Mason Competitive Cyber

Intro To CTF Forensics

What is Forensics

Forensics in the context of CTFs usually involves some thing to do with either recovering deleted files from an image file or fixing broken files to being able to find files hidden inside of the other

Types of files you might see

- There are many different types of files you might come across but here are some important ones and the tools/programs you should try first
  - .img, .raw, .e01 These should be opened with autopsy, or FTK imager
  - .dmp or other memory dumps you can use volatility
  - Pcap, cap uses wireshark usually

Methodology

- The first thing that I usually use is the **file** command in linux
  - This can be confused if the magic bytes are manipulated
  - The file extension means nothing
- Strings is useful for finding text in the file
  - You can also pipe strings into grep or awk
- Xxd or hexdump to look at the hex output to look for magic bytes

File Carving

- File inside files is a common theme in many ctfs
- There are several tools that can be used for file carving
  - Binwalk
  - Scalpel/foremost
  - You can also use DD for manual file carving

    -
      ```
      $ dd if=./file_with_a_file_in_it.xxx of=./extracted_file.xxx bs=1 skip=1335205 count=40668937
      ```

Useful options for binwalk

- Binwalk -e [file.ext]
    - This will extract the files found the the file to your current directory
- Binwalk -dd='*.png' [file.ext]
    - This will extract all pngs from the file but you can use any extension

Images/Steg

- Exiftool
- NCL really likes digital invisible ink toolkit
- Analyze the header and contents with a hex editor
- Pngcheck can help check for corruption
- Zsteg can find hidden data
- Stegsolve can unhide flags easily

Audio Files

- Check file with binwalk
- Use audacity
- Check spectrograms
- Sonic visualizer is good for that

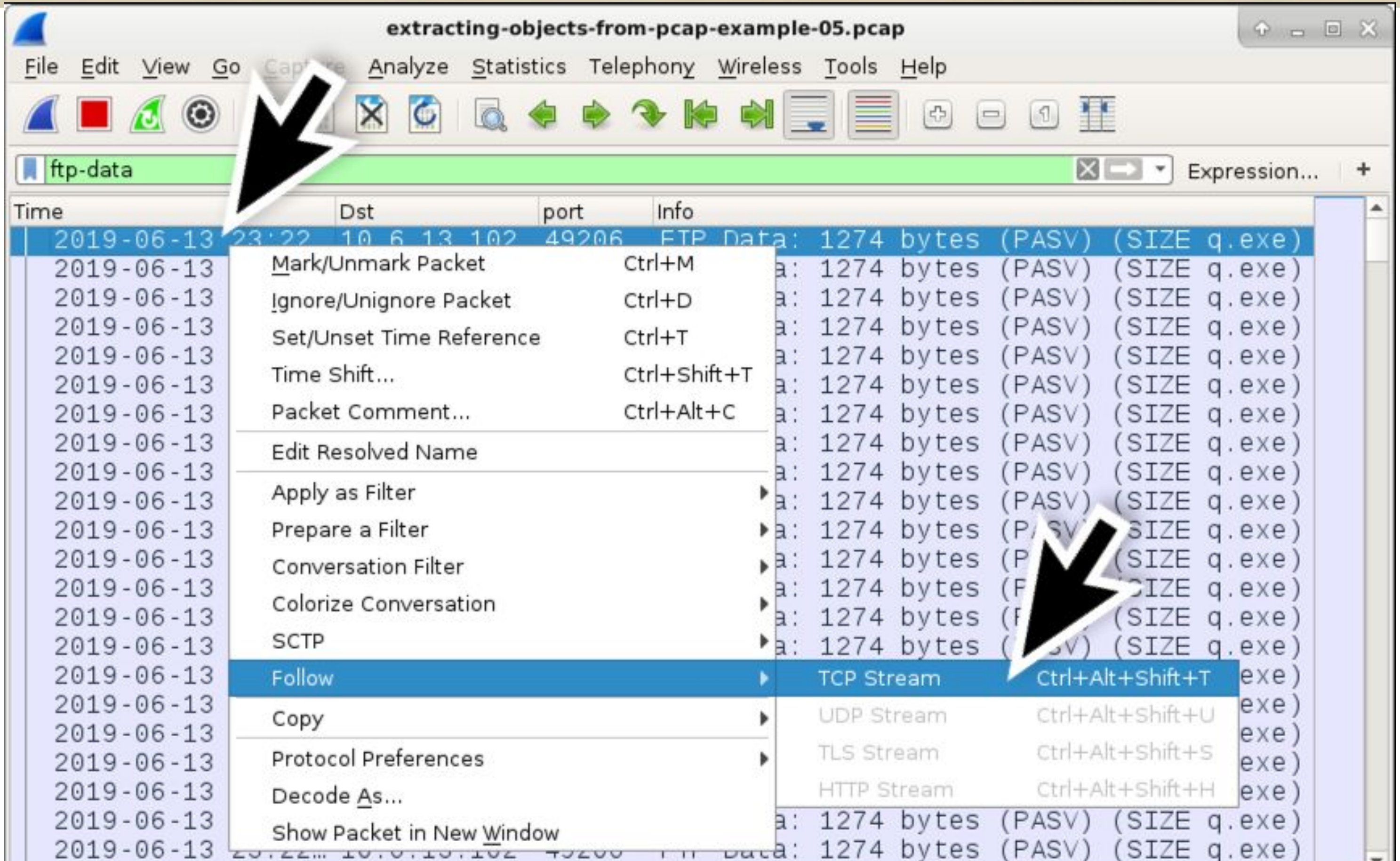
Volatility

- Used for memory dump analysis
- Basic commands
  - python vol.py -f %image_name% imageinfo
    - Gets the profile to continue working on the dump
  - python vol.py -f %path_to_image% --profile=%profile_name% pstree
    - Shows all of the running processes

Wireshark

- Used for looking at pcaps
- Things to look for include insecure protocols like HTTP, FTP, Telnet
- Following http streams can help make things more visible
- You can export things from the packet analysis using export and then http objects or you can follow the tcp steam and then save it to your desktop

Wireshark



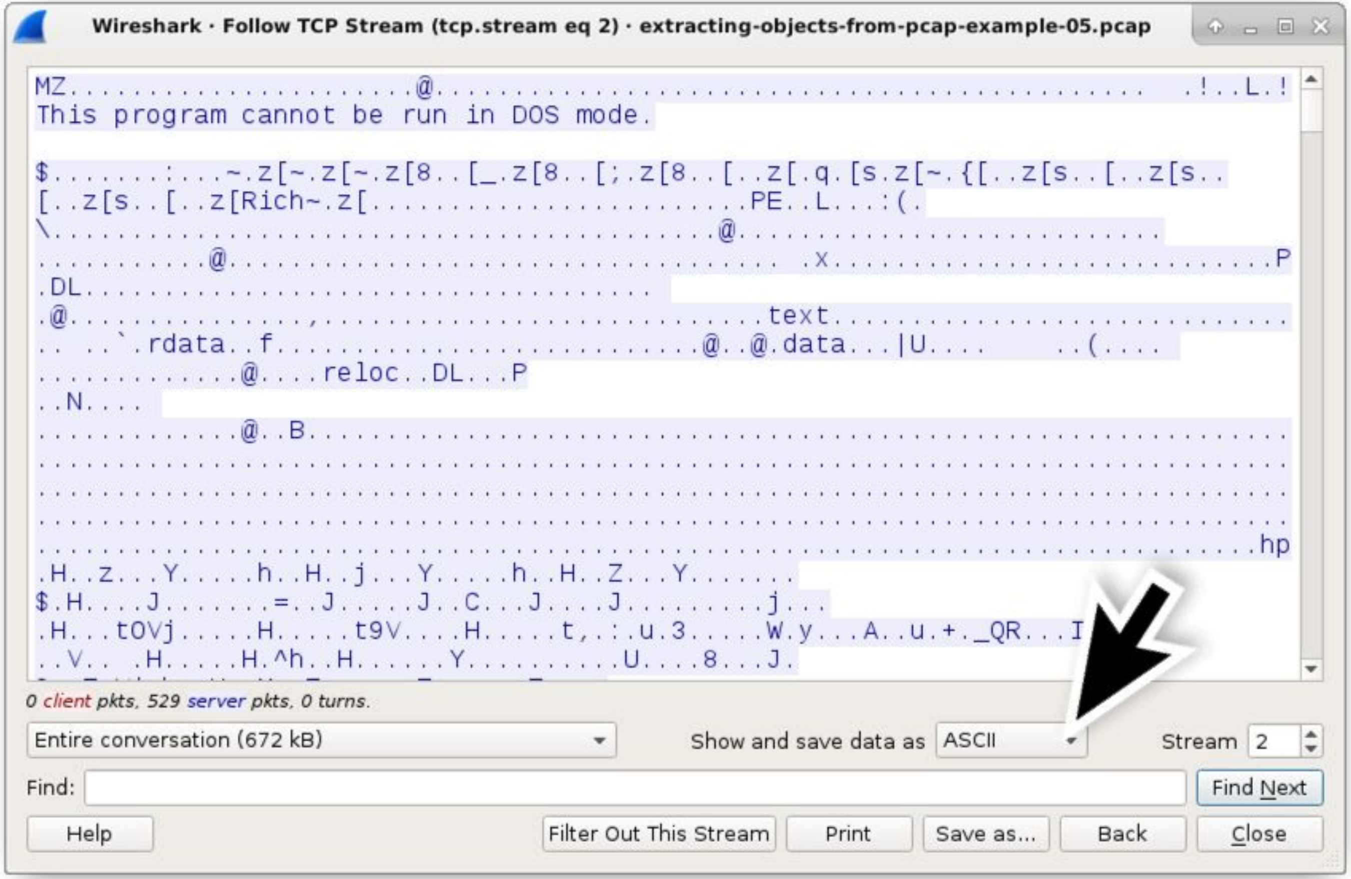
extracting-objects-from-pcap-example-05.pcap

ftp-data

```
Time                       Dst            port    Info
2019-06-13 23:22           10.6.13.102    49206   FTP Data: 1274 bytes (PASV) (SIZE q.exe)
```

File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Expression…
+
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As…
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

Wireshark



Wireshark · Follow TCP Stream (tcp.stream eq 2) · extracting-objects-from-pcap-example-05.pcap

```
MZ......................@...................................   .!..L.!
This program cannot be run in DOS mode.

$.......:...~.z[~.z[~.z[8..[_.z[8..[;.z[8..[..z[.q.[s.z[~.{[..z[s..[..z[s..
[..z[s..[..z[Rich~.z[......................PE..L...:(.
\.......................................@.......................
..........@..........................  .X........................P
.DL..................................
.@...............,.....................text.........................
..  ...`.rdata..f.......................@..@.data...|U....    ..(....
............@....reloc..DL...P
..N....
............@..B..............................................................
.................................................................................
.................................................................................
.................................................................................
..............................................................................hp
.H..z...Y.....h..H..j...Y.....h..H..Z...Y......
$.H....J.......=..J.....J..C...J....J.........j...
.H...tOVj.....H.....t9V....H.....t,.:.u.3.....W.y...A..u.+._QR...I
..V..  .H.....H.^h..H......Y..........U....8...J.
```

0 client pkts, 529 server pkts, 0 turns.

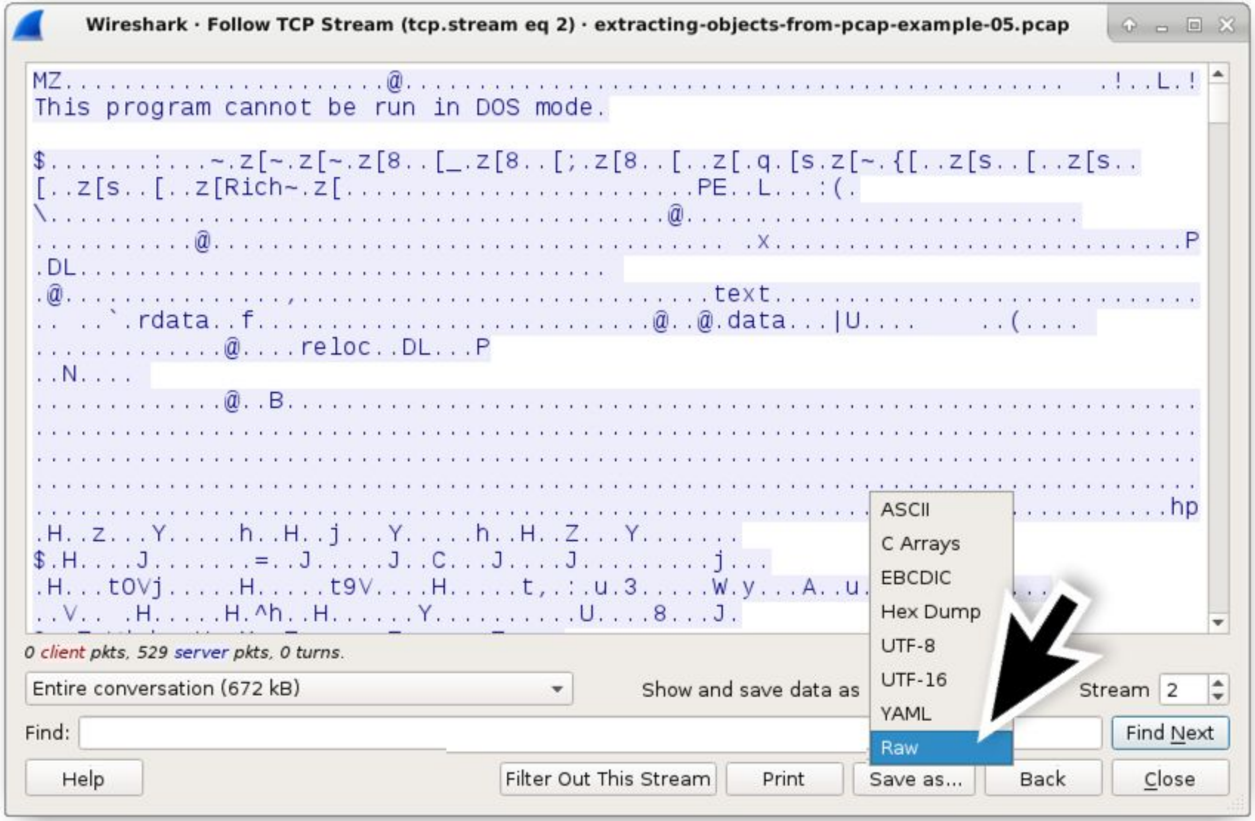
Entire conversation (672 kB)

Show and save data as ASCII

Stream 2

Find:

Wireshark



Wireshark · Follow TCP Stream (tcp.stream eq 2) · extracting-objects-from-pcap-example-05.pcap

```
MZ......................@...........................................  .!..L.!
This program cannot be run in DOS mode.

$.......:...~.z[~.z[~.z[8..[_.z[8..[;.z[8..[..z[.q.[s.z[~.{[..z[s..[..z[s..
[..z[s..[..z[Rich~.z[......................PE..L...:(.
\.........................................@...........................
..........@...................................  .x..........................P
.DL...............................
.@..............,..........................text...............................
..  ..`.rdata..f..........................@..@.data...|U....     ..(....
.............@....reloc..DL...P
..N....
.............@..B.............................................................
..............................................................................
..............................................................................
..............................................................................
..............................................................................hp
.H..Z...Y.....h..H..j...Y.....h..H..Z...Y.......
$.H....J.......=..J.....J..C...J....J.........j...
.H...tOVj.....H......t9V....H......t,.:.u.3.....W.y...A..u.
..V..  .H.....H.^h..H......Y...........U....8...J.
```

0 client pkts, 529 server pkts, 0 turns.

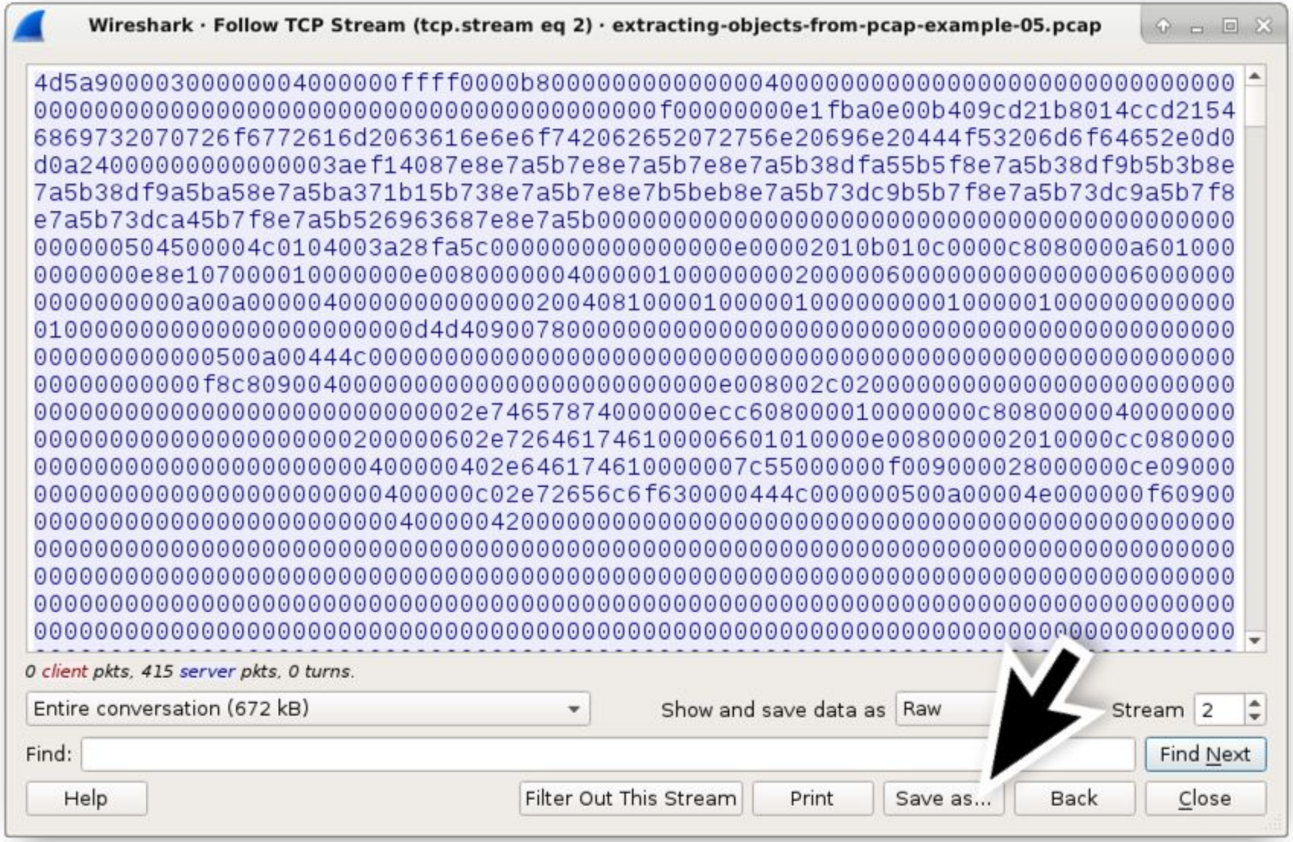
Entire conversation (672 kB)

Show and save data as: Raw

Stream 2

Find:

Wireshark



Wireshark · Follow TCP Stream (tcp.stream eq 2) · extracting-objects-from-pcap-example-05.pcap

```
4d5a90000300000004000000ffff0000b8000000000000004000000000000000000000000000000
00000000000000000000000000000000000000000f00000000e1fba0e00b409cd21b8014ccd2154
6869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0
d0a24000000000000003aef14087e8e7a5b7e8e7a5b7e8e7a5b38dfa55b5f8e7a5b38df9b5b3b8e
7a5b38df9a5ba58e7a5ba371b15b738e7a5b7e8e7b5beb8e7a5b73dc9b5b7f8e7a5b73dc9a5b7f8
e7a5b73dca45b7f8e7a5b526963687e8e7a5b000000000000000000000000000000000000000000
000000504500004c0104003a28fa5c0000000000000000e00002010b010c0000c8080000a601000
0000000e8e107000010000000e00800000040000010000000020000060000000000000006000000
0000000000a00a00000400000000000002004081000010000010000000001000001000000000000
010000000000000000000000000d4d409007800000000000000000000000000000000000000000
000000000000000500a00444c0000000000000000000000000000000000000000000000000000000
00000000000f8c809004000000000000000000000000000e008002c02000000000000000000000000
00000000000000000000000000002e74657874000000ecc608000010000000c8080000040000000
000000000000000000000200000602e726461746100006601010000e008000002010000cc080000
0000000000000000000000400000402e646174610000007c55000000f009000028000000ce09000
00000000000000000000000400000c02e72656c6f630000444c000000500a00004e000000f60900
000000000000000000000000400000420000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
```

0 client pkts, 415 server pkts, 0 turns.

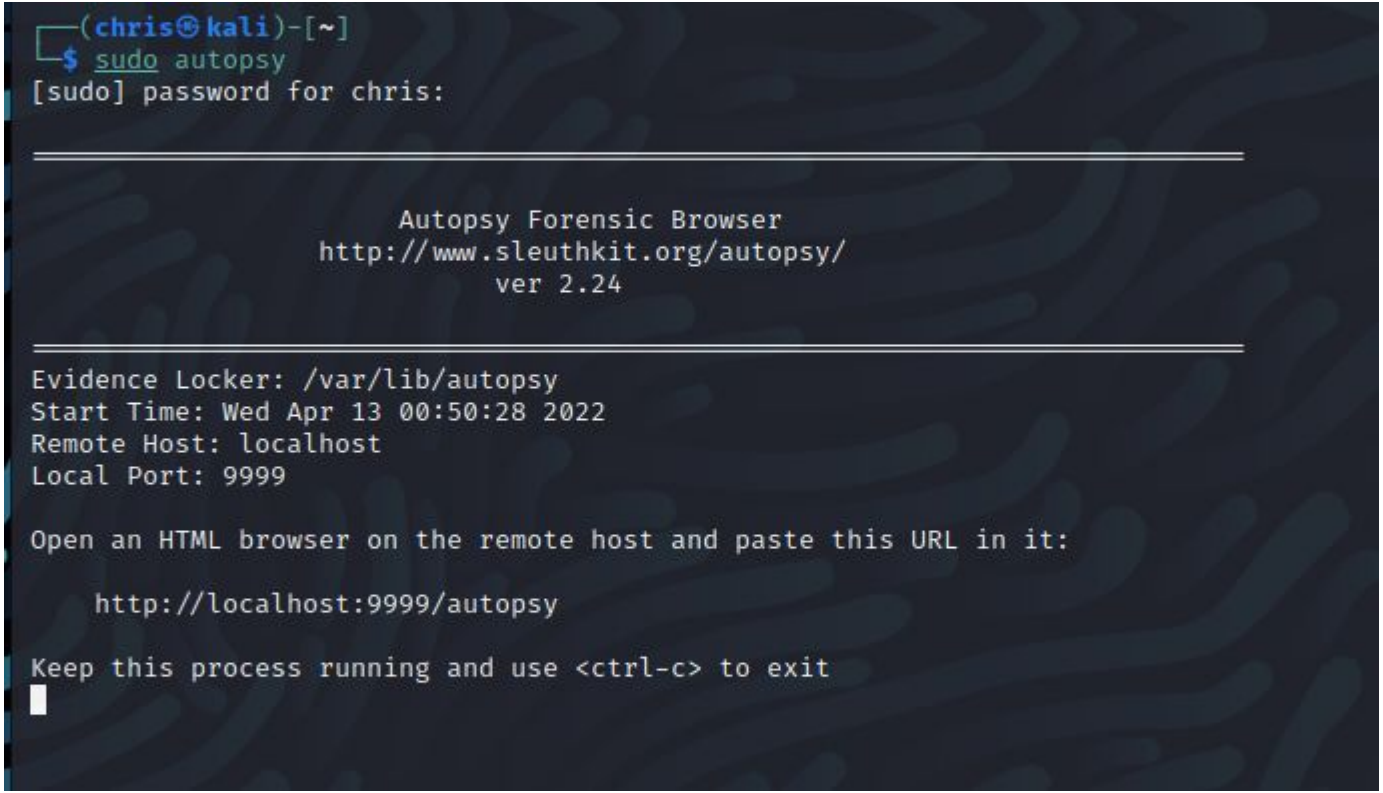
Entire conversation (672 kB)

Show and save data as: Raw

Stream: 2

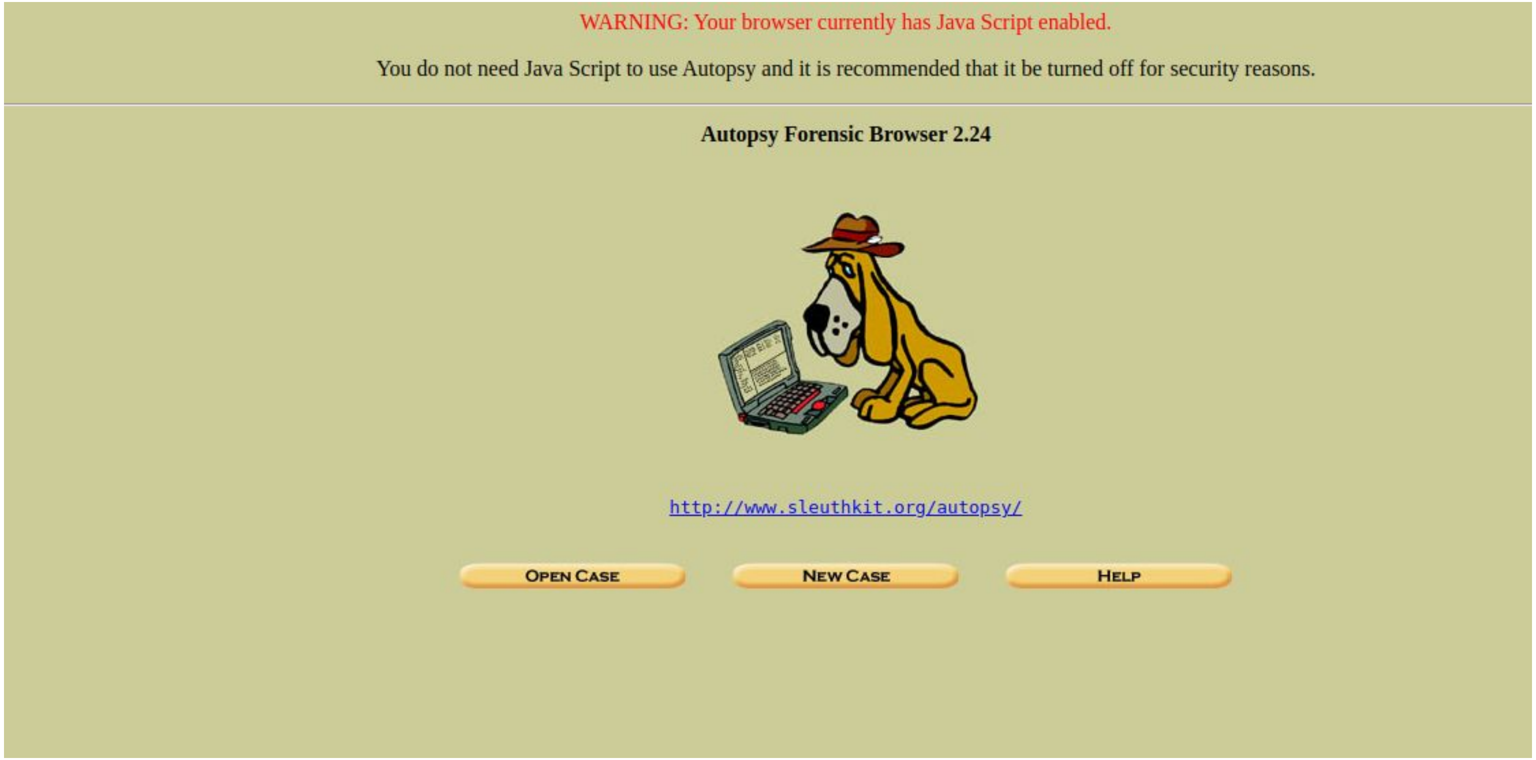
Find:

Autopsy



```
┌──(chris㉿kali)-[~]
└─$ sudo autopsy
[sudo] password for chris:

============================================================================

                        Autopsy Forensic Browser
                   http://www.sleuthkit.org/autopsy/
                               ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Wed Apr 13 00:50:28 2022
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Autopsy



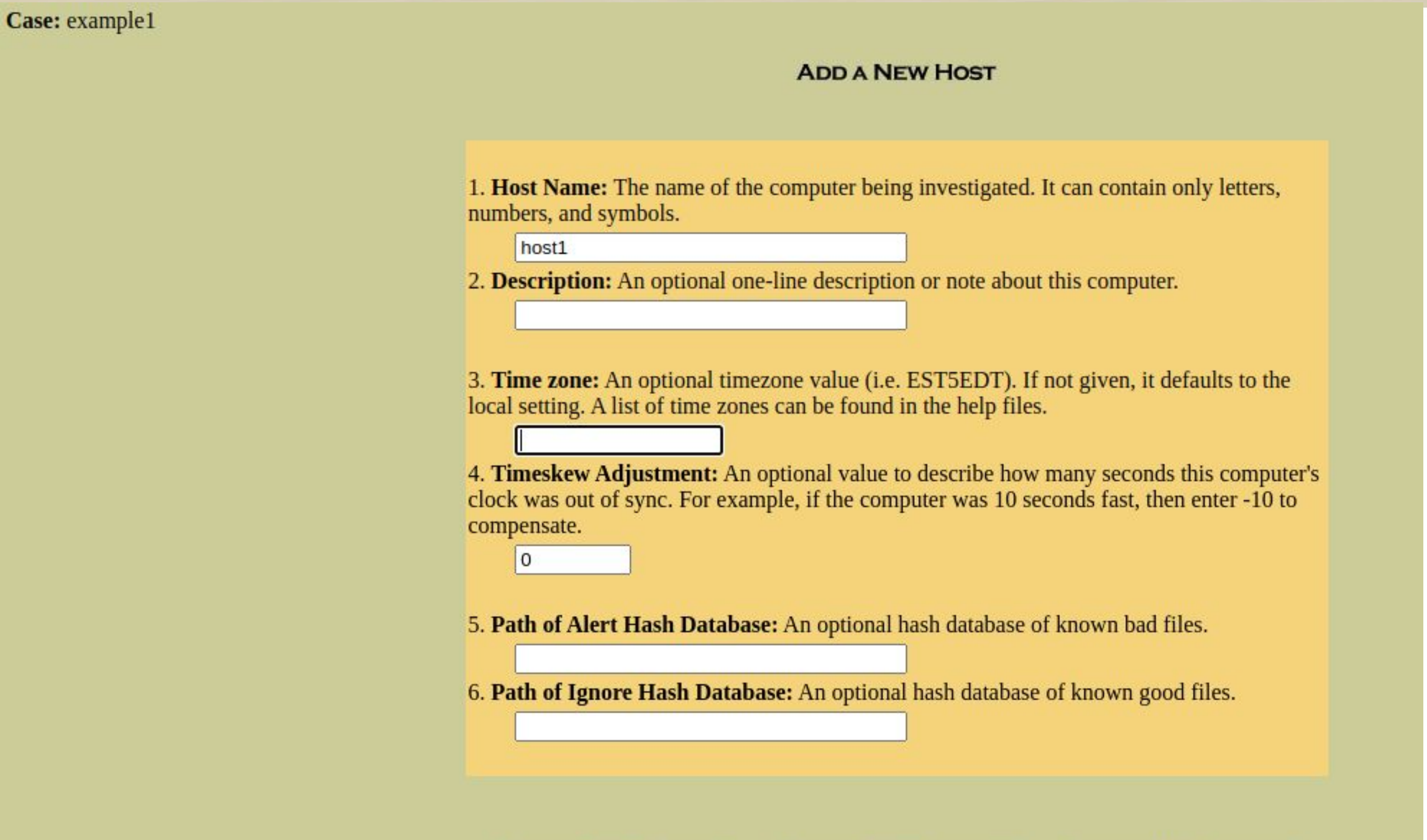
WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

Autopsy



Case: example1

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

   host1

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

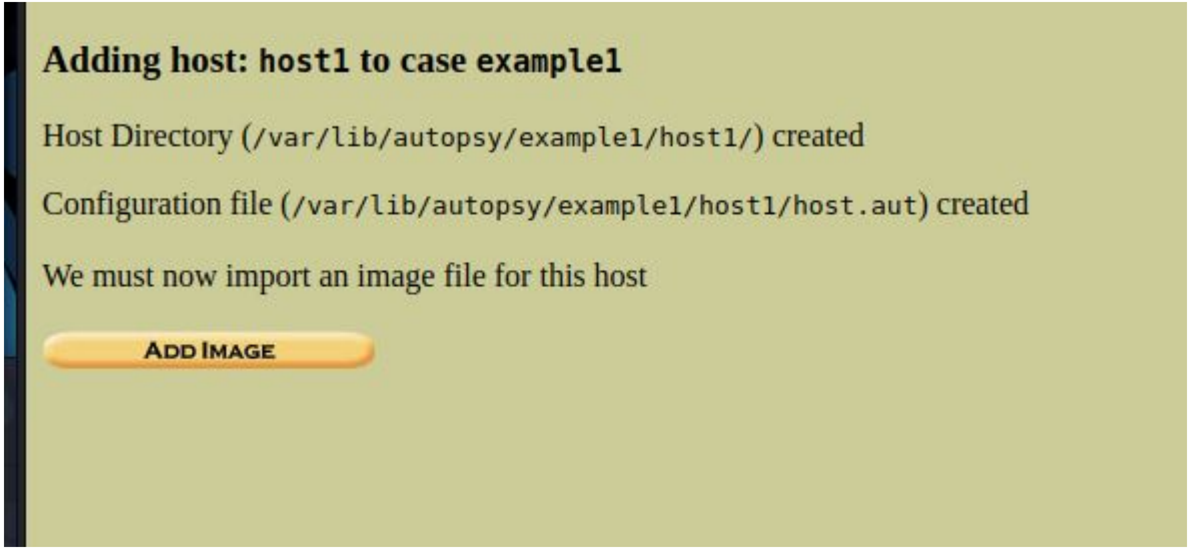
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

   0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Autopsy



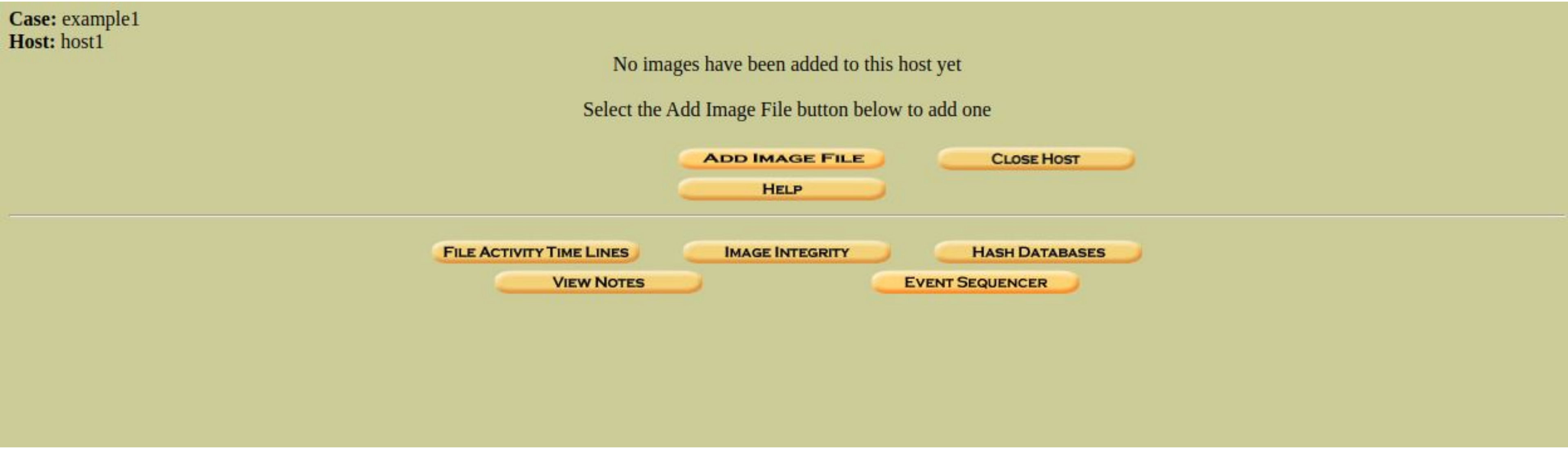
Adding host: `host1` to case `example1`

Host Directory (`/var/lib/autopsy/example1/host1/`) created

Configuration file (`/var/lib/autopsy/example1/host1/host.aut`) created

We must now import an image file for this host

Autopsy

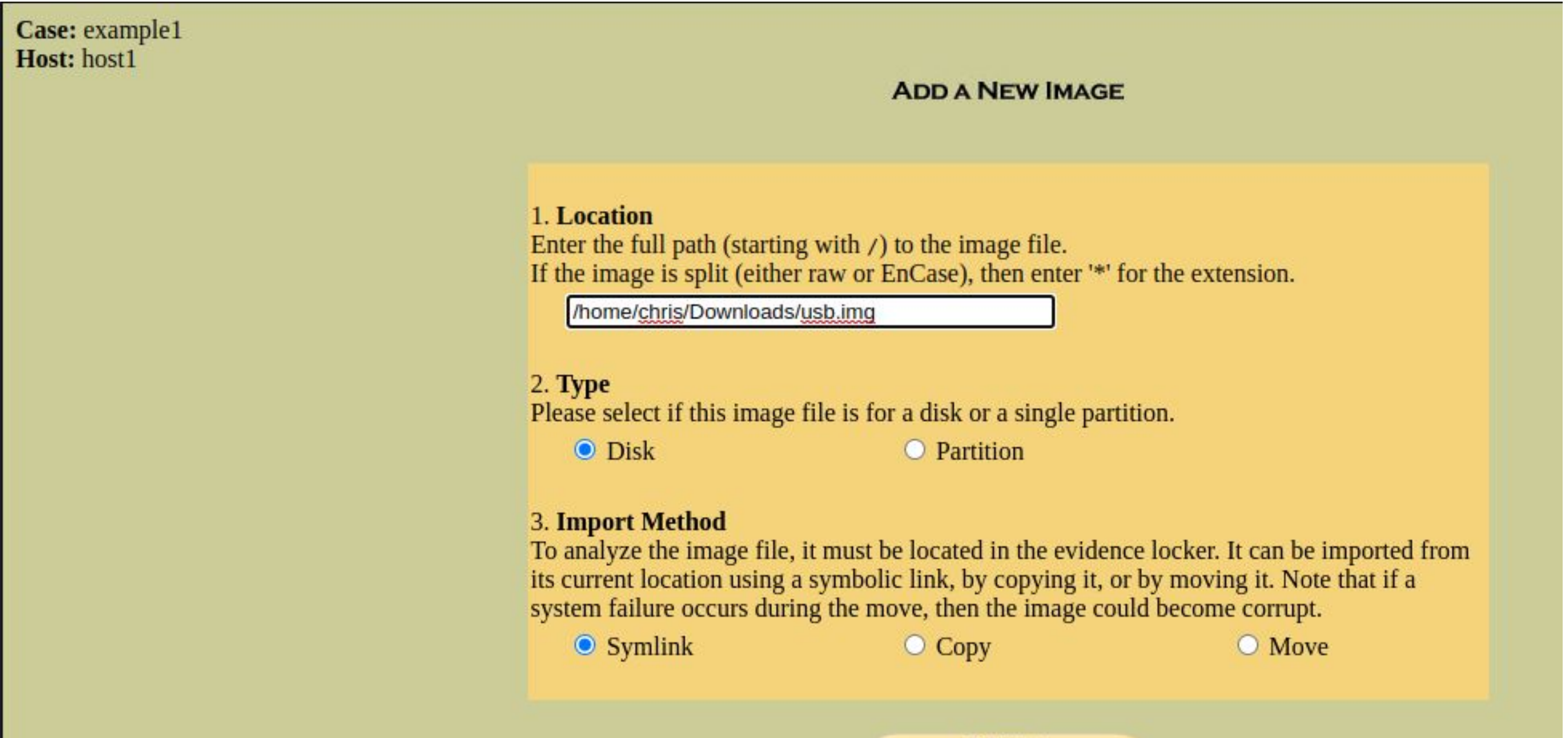


Case: example1
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one

Autopsy



Case: example1
Host: host1

ADD A NEW IMAGE

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/home/chris/Downloads/usb.img

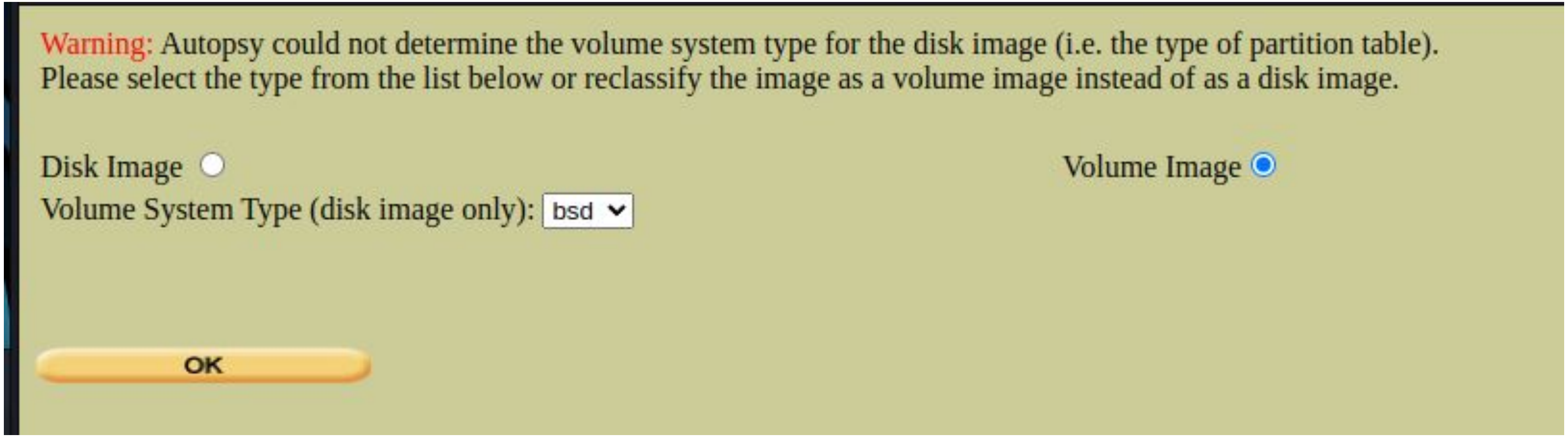
2. **Type**
Please select if this image file is for a disk or a single partition.

● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move

Autopsy



Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image ○ Volume Image ●

Volume System Type (disk image only): bsd

Autopsy

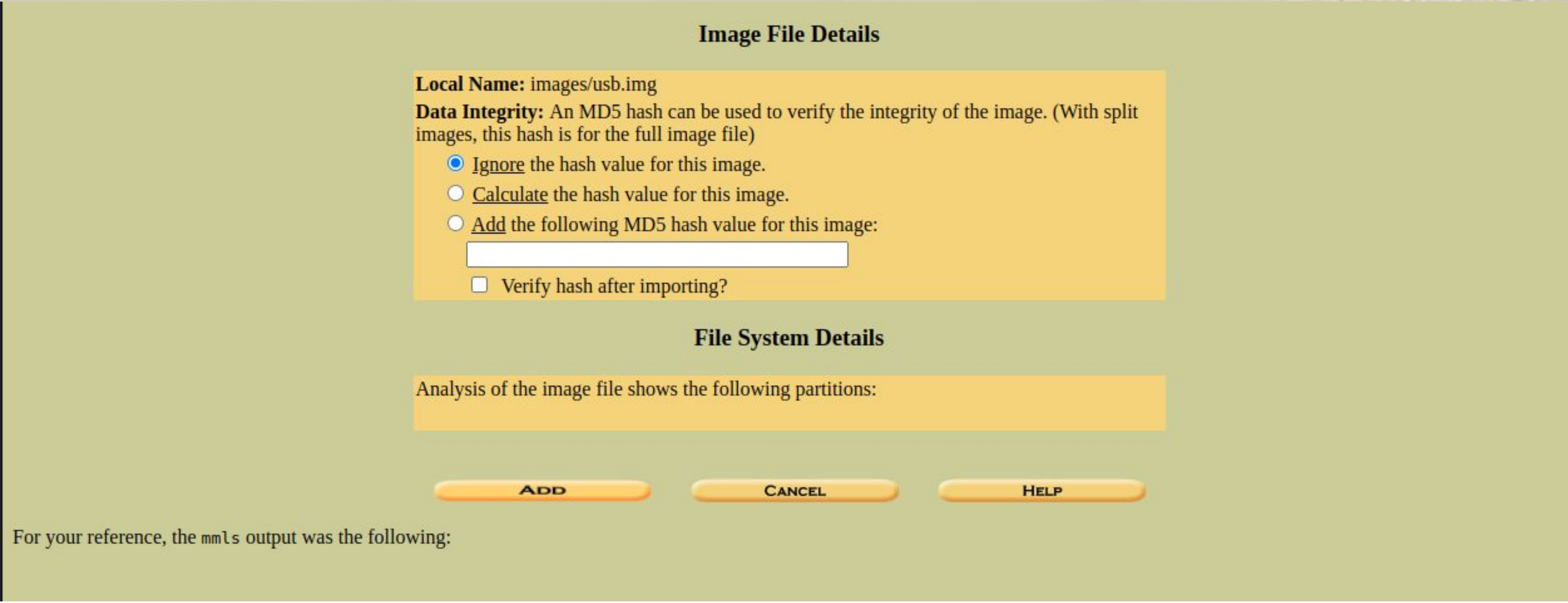


Image File Details

Local Name: images/usb.img

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- ● Ignore the hash value for this image.
- ○ Calculate the hash value for this image.
- ○ Add the following MD5 hash value for this image:

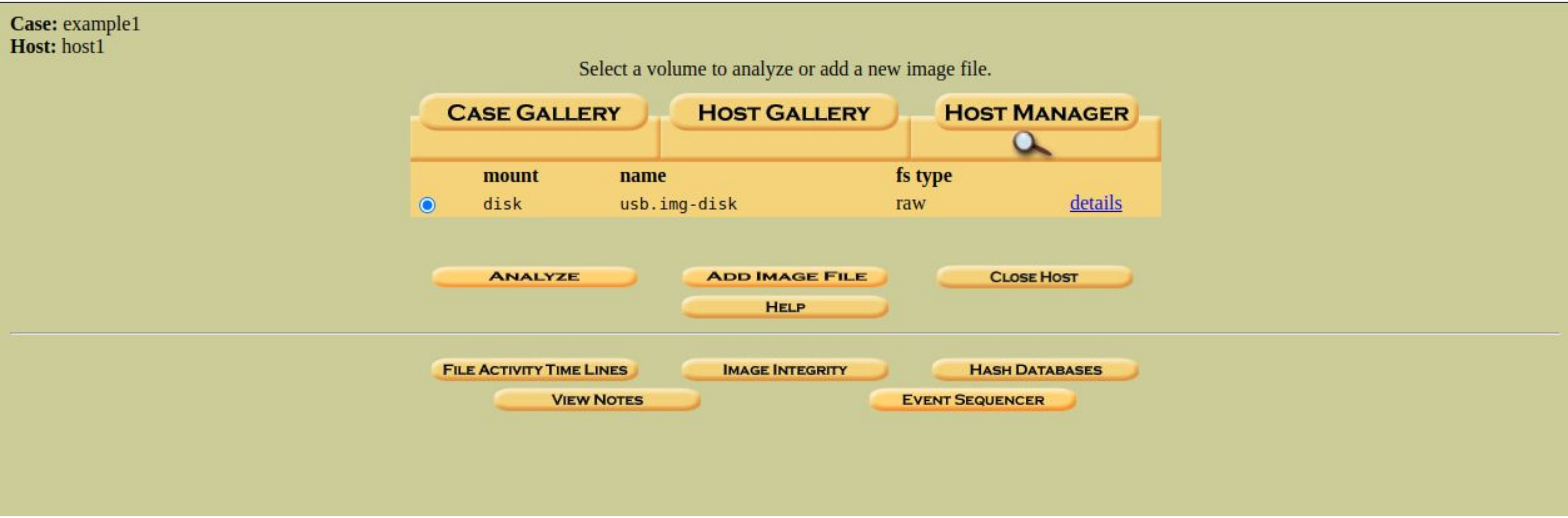
□ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

For your reference, the `mmls` output was the following:

Autopsy



Case: example1
Host: host1

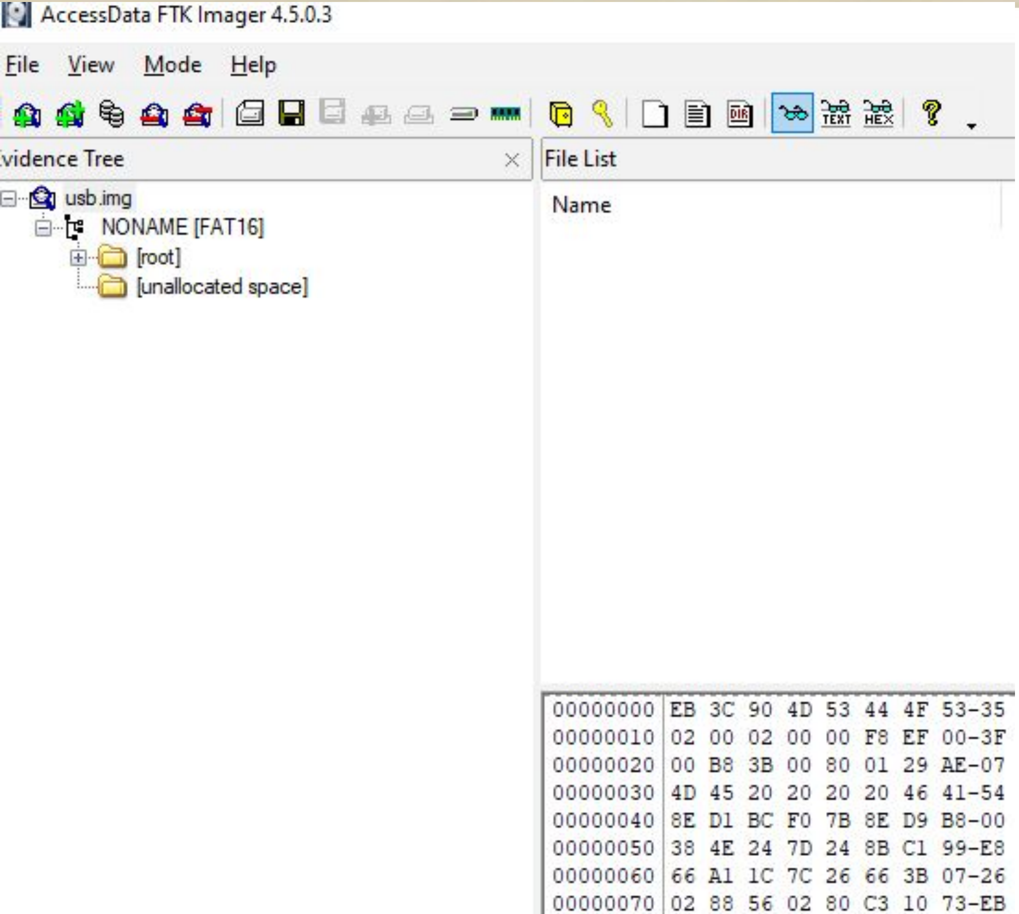
Select a volume to analyze or add a new image file.

	mount	name	fs type	
●	disk	usb.img-disk	raw	details

Autopsy/FTK imager

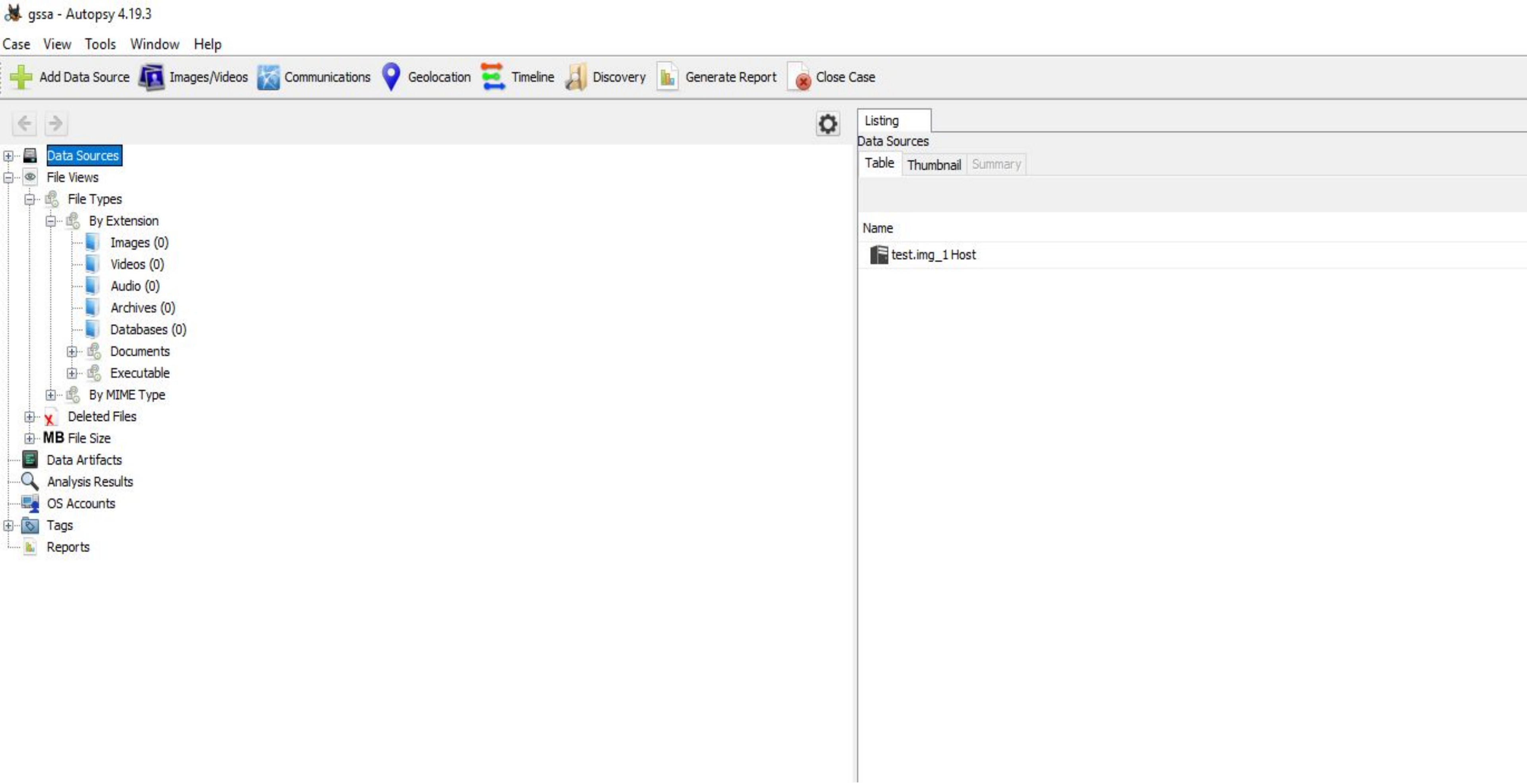
- Autopsy is also available on windows
  - This provides a better GUI
- FTK imager is also available for forensic analysis
  - This also has a decent GUI

FTK GUI



usb.img
NONAME [FAT16]
[root]
[unallocated space]

```
00000000 EB 3C 90 4D 53 44 4F 53-35
00000010 02 00 02 00 00 F8 EF 00-3F
00000020 00 B8 3B 00 80 01 29 AE-07
00000030 4D 45 20 20 20 20 46 41-54
00000040 8E D1 BC F0 7B 8E D9 B8-00
00000050 38 4E 24 7D 24 8B C1 99-E8
00000060 66 A1 1C 7C 26 66 3B 07-26
00000070 02 88 56 02 80 C3 10 73-EB
```



Name
test.img_1 Host

Proud Sponsors