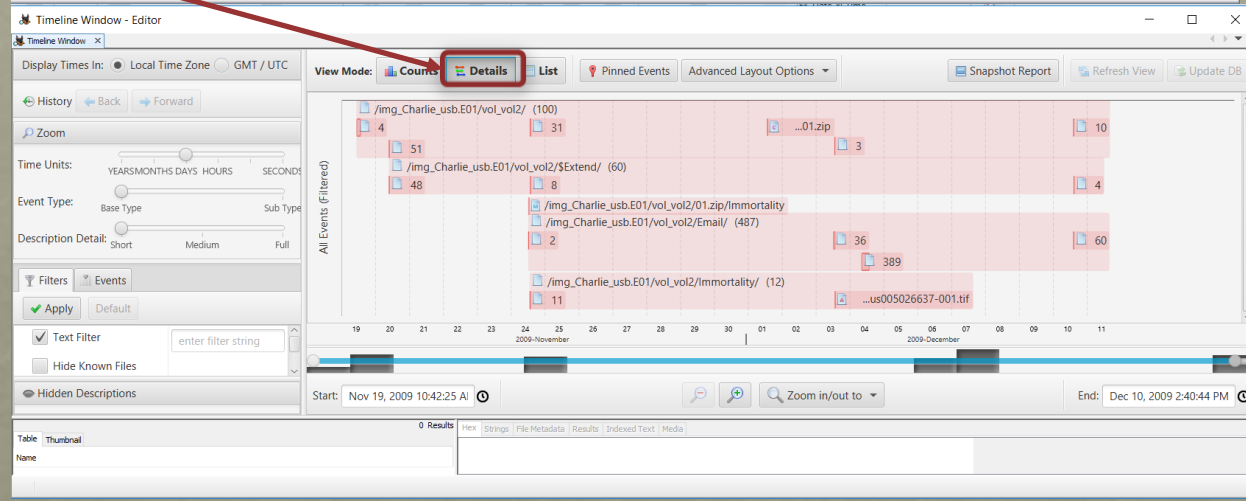
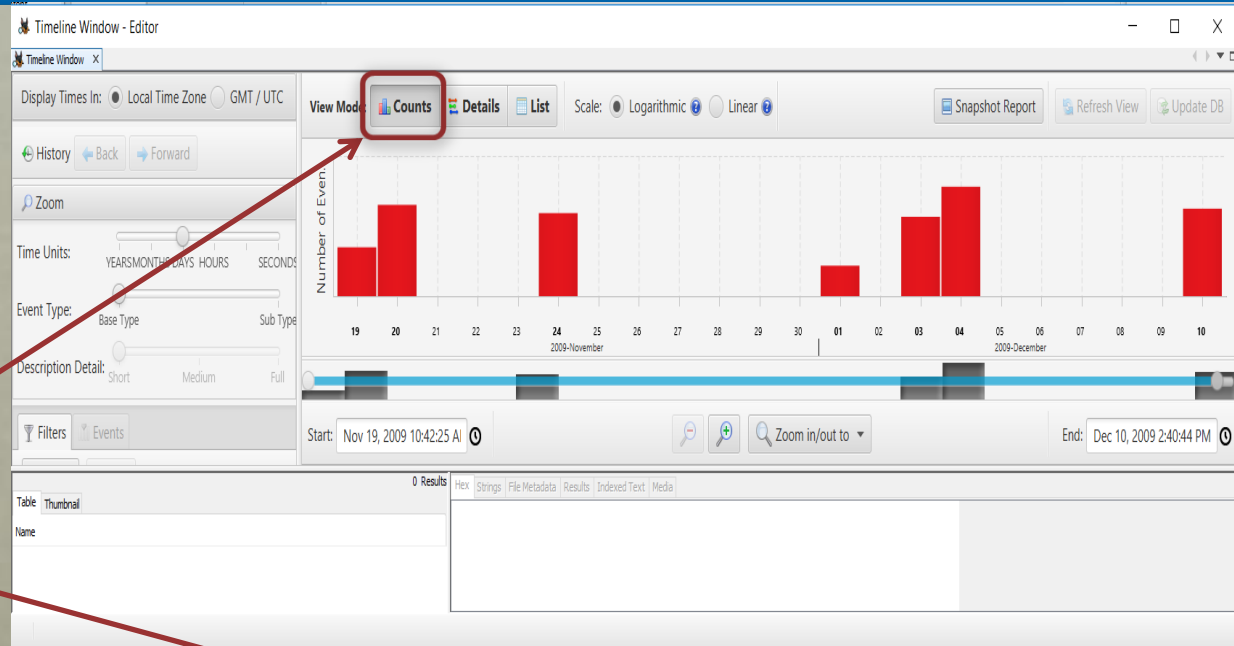
Property	Value
Name	/img_Charlie_usb.E01/vol_vol2/Email/other/Charlie_2009-12-07_1144_Sent_microscope1.jpg
Type	File System
MIME Type	image/jpeg
Size	136274
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2009-12-10 14:29:38 PST
Accessed	2009-12-10 14:29:38 PST
Created	2009-12-10 14:29:37 PST
Changed	2009-12-10 14:37:59 PST
MD5	4be2c4abb48c4389ca798e6c21736ea1

The 'Hash Lookup Results' section shows 'UNKNOWN'. The 'Internal ID' is 175. The 'From The Sleuth Kit istat Tool:' section shows the following values:

```
MFT Entry Header Values:  
Entry: 141 Sequence: 2  
$LogFile Sequence Number: 17838836  
Allocated File  
Links: 2  
$STANDARD_INFORMATION Attribute Values:  
Flags: Archive  
Owner ID: 0  
Security ID: 261 ()  
Last User Journal Update Sequence Number: 108912  
Created: 2009-12-10 14:29:37.796875000 (Pacific Standard Time)  
File Modified: 2009-12-10 14:29:38.390625000 (Pacific Standard Time)
```

TIMELINE

- Go to Tools → Timeline
- Counts View
- Details View



TIMELINE (CONT)

- List View shows 346 Events

The screenshot displays the 'Timeline Window - Editor' interface. The 'View Mode' is set to 'List', which is highlighted with a red box. A red arrow points from the text 'List View shows 346 Events' to this 'List' button. Another red arrow points from the same text to a badge in the top right corner of the event table that reads '346 events'. The table below shows a list of events with columns for Date/Time, Event Type, Description, Known, Tagged, and Hash Hit. The 'Event Type' column includes icons for File System, Web Activity, and Misc Types. The 'Description' column contains file paths and email-related text. The 'Known' column is mostly 'unknown'. The 'Tagged' and 'Hash Hit' columns are empty.

Date/Time	Event Type	Description	Known	Tagged	Hash Hit
2009-11-24 14:19:21	M_C_	/img_Charlie_usb.E01/vol_vol2/microscope1.jpg	unknown		
2009-11-24 14:19:24	_A_	/img_Charlie_usb.E01/vol_vol2/microscope1.jpg	unknown		
2009-12-01 13:18:30	_C_	/img_Charlie_usb.E01/vol_vol2/01.zip	unknown		
2009-12-03 12:19:14	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1102_Received.txt	unknown		
2009-12-03 12:19:28	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1122_Received.txt	unknown		
2009-12-03 12:19:44	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1338_Received.txt	unknown		
2009-12-03 12:19:56	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1433_Received.txt	unknown		
2009-12-03 12:20:12	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1553_Received.txt	unknown		
2009-12-03 12:20:26	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-17_0845_Received.txt	unknown		
2009-12-03 12:20:38	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-17_1030_Received.txt	unknown		
2009-12-03 12:21:10	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-17_1039_Received.txt	unknown		
2009-12-03 12:21:24	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-17_1040_Received.txt	unknown		
2009-12-03 12:21:42	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-17_1033_Received.txt	unknown		
2009-12-03 13:16:47	_A_	/img_Charlie_usb.E01/vol_vol2/Immortality/us005026637-001.tif	unknown		
2009-12-03 13:16:59	_B_	/img_Charlie_usb.E01/vol_vol2/Email	unknown		
2009-12-03 13:17:01	M_C_	/img_Charlie_usb.E01/vol_vol2/	unknown		
2009-12-03 13:19:12	M_B_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-16_1102_Received.txt	unknown		
2009-12-03 13:19:27	M_B_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-16_1122_Received.txt	unknown		
2009-12-03 13:19:43	MA_B	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-16_1338_Received.txt	unknown		
2009-12-03 13:19:55	MA_B	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-16_1433_Received.txt	unknown		
2009-12-03 13:20:10	MA_B	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-16_1553_Received.txt	unknown		
2009-12-03 13:20:25	_B_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-17_0845_Received.txt	unknown		
2009-12-03 13:20:26	MA_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-17_0845_Received.txt	unknown		
2009-12-03 13:20:27	M_B_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-17_1030_Received.txt	unknown		

SNAPSHOT REPORT

- Click **Snapshot** button
- Click **Open Report** button to see the Summary

The screenshot shows the 'Timeline Window - Editor' interface. The 'View Mode' is set to 'Counts'. A red circle highlights the 'Snapshot Report' button in the top right corner. A red arrow points from this button to the 'Open Report' button in the second screenshot.

Date/Time	Event Type	Description
2009-11-24 14:19:21	M_C_	/img_Charlie_usb.E01/vol_vol2/microscope1.jpg
2009-11-24 14:19:24	_A_	/img_Charlie_usb.E01/vol_vol2/microscope1.jpg
2009-12-01 13:18:30	_C_	/img_Charlie_usb.E01/vol_vol2/01.zip
2009-12-03 12:19:14	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1338_Received.txt
2009-12-03 12:19:28	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1338_Received.txt
2009-12-03 12:19:44	M_	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Charlie_2009-11-16_1338_Received.txt

The screenshot shows the 'Timeline Window - Editor' interface with a 'Success' dialog box open. The dialog box contains the text 'Report saved at' followed by a file path. A red circle highlights the 'Open Report' button in the dialog box. A red arrow points from the 'Open Report' button in the first screenshot to this button.

Success

Report saved at
D:\CHARLIE\Reports\CHARLIE Timeline Snapshot Report\Timeline Snapshot Index.html

Open Report OK

SNAPSHOT REPORT (CONT)

- This is a Timeline Snapshot Report Summary

The screenshot shows a web browser window displaying the 'Autopsy Forensic Report: CHARLIE Timeline Snapshot Report'. The page title is 'Autopsy Forensic Report: CHARLIE Timeline Snapshot Report' and it was generated on 2017/03/25 19:38:34. The report details include:

- Case: CHARLIE
- Case Number: No case number
- Examiner: Nhan Nguyen
- Number of Images: 1

Image Information:

- Image Name: Charlie_usb.E01
- Timezone: America/Los_Angeles
- Path: D:\Thumb Drives\Charlie_usb.E01

A cartoon illustration of a dog is shown below the image information. The footer of the report states: 'Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org'.

The screenshot shows the 'Timeline Snapshot' section of the report. It displays a table with columns for Date/Time, Event Type, Description, Action, Tagged, and Hash (MD5). The table contains several entries, including file system events like File Modified, File Accessed, File Created, and File Changed, as well as Web Activity and Misc Types.

Time Range: Thursday, November 19, 2009 10:42:25 AM -08:00 to Thursday, December 10, 2009 2:40:44 PM -08:00

Description Level of Detail: Short

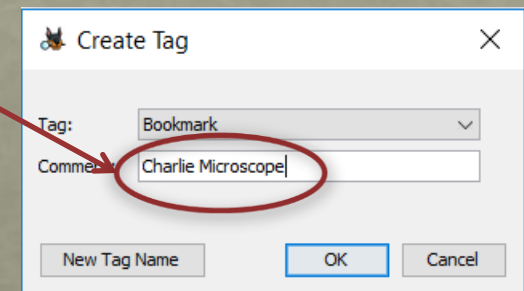
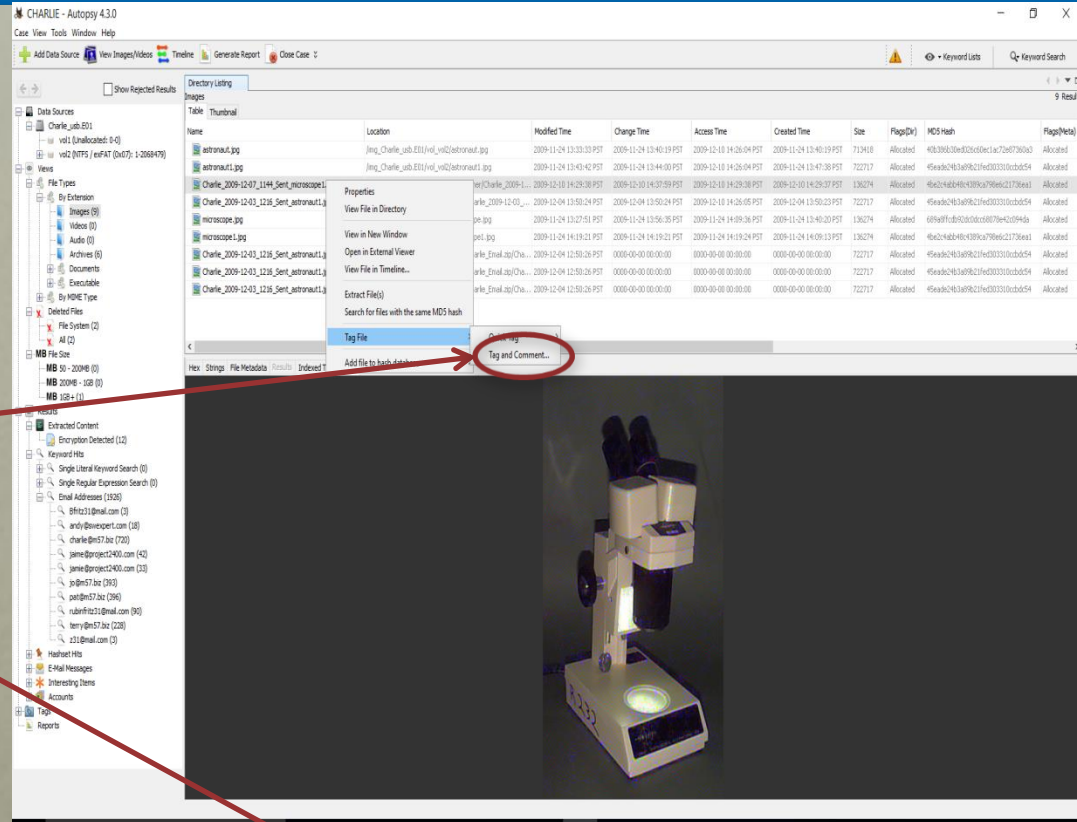
Event Type Zoom Level: Basic Type

- text = "" [x]
- Hide Known Files []
- Data Source [x]
 - Charlie_usb.E01 [x]
- Tags []
- Hash Sets []
- Event Type [x]
 - File System [x]
 - File Modified [x]
 - File Accessed [x]
 - File Created [x]
 - File Changed [x]
 - Web Activity [x]
 - Web Downloads [x]
 - Web Cookies [x]
 - Web Bookmarks [x]
 - Web History [x]
 - Web Searches [x]
 - Misc Types [x]
 - Messages [x]
 - GPS Routes [x]
 - Location History [x]
 - Calls [x]
 - Email [x]
 - Recent Documents [x]
 - Installed Programs [x]
 - Exit [x]
 - Devices Attached [x]

Filters:

MANUAL ANALYSIS

- **Bookmark Relevant Files**
- **Right Click** on the file the go to **Tag File** → **Tag and Comment**
- Name the Bookmark file is **Charlie Microscope**



MANUAL ANALYSIS (CONT)

- The Tag in the Tree Viewer now has one item
- Name the Bookmark file is **Charlie Microscope**

The screenshot displays the CHARLIE - Autopsy 4.3.0 interface. The left sidebar shows a tree view with a 'bookmark (1)' tag circled in red. The main window shows a table of search results for 'Charlie Microscope'. The table has columns for File Path, Comment, Modified Time, Changed Time, Accessed Time, Created Time, and Size. The first row shows a file named 'Charlie_2009-12-07_1144_Sent_microscope1.jpg' with a comment of 'Charlie Microscope'. Below the table, a preview of a microscope is visible.

File	File Path	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size
Charlie_2009-12-07_1144_Sent_microscope1.jpg	/img_Charlie_usb.E01/vol_vol2/Email/other/Charlie_2009-12-07_1144_Sent_microscope1.jpg	Charlie Microscope	2009-12-10 14:29:38 PST	2009-12-10 14:37:59 PST	2009-12-10 14:29:38 PST	2009-12-10 14:29:37 PST	136274

MANUAL ANALYSIS (CONT)

- Keyword search for “Time Machine”
- There are a total of 6 hits

CHARLIE - Autopsy 4.3.0

Case View Tools Window Help

Show Rejected Results

 Keyword Lists

Directory Listing
 Keyword search 1 - Time Machine

Exact Match
 Substring Match
 Regular Expression

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	...
Nitroba work.odt	/img_Charlie_usb.E01/vol_vol2/Nitroba work.odt	2009-11-19 13:26:42 PST	2009-11-19 13:27:44 PST	2009-11-24 13:55:08 PST	2009-11-24 13:55:08 PST	10906	Allocated
Charlie_2009-11-17_1033_Received.txt	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Cha...	2009-12-03 12:21:42 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	650	Allocated
Charlie_2009-11-18_0939_Received.txt	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-18...	2009-12-04 09:20:52 PST	2009-12-04 09:20:52 PST	2009-12-04 09:20:52 PST	2009-12-04 09:20:52 PST	3215	Allocated
Charlie_2009-11-17_1033_Received.txt	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Cha...	2009-12-03 12:21:42 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	650	Allocated
Charlie_2009-11-17_1033_Received.txt	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_2009-11-17...	2009-12-03 13:21:40 PST	2009-12-04 09:14:21 PST	2009-12-04 13:47:41 PST	2009-12-03 13:21:40 PST	650	Allocated
Charlie_2009-11-17_1033_Received.txt	/img_Charlie_usb.E01/vol_vol2/Email/Charlie_Email.zip/Cha...	2009-12-03 12:21:42 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	650	Allocated

Hex
 Strings
 File Metadata
 Results
 Indexed Text
 Media

Matches on page: 1 of 2 Match Page: 1 of 2

teleporter patent search. Charlie, I want you to take the **time machine** =
 patent search. This is our first real job, so let's make sure we do =
 some quality research. Our reputation will depend on the time and
 effort that we put into this contract and on Nitroba's satisfaction with =
 our results. Come by my office and we'll talk details.
 -----NextPart_000_0019_01CA6771.6D4193A0
 Content-Type: text/html;
 charset="iso-8859-1"
 Content-Transfer-Encoding: quoted-printable
 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
 <HTML><HEAD>
 <META content=3D"text/html; charset=3Diso-8859-1" =
 http-equiv=3DContent-Type
 <META name=3DGENERATOR content=3D"MSHTML 8.00.6001.18852">
 </STYLE></STYLE>
 </HEAD>
 <BODY bgcolor=3D#ffffff>
 <DIV style=3Dfont-size: 12pt; font-family: Arial; font-weight: normal;>
 <DIV style=3Dfont-size: 12pt; font-family: Arial; font-weight: normal;>
 <DIV style=3Dfont-size: 12pt; font-family: Arial; font-weight: normal;>
 Nitroba wants us=20
 to investigate the teleporter patent search. Charlie, I want you =
 responsible for the teleporter patent search. Charlie, I want you =
 to take=20
 the **time machine** patent search. This is our first real job, so =
 let's make=20
 sure we do some quality research. Our reputation will depend on =
 the time=20
 and effort that we put into this contract and on Nitroba's satisfaction =
 with our=20
 results. Come by my office and we'll talk details.</DIV></DIV>
 </DIV>

REPORT GENERATION

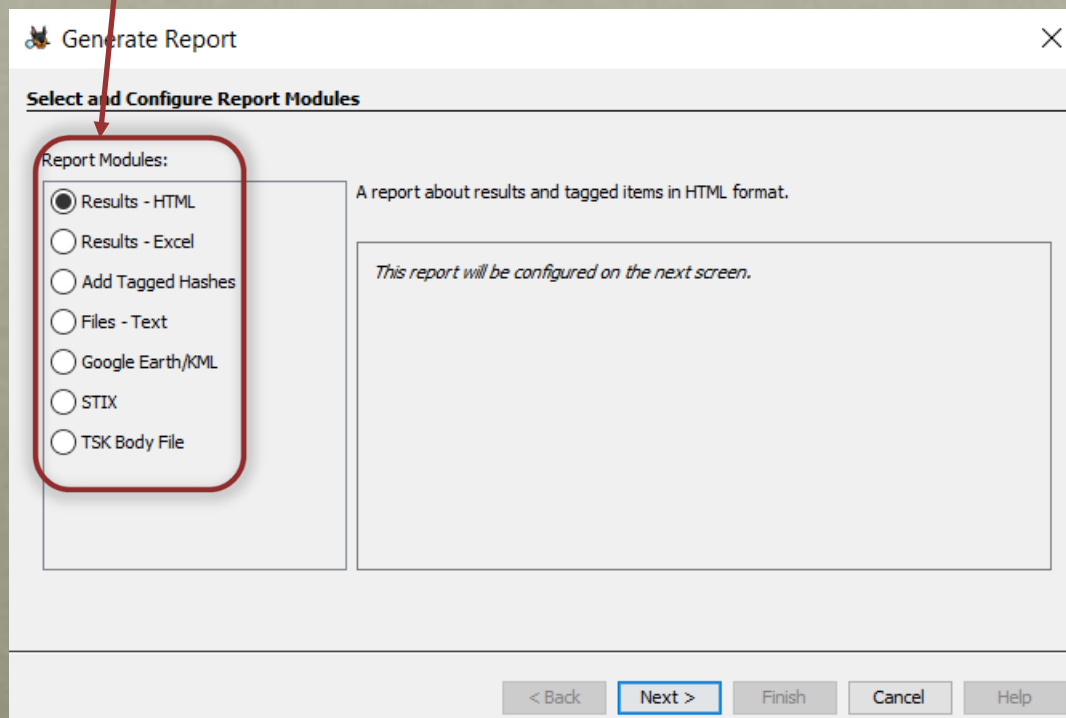
- Go to **Tools** → **Generate Report** or Click **Generate Report** Button

The screenshot shows the Autopsy 4.3.0 interface. The 'Tools' menu is open, and the 'Generate Report' option is highlighted with a red circle. A red arrow points from this menu item to the 'Generate Report' button in the top toolbar, which is also circled in red. Another red arrow points from the text 'Click Generate Report Button' to the same button. The main window displays a file gallery with several thumbnails, including 'astronaut.jpg' and 'microscope.jpg'. A table at the bottom left shows the file categories and their counts.

Category	# Files
CAT-2: Child Exploitati...	0
CAT-3: CGI/Animation...	0
CAT-4: Exemplar/Com...	0
CAT-5: Non-pertinent	0
CAT-0: Uncategorized	11

REPORT GENERATION (CONT)

- There are 6 Report Modules to choose from, but the most common are **HTML** and **Excel**



The screenshot shows a dialog box titled "Generate Report" with a close button (X) in the top right corner. Below the title bar is the section "Select and Configure Report Modules". Underneath, there is a "Report Modules:" section with a list of radio buttons. A red rounded rectangle highlights this list, and a red arrow points from the text "HTML and Excel" in the bullet point above to the "Results - HTML" option. The options are:

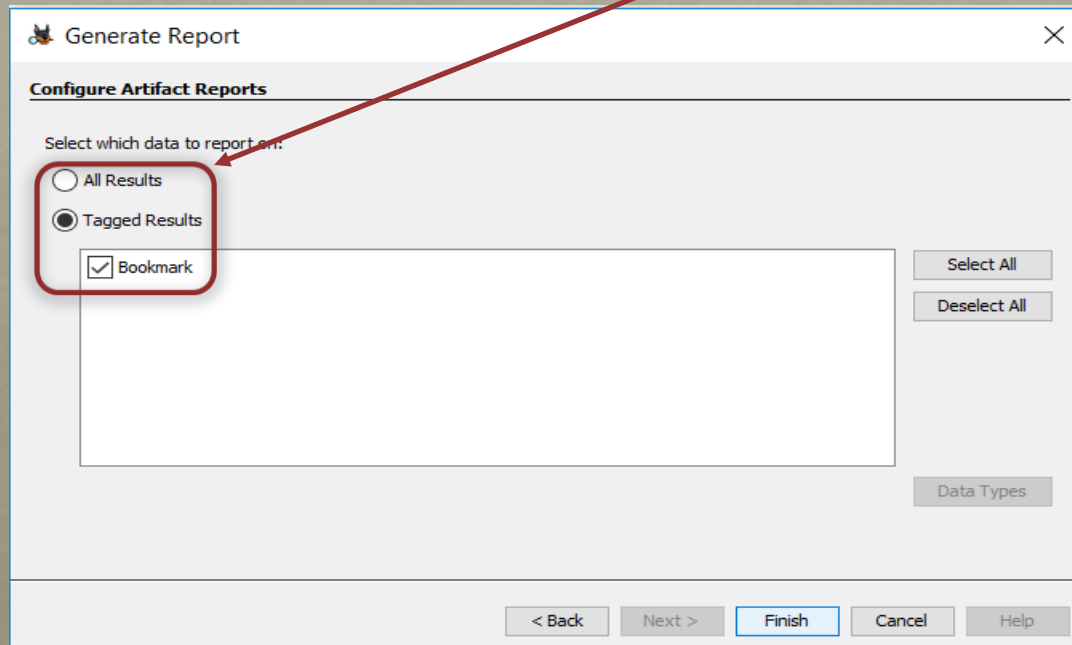
- Results - HTML
- Results - Excel
- Add Tagged Hashes
- Files - Text
- Google Earth/KML
- STIX
- TSK Body File

To the right of the list, there is a description: "A report about results and tagged items in HTML format." Below this is a text area containing the message: "This report will be configured on the next screen." At the bottom of the dialog, there are five buttons: "< Back", "Next >" (highlighted with a blue border), "Finish", "Cancel", and "Help".

REPORT GENERATION (CONT)

There are 2 options to choose include in the Report

1. All Results
2. Tagged Results



Generate Report [Close]

Configure Artifact Reports

Select which data to report on:

All Results

Tagged Results

Bookmark

Select All

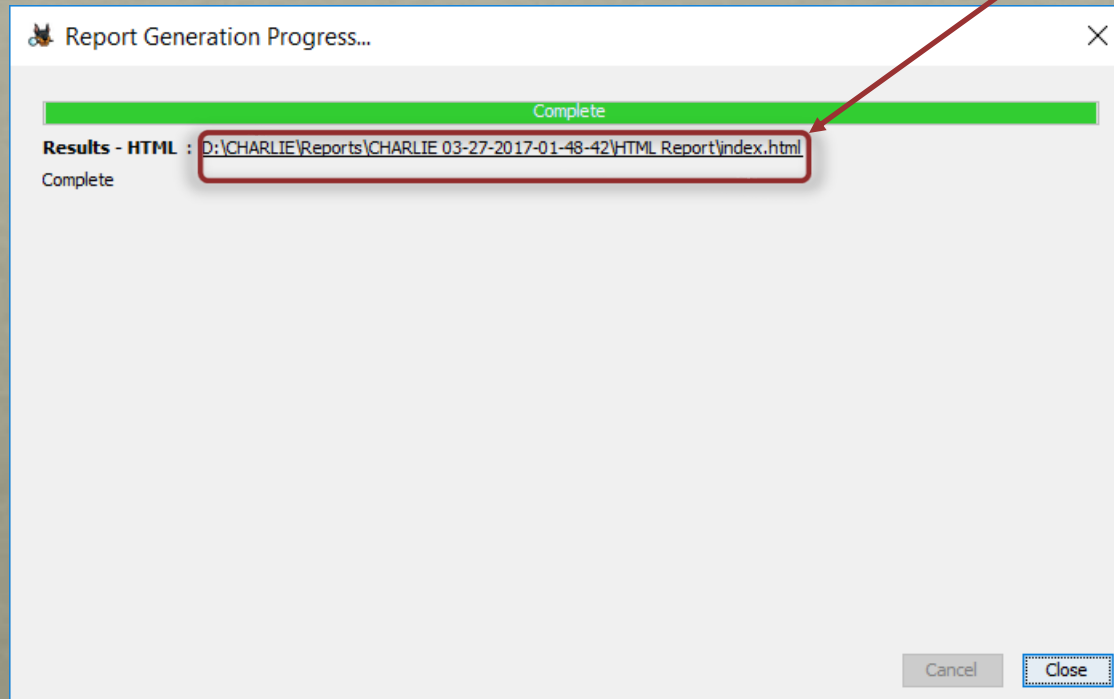
Deselect All

Data Types

< Back Next > **Finish** Cancel Help

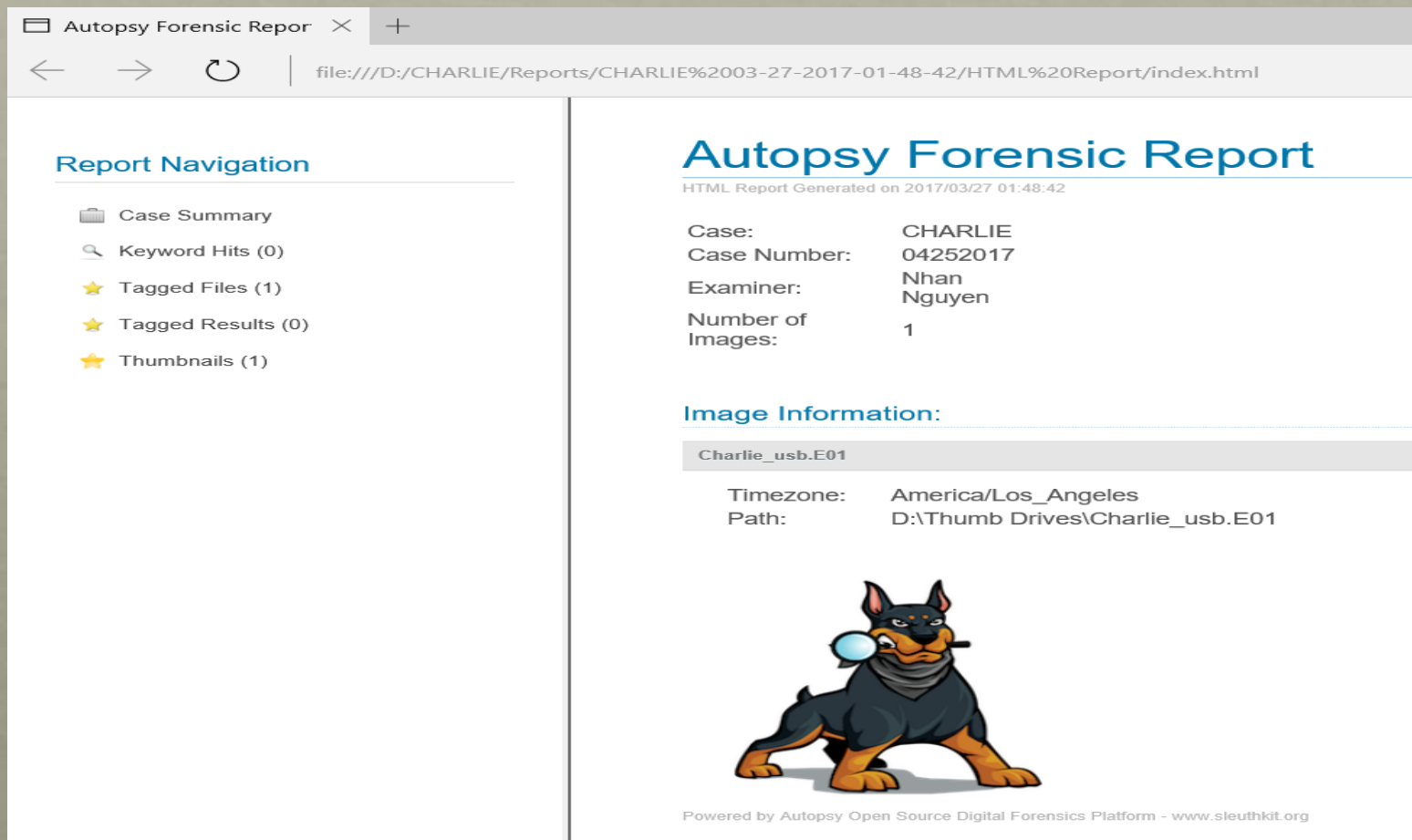
REPORT GENERATION (CONT)

- After the Report is generated, click on the link below to view the Report



REPORT GENERATION (CONT)

- This is a Autopsy Forensic Report



The screenshot shows a web browser window displaying an Autopsy Forensic Report. The browser's address bar shows the file path: file:///D:/CHARLIE/Reports/CHARLIE%2003-27-2017-01-48-42/HTML%20Report/index.html. The report page has a navigation sidebar on the left and a main content area on the right.

Report Navigation


- Case Summary
- Keyword Hits (0)
- Tagged Files (1)
- Tagged Results (0)
- Thumbnails (1)

Autopsy Forensic Report
HTML Report Generated on 2017/03/27 01:48:42

Case:	CHARLIE
Case Number:	04252017
Examiner:	Nhan Nguyen
Number of Images:	1

Image Information:

Charlie_usb.E01	
Timezone:	America/Los_Angeles
Path:	D:\Thumb Drives\Charlie_usb.E01



Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

QUESTIONS?