

HackerFrogs Afterschool

Disk Image Forensics Part 2

Class:
Digital Forensics

Workshop Number:
AS-FOR-06

Document Version:
1.75

Special Requirements:
- Registered account at
tryhackme.com



Welcome to HackerFrogs Afterschool!

This workshop is the sixth class for digital forensics.

In the last workshop, we learned about the following digital forensics concepts:



The Sleuthkit Software

The Sleuthkit is a popular program used in digital disk forensics, and it includes several useful commands for interacting with disk image files, including...



The MmLs Command

```
theshyhat-picocftf@webshell:/tmp/...theshyhat$ mmls disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-----	0000000000	0000002047	0000002048	Unallocated
002:	000:000	0000002048	0000204799	0000202752	Linux (0x83)

The MmLs command displays the media management (Mm) of a disk image file in list (Ls) format

The FsStat Command

```
theshyhat-picocftf@webshell:/tmp/...theshyhat$ fsstat -o 2048 disk.flag.img  
FILE SYSTEM INFORMATION  
-----  
File System Type: Ext4  
Volume Name:  
Volume ID: 8e023955b4e7dab7e04b7643076ccf0f
```

The FsStat command is used to display statistics (Stat) associated with a filesystem (Fs)

The Fls Command

```
theshyhat-picocftf@webshell:/tmp/...theshyhat$ fls -f ext4 -o 2048 -r disk.flag.img  
d/d 11: lost+found  
r/r 12: ldlinux.sys
```

The Fls (Filesystem Ls) command is used to list out files and directories within a specified filesystem

The lcat Command

```
theshyhat-picoctf@webshell:/tmp/...theshyhat$ lcat -f ext4 -o 360448 disk.flag.img 2371  
picoCTF{0x71_4a7b_2f2a2f2a}  
theshyhat-picoctf@webshell:/tmp/...theshyhat$ █
```

The lcat (inode cat) command is used to read specific files in a disk partition according to its inode number

This Workshop's Topics

- Digital Disk Forensics with Autopsy
- Advent of Cyber 2023: Day 24 Challenge
 - Disk Analysis & Autopsy Challenge

Autopsy Forensics Software

Autopsy is the GUI Implementation of the Sleuthkit, and it allows users to view the contents of disk image files in a much more intuitive manner

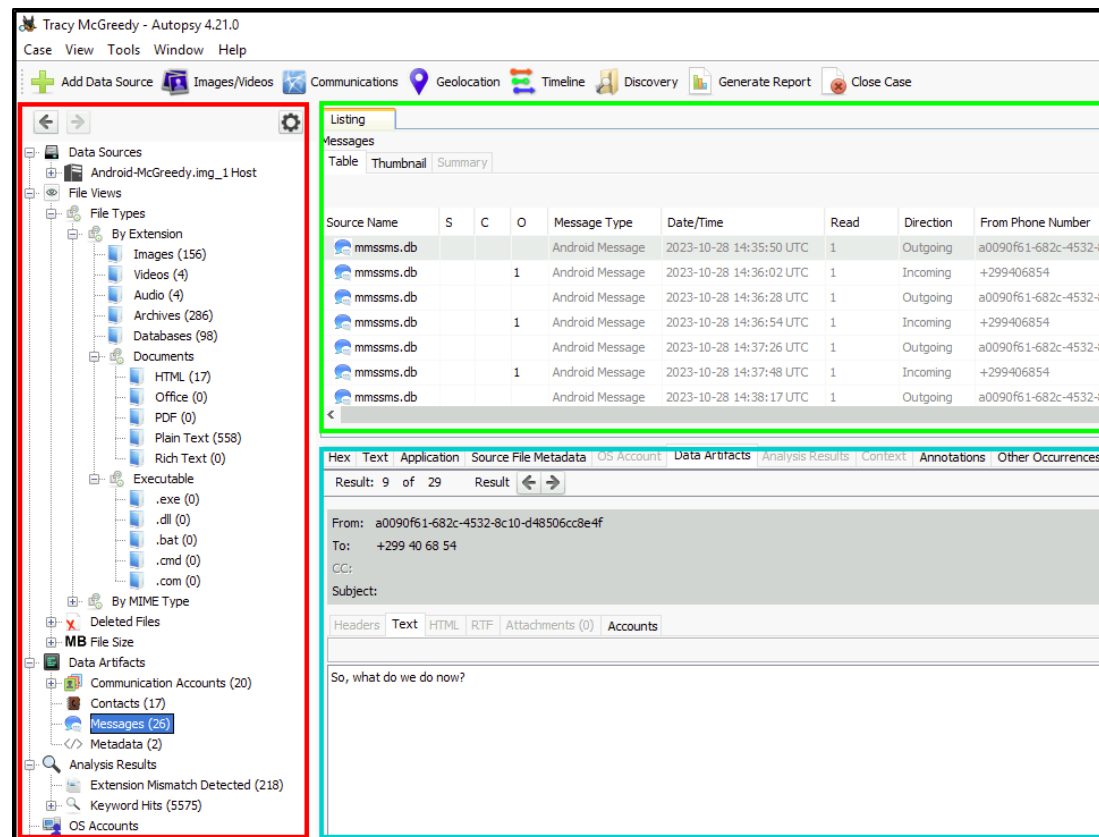


TryHackMe Advent 2023 Challenge

Let's start our look at Autopsy with an easy challenge from the TryHackMe Advent 2023 event:

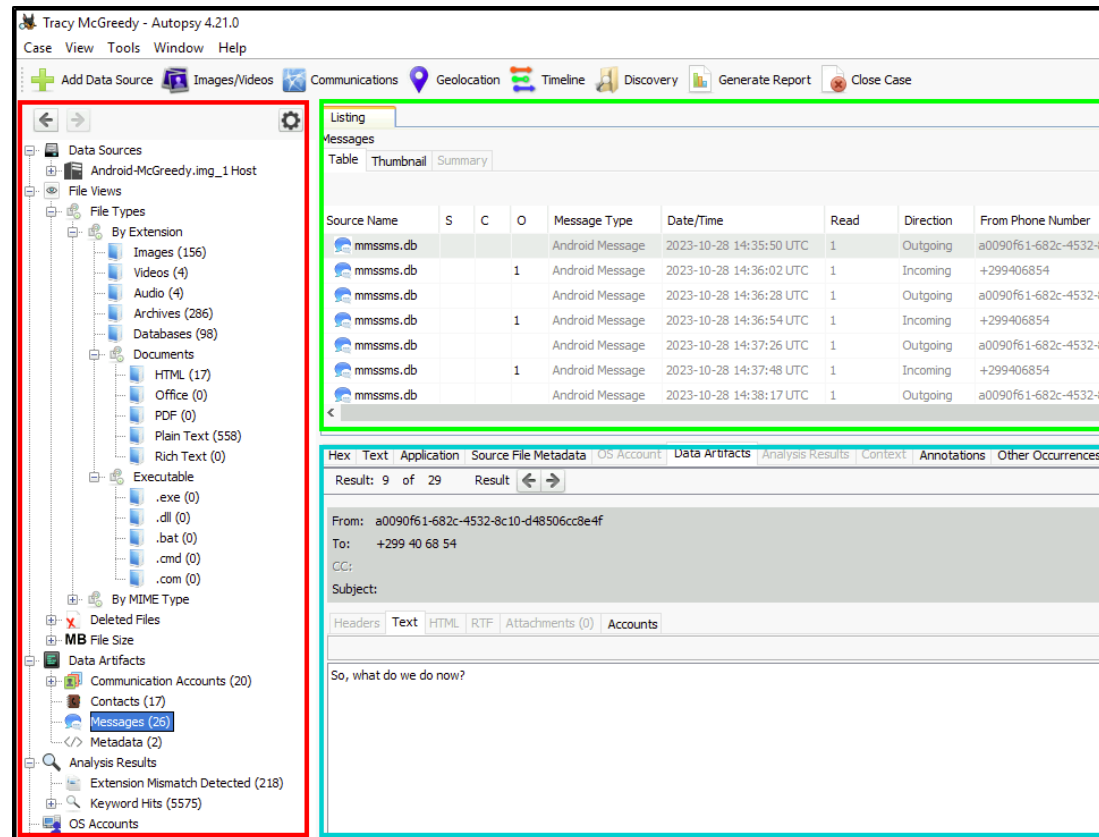
<https://tryhackme.com/room/adventofcyber2023>

Views in the Autopsy UI



There are three major views to pay attention to in Autopsy

Views in the Autopsy UI



The Tree Viewer (red)

Views in the Autopsy UI

The screenshot displays the Autopsy 4.21.0 interface. On the left, the 'Data Sources' view (outlined in red) shows a tree structure of file types and artifacts. The 'Messages' artifact is selected. On the right, the 'Results Viewer' (outlined in green) displays a table of messages and a detailed view of a selected message.

Data Sources View (Red Border):

- Data Sources
 - Android-McGreedy.img_1 Host
- File Views
 - By Extension
 - Images (156)
 - Videos (4)
 - Audio (4)
 - Archives (286)
 - Databases (98)
 - Documents
 - HTML (17)
 - Office (0)
 - PDF (0)
 - Plain Text (558)
 - Rich Text (0)
 - Executable
 - .exe (0)
 - .dll (0)
 - .bat (0)
 - .cmd (0)
 - .com (0)
 - By MIME Type
 - Deleted Files
 - MB File Size
- Data Artifacts
 - Communication Accounts (20)
 - Contacts (17)
 - Messages (26)
 - Metadata (2)
- Analysis Results
 - Extension Mismatch Detected (218)
 - Keyword Hits (5575)
- OS Accounts

Results Viewer (Green Border):

Listing Messages

Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number
mmssms.db				Android Message	2023-10-28 14:35:50 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f
mmssms.db			1	Android Message	2023-10-28 14:36:02 UTC	1	Incoming	+299406854
mmssms.db				Android Message	2023-10-28 14:36:28 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f
mmssms.db			1	Android Message	2023-10-28 14:36:54 UTC	1	Incoming	+299406854
mmssms.db				Android Message	2023-10-28 14:37:26 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f
mmssms.db			1	Android Message	2023-10-28 14:37:48 UTC	1	Incoming	+299406854
mmssms.db				Android Message	2023-10-28 14:38:17 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f

Result: 9 of 29

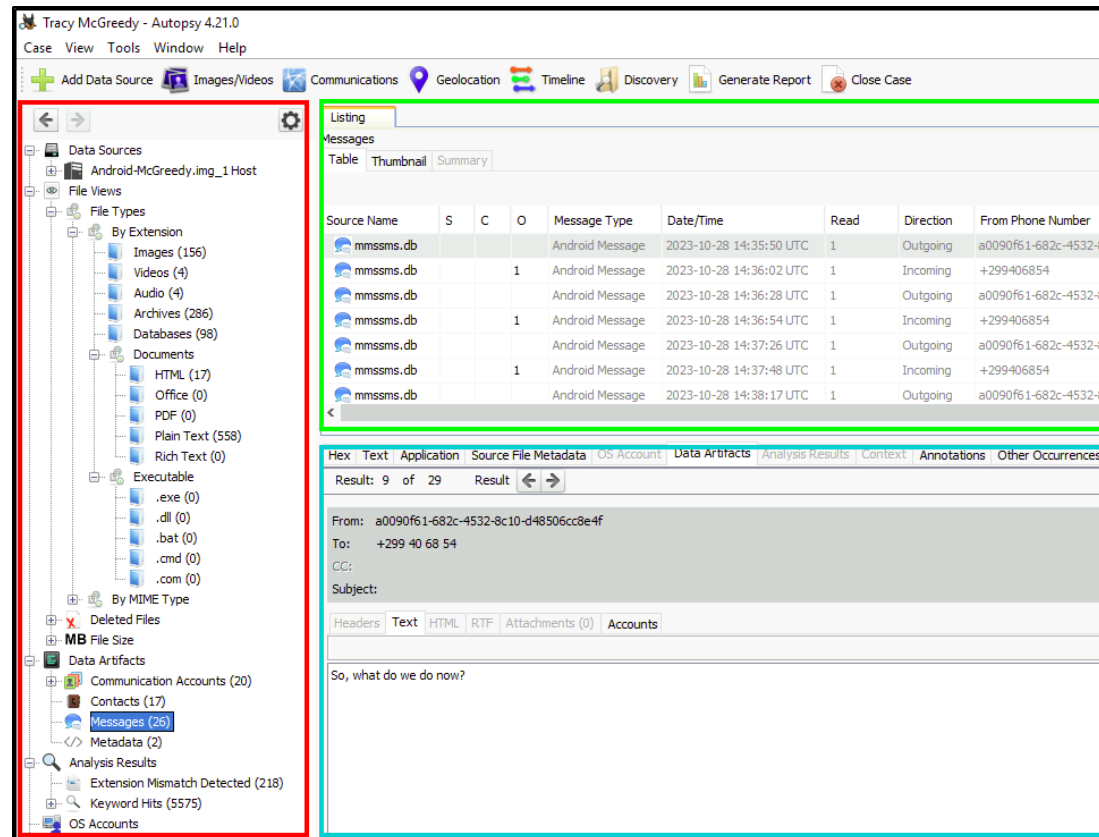
From: a0090f61-682c-4532-8c10-d48506cc8e4f
To: +299 40 68 54
CC:
Subject:

Headers Text HTML RTF Attachments (0) Accounts

So, what do we do now?

The Results Viewer (green)

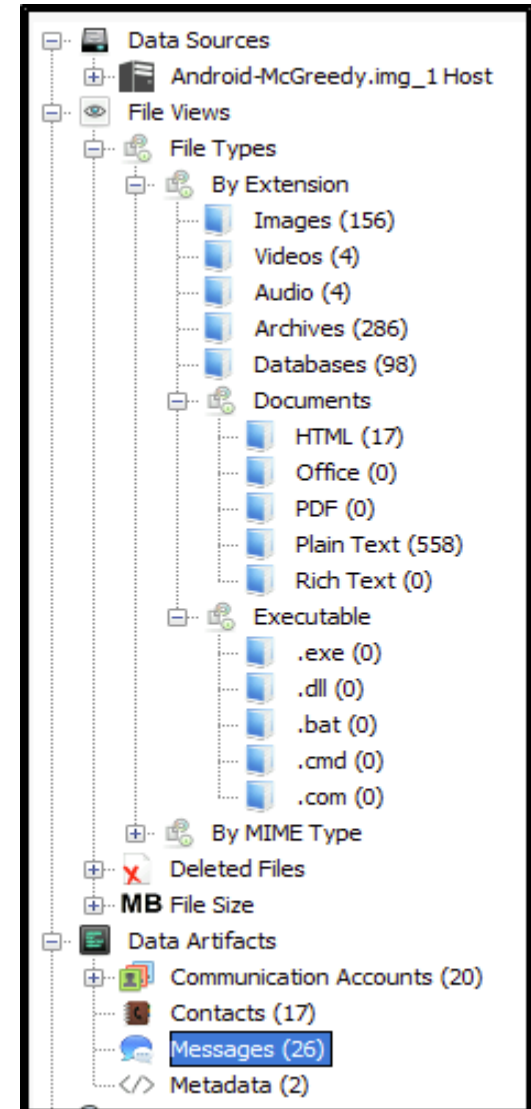
Views in the Autopsy UI










And the Contents Viewer (blue)

The Tree Viewer

The Tree Viewer is the most general view, and allows us to browse the disk image contents by directory tree or by sorted categories created by Autopsy plugins










The Results Viewer

Listing									
Messages									
Table Thumbnail Summary									
Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number	To Phone Number
 mmssms.db				Android Message	2023-10-28 14:35:50 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:02 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:36:28 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:54 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:37:26 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:37:48 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:38:17 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54

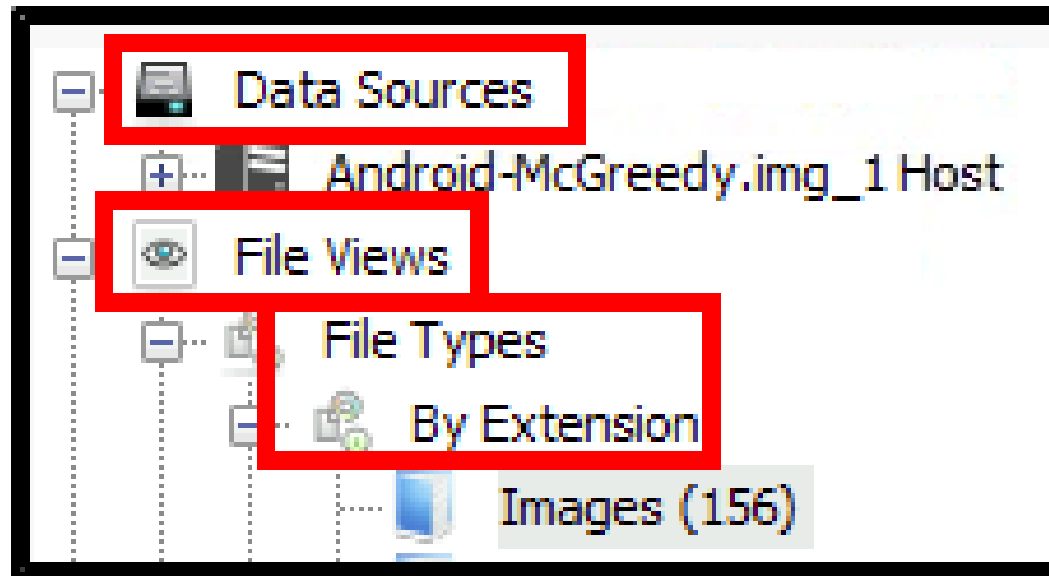
The Results Viewer is where we look after we've selected an item from the Tree Viewer, and it provides more information in a list

The Contents Viewer

Listing									
Messages									
Table Thumbnail Summary									
Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number	To Phone Number
 mmssms.db				Android Message	2023-10-28 14:35:50 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:02 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:36:28 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:54 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:37:26 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:37:48 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:38:17 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54

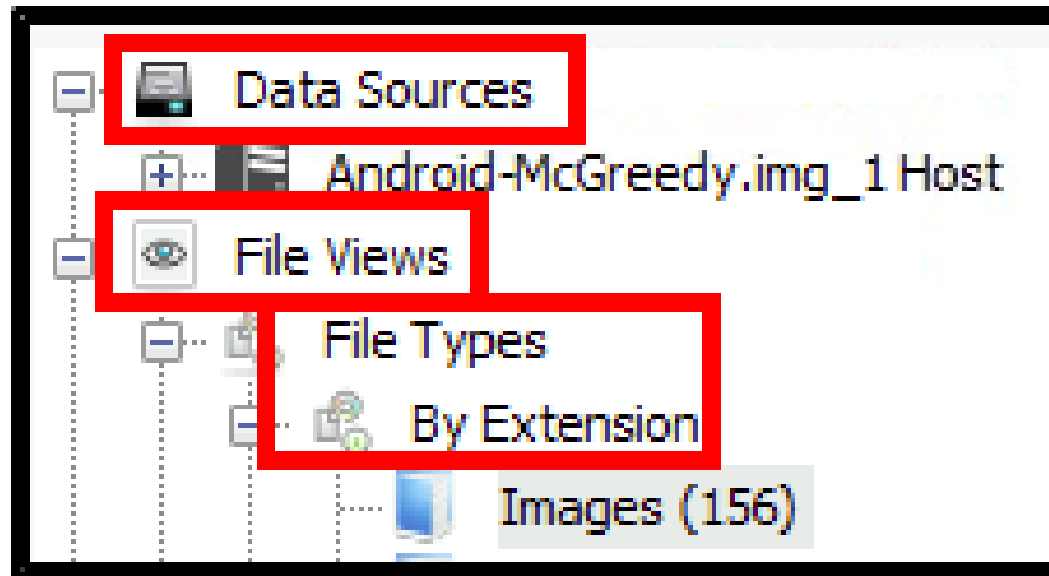
The Contents Viewer is where we can inspect individual files

Inspecting Photos



The first question from the task requires us to look at photo files

Inspecting Photos



We can access photos in Autopsy by selecting
**Data Sources -> File View -> File Types -> By
Extension -> Images**

Viewing Contacts



Next we need to check the contacts on the image

Viewing Contacts



We need to access **Data Artifacts** ->
Communication Accounts -> **Contacts**

Viewing SMS Messages



We navigate to **Data Artifacts** ->
Communication Accounts -> **Messages**

TryHackMe Disk Analysis and Autopsy

We can practice more with this next TryHackMe room

<https://tryhackme.com/room/autopsy2ze0>

Summary



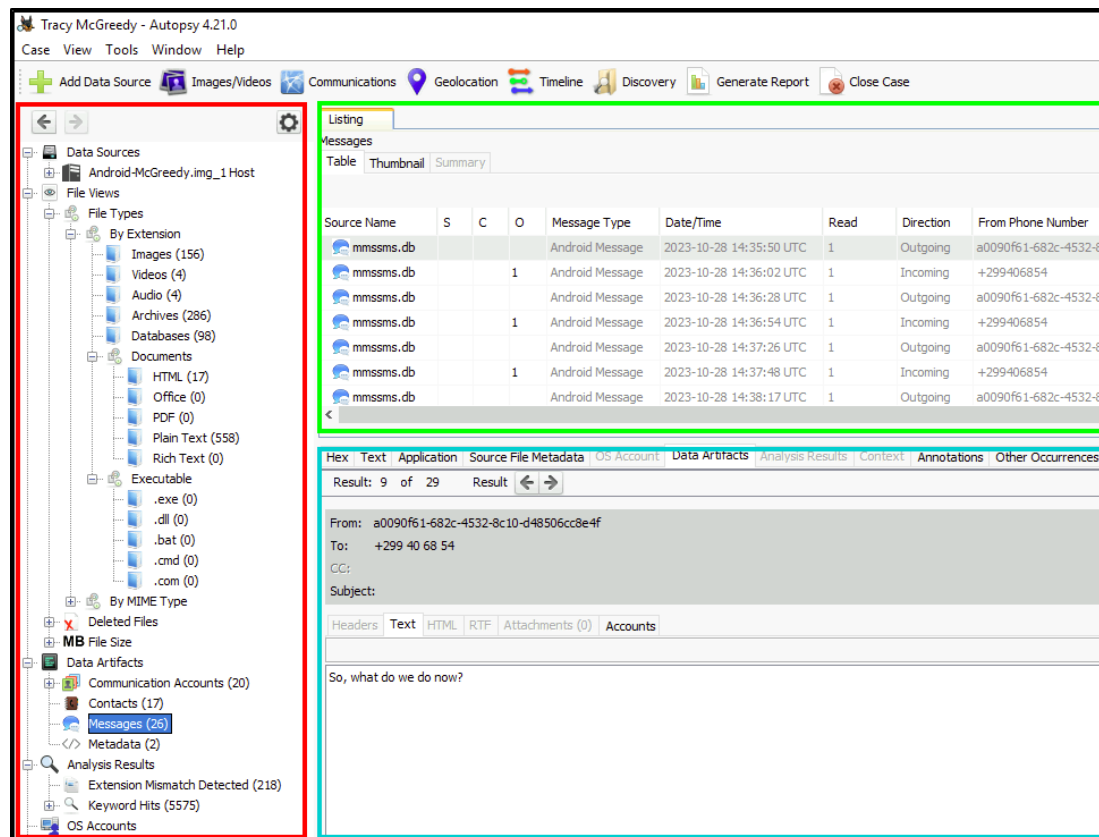
Let's review the digital forensics concepts we learned in this workshop:

Autopsy Forensics Software

Autopsy is the GUI Implementation of the Sleuthkit, and it allows users to view the contents of disk image files in a much more intuitive manner

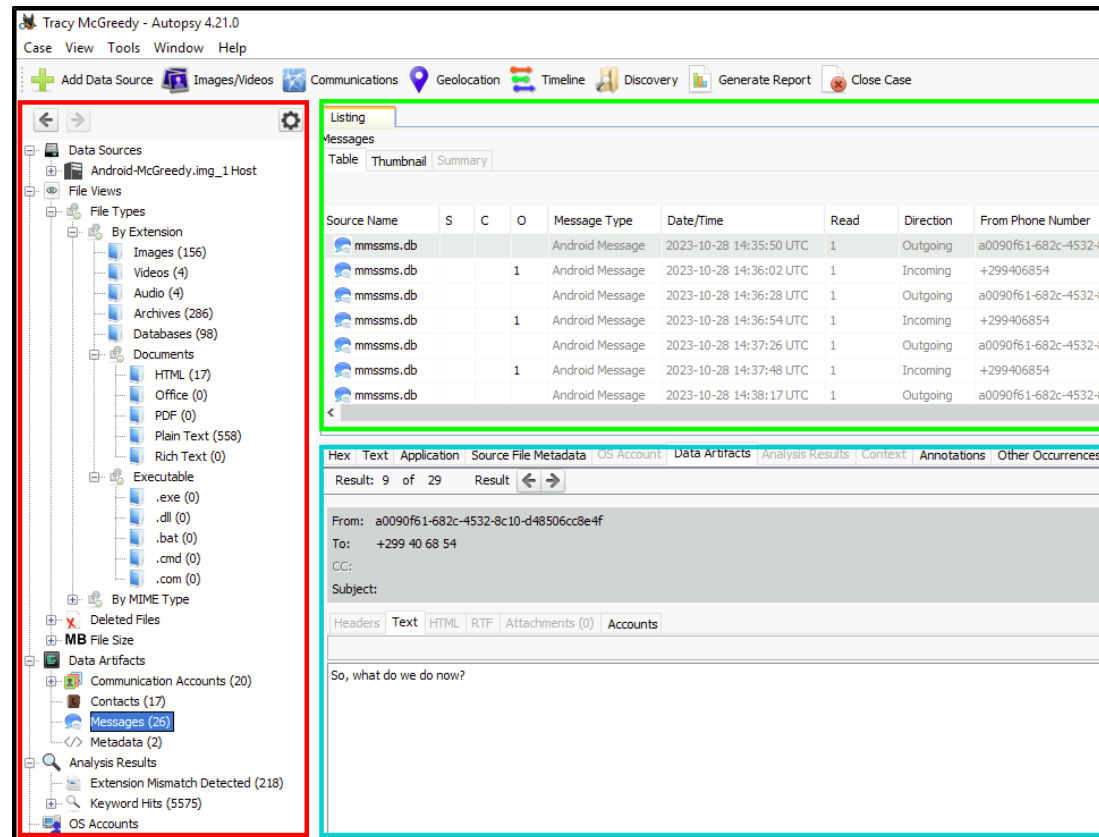


Views in the Autopsy UI



There are three major views to pay attention to in Autopsy

Views in the Autopsy UI



The Tree Viewer (red)

Views in the Autopsy UI

The screenshot displays the Autopsy 4.21.0 interface. On the left, the 'Data Sources' view (outlined in red) shows a tree structure of file types and artifacts. The 'Messages' artifact is selected. On the right, the 'Results Viewer' (outlined in green) displays a table of messages and a detailed view of a selected message.

Data Sources View (Red Border):

- Data Sources
 - Android-McGreedy.img_1 Host
- File Views
 - By Extension
 - Images (156)
 - Videos (4)
 - Audio (4)
 - Archives (286)
 - Databases (98)
 - Documents
 - HTML (17)
 - Office (0)
 - PDF (0)
 - Plain Text (558)
 - Rich Text (0)
 - Executable
 - .exe (0)
 - .dll (0)
 - .bat (0)
 - .cmd (0)
 - .com (0)
 - By MIME Type
 - Deleted Files
 - MB File Size
- Data Artifacts
 - Communication Accounts (20)
 - Contacts (17)
 - Messages (26)
 - Metadata (2)
- Analysis Results
 - Extension Mismatch Detected (218)
 - Keyword Hits (5575)
- OS Accounts

Results Viewer (Green Border):

Listing
Messages
Table Thumbnail Summary

Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number
mmssms.db				Android Message	2023-10-28 14:35:50 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f
mmssms.db			1	Android Message	2023-10-28 14:36:02 UTC	1	Incoming	+299406854
mmssms.db				Android Message	2023-10-28 14:36:28 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f
mmssms.db			1	Android Message	2023-10-28 14:36:54 UTC	1	Incoming	+299406854
mmssms.db				Android Message	2023-10-28 14:37:26 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f
mmssms.db			1	Android Message	2023-10-28 14:37:48 UTC	1	Incoming	+299406854
mmssms.db				Android Message	2023-10-28 14:38:17 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 9 of 29 Result < >

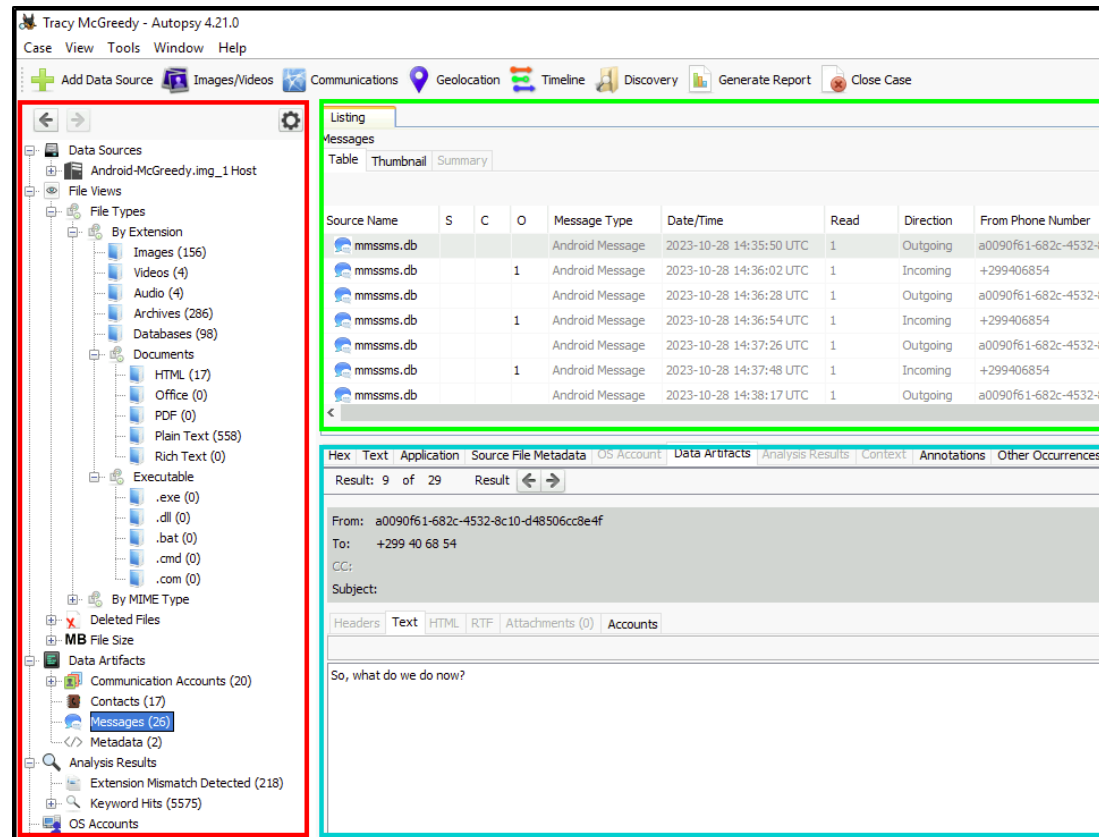
From: a0090f61-682c-4532-8c10-d48506cc8e4f
To: +299 40 68 54
CC:
Subject:

Headers Text HTML RTF Attachments (0) Accounts

So, what do we do now?

The Results Viewer (green)

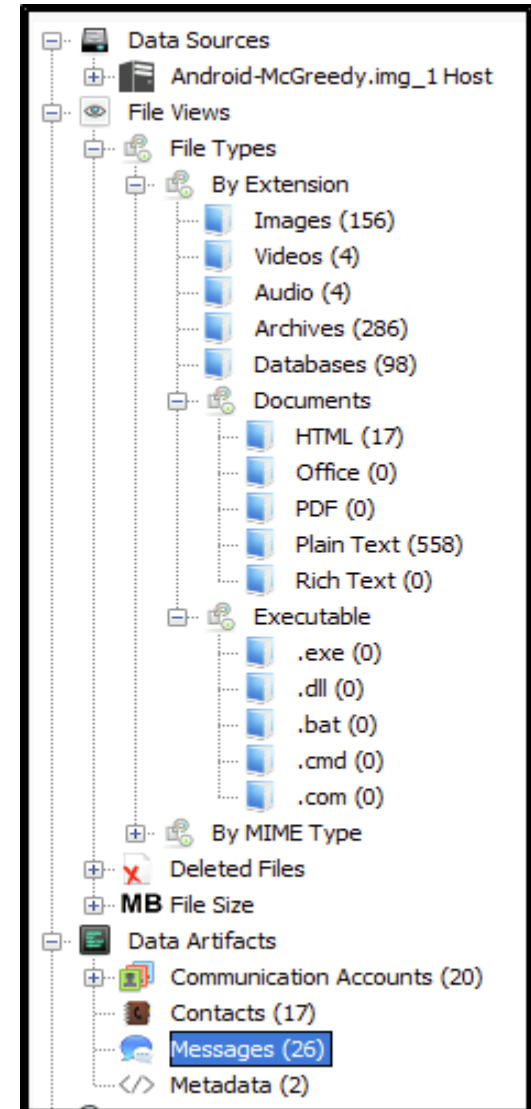
Views in the Autopsy UI










And the Contents Viewer (blue)

The Tree Viewer

The Tree Viewer is the most general view, and allows us to browse the disk image contents by directory tree or by sorted categories created by Autopsy plugins










The Results Viewer

Listing									
Messages									
Table Thumbnail Summary									
Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number	To Phone Number
 mmssms.db				Android Message	2023-10-28 14:35:50 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:02 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:36:28 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:54 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:37:26 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:37:48 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:38:17 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54

The Results Viewer is where we look after we've selected an item from the Tree Viewer, and it provides more information in a list

The Contents Viewer

Listing									
Messages									
Table Thumbnail Summary									
Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number	To Phone Number
 mmssms.db				Android Message	2023-10-28 14:35:50 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:02 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:36:28 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:36:54 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:37:26 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54
 mmssms.db			1	Android Message	2023-10-28 14:37:48 UTC	1	Incoming	+299406854	a0090f61-682c-4532-8c10-d48506cc8e4f
 mmssms.db				Android Message	2023-10-28 14:38:17 UTC	1	Outgoing	a0090f61-682c-4532-8c10-d48506cc8e4f	+299 40 68 54

The Contents Viewer is where we can inspect individual files

What's Next?

In the next HackerFrogs Afterschool digital forensics workshop, we'll learn how to investigate memory forensics files with Volatility!



Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!



Until Next Time, HackerFrogs!

