HackerFrogs Afterschool
Disk Image Forensics Part 1

Class:
Digital Forensics

Workshop Number:
AS-FOR-05

Document Version:
1.75

Special Requirements:
- Registered account at picoctf.org

Welcome to HackerFrogs Afterschool!

This workshop is the fifth class for digital forensics.

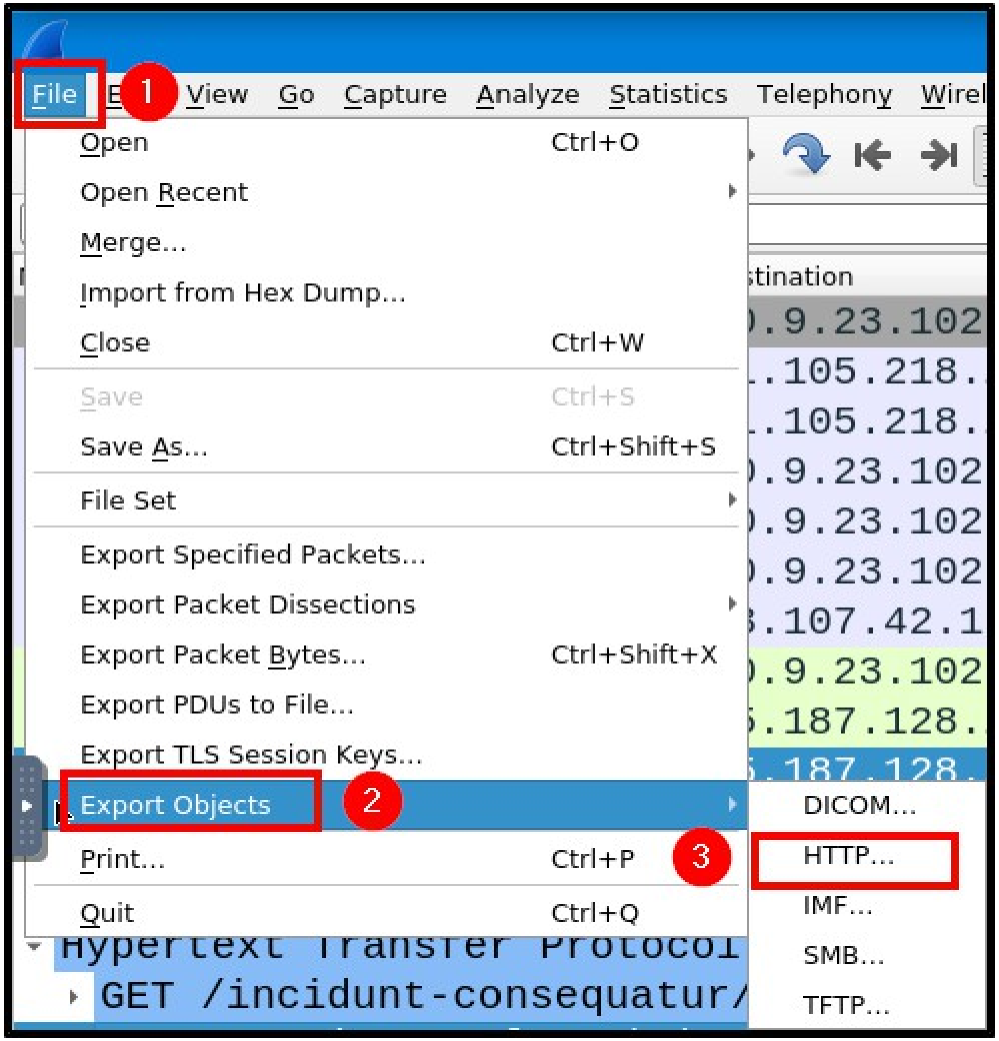
In the last workshop, we learned about the following digital forensics concepts:

Wireshark

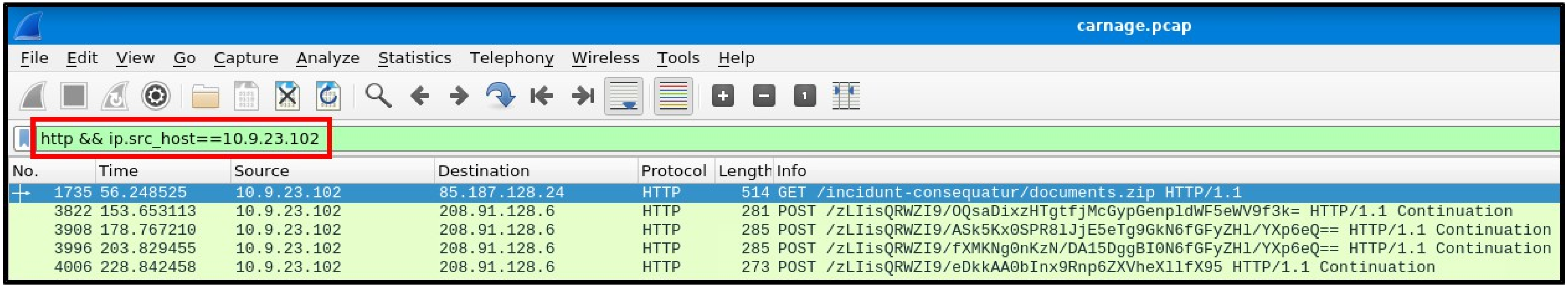
Wireshark is a program which is widely used for network traffic analysis, and we'll learn to use it to analyze PCAP files.

Exporting Files From Wireshark

We can use the **Export Objects** option in Wireshark to look for files downloaded in the PCAP file, and most files are downloaded using the HTTP protocol



Isolating IP Addresses



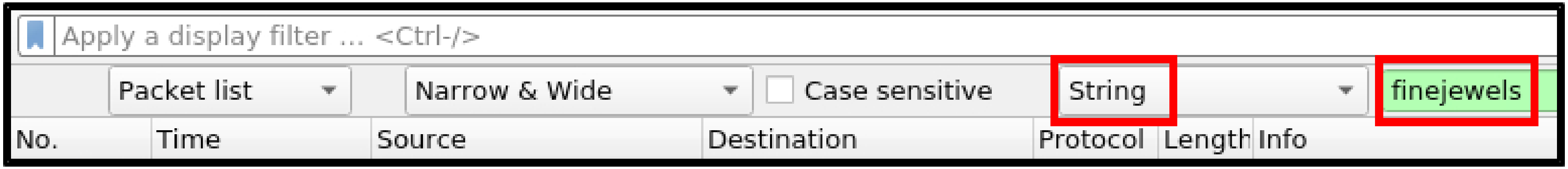
carnage.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && ip.src_host==10.9.23.102

```
No.  Time        Source       Destination   Protocol Length Info
1735 56.248525   10.9.23.102  85.187.128.24 HTTP     514 GET /incidunt-consequatur/documents.zip HTTP/1.1
3822 153.653113  10.9.23.102  208.91.128.6  HTTP     281 POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1 Continuation
3908 178.767210  10.9.23.102  208.91.128.6  HTTP     285 POST /zLIisQRWZI9/ASk5Kx0SPR8lJjE5eTg9GkN6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
3996 203.829455  10.9.23.102  208.91.128.6  HTTP     285 POST /zLIisQRWZI9/fXMKNg0nKzN/DA15DggBI0N6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
4006 228.842458  10.9.23.102  208.91.128.6  HTTP     273 POST /zLIisQRWZI9/eDkkAA0bInx9Rnp6ZXVheXllfX95 HTTP/1.1 Continuation
```

We can apply more than one display filter at once: and this is a good way to isolate traffic coming from specific IP addresses

Searching For Strings in Packet Contents



Apply a display filter … <Ctrl-/>

Packet list ▾ | Narrow & Wide ▾ | □ Case sensitive | String ▾ | finejewels

The search function in Wireshark can be very useful for searching for specific text strings in packets

This Workshop's Topics

- Disk Image Forensics Overview

- Pico SleuthKit Intro

- Pico SleuthKit Apprentice

- Pico SleuthKit Operation Orchid

What is Digital Disk Forensics?

Digital disk forensics is the examination and analysis of information stored on digital disks, such as hard drives (HDD), USB drives, or any other type of storage media.

Digital Disk Forensics

Disk forensics is often used in cybersecurity incident response to analyze and identify devices that may have been compromised in security incidents.

The Sleuthkit Software

The Sleuth Kit is a popular program used in digital disk forensics, and we can access it from the PicoCTF webshell

The Sleuthkit Software

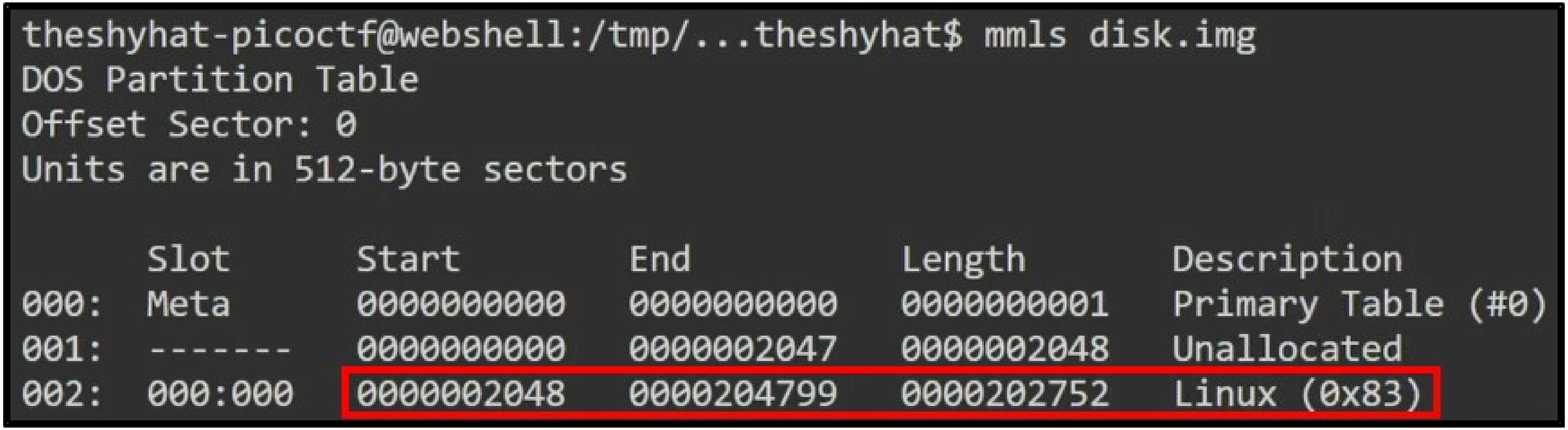
We'll be learning some basic operations of The Sleuth Kit in this workshop to learn digital disk forensics

PicoCTF: Sleuthkit Intro

Let's get acquainted with the Sleuthkit with this PicoCTF challenge

https://play.picoctf.org/practice/challenge/301?page=1&search=sleuth

The MmLs Command

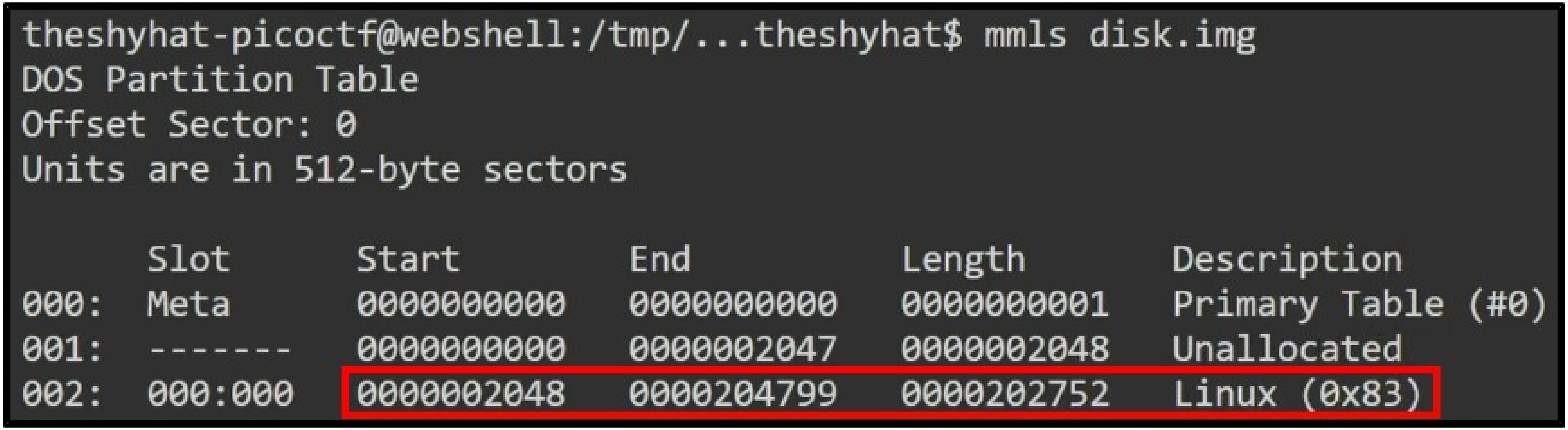


```
theshyhat-picoctf@webshell:/tmp/...theshyhat$ mmls disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      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 MnLs Command



```
theshyhat-picoctf@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)
```

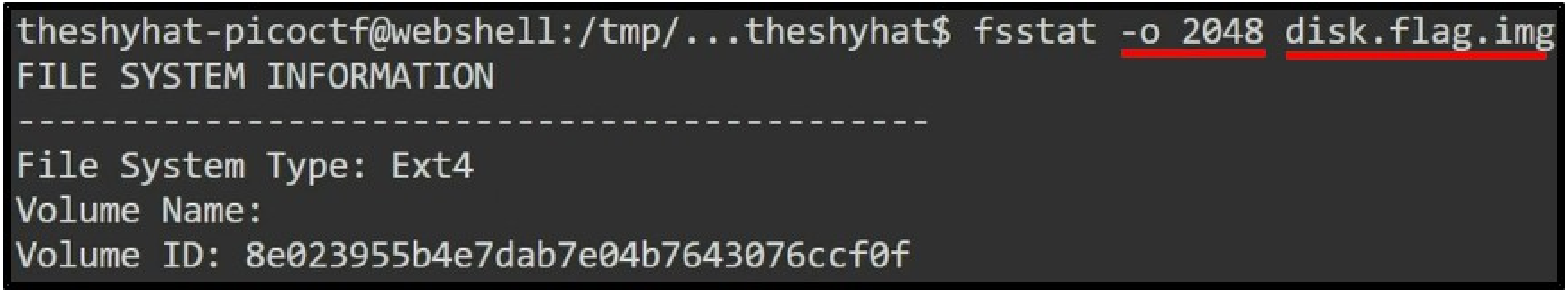
We can see where the partition starts (offset in bytes), where the partition ends, and the length (size in bytes) of the partition

PicoCTF: Sleuthkit Apprentice

Let's learn more Sleuthkit commands with this PicoCTF challenge

https://play.picoctf.org/practice/challenge/300?page=1&search=sleuth

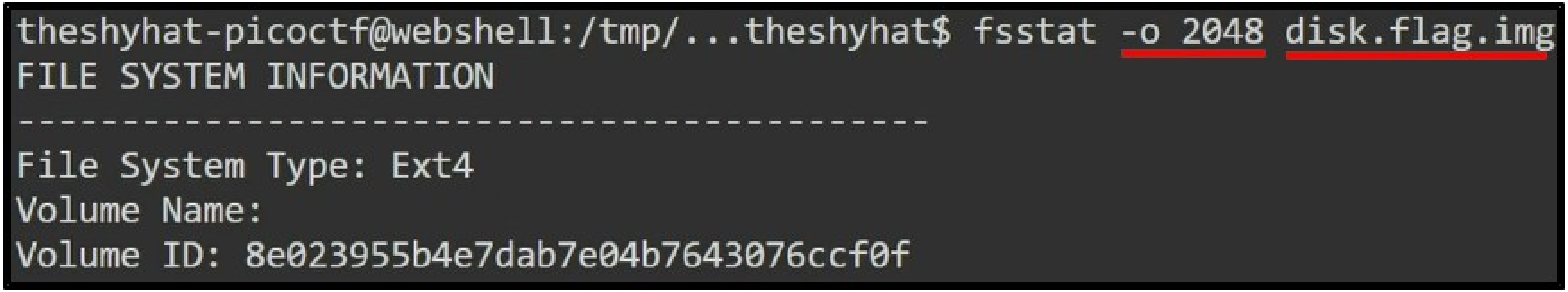
The FsStat Command



```
theshyhat-picoctf@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)

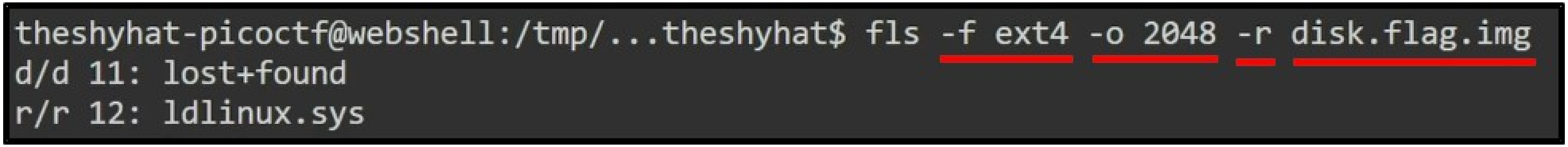
The FsStat Command



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

To use this command, we'll need to supply the byte offset of the disk partition (-o), and the name of the disk image

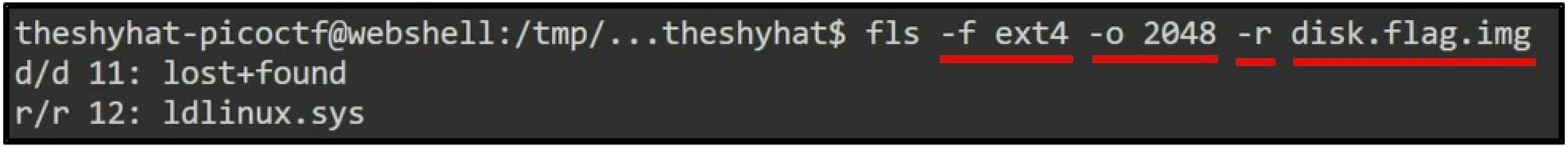
The Fls Command



```
theshyhat-picoctf@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

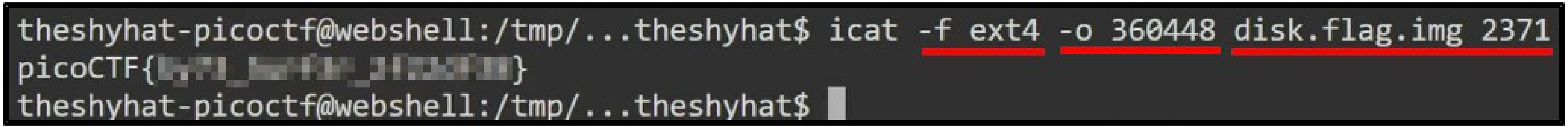
The Fls Command



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

To run this command, we need the format of the disk partition (-f), the offset of the disk partition (-o), run it recursively (-r), and supply the disk image name

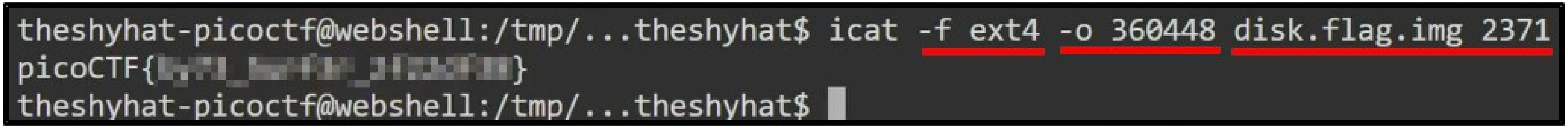
The Icat Command



```
theshyhat-picoctf@webshell:/tmp/...theshyhat$ icat -f ext4 -o 360448 disk.flag.img 2371
picoCTF{[redacted]}
theshyhat-picoctf@webshell:/tmp/...theshyhat$ 
```

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

The Icat Command



```
theshyhat-picoctf@webshell:/tmp/...theshyhat$ icat -f ext4 -o 360448 disk.flag.img 2371
picoCTF{[redacted]}
theshyhat-picoctf@webshell:/tmp/...theshyhat$
```

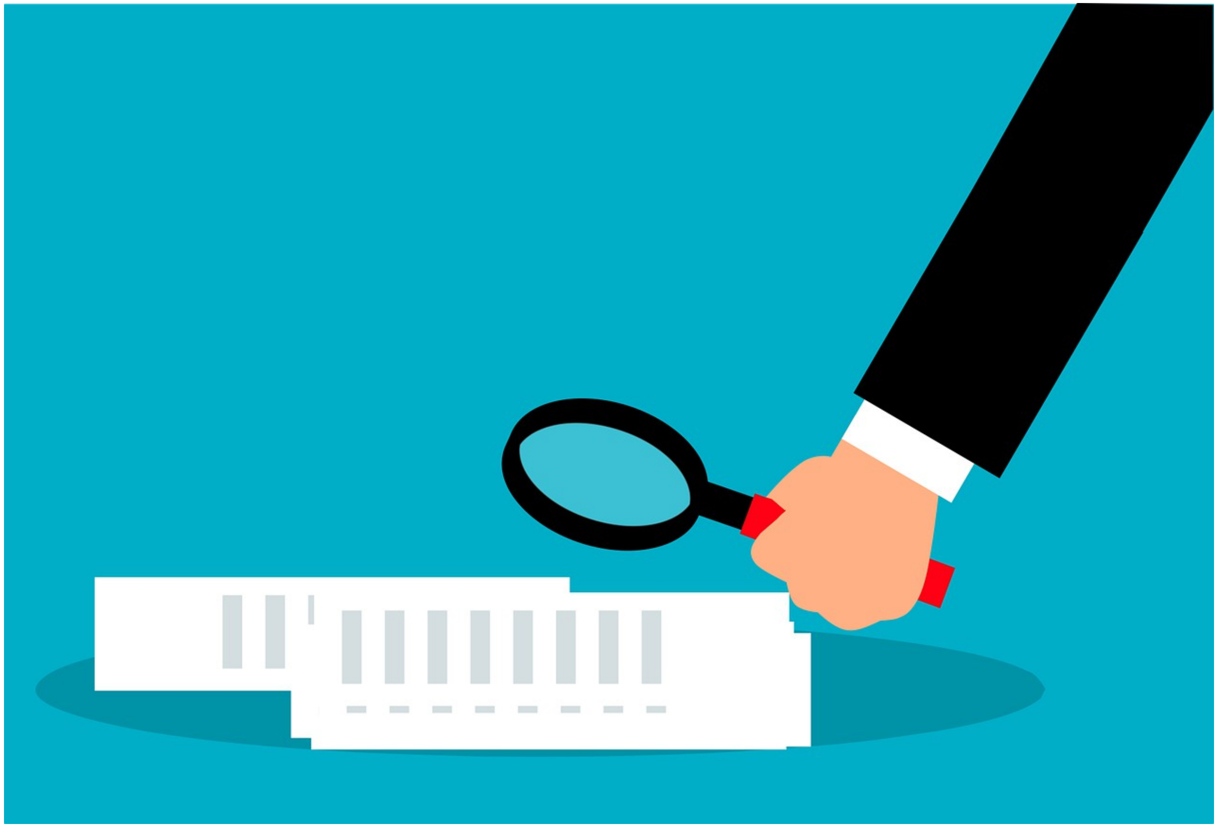
To use the command, we need to supply the format of the disk partition (-f), the offset of the disk partition (-o), and finally, the name of the disk image and the inode number (disk.flag.img 2371)

PicoCTF: Operation Orchid

Let's use all the Sleuthkit command we've learned so far with this PicoCTF challenge

https://play.picoctf.org/practice/challenge/285?page=1&search=orc

Summary

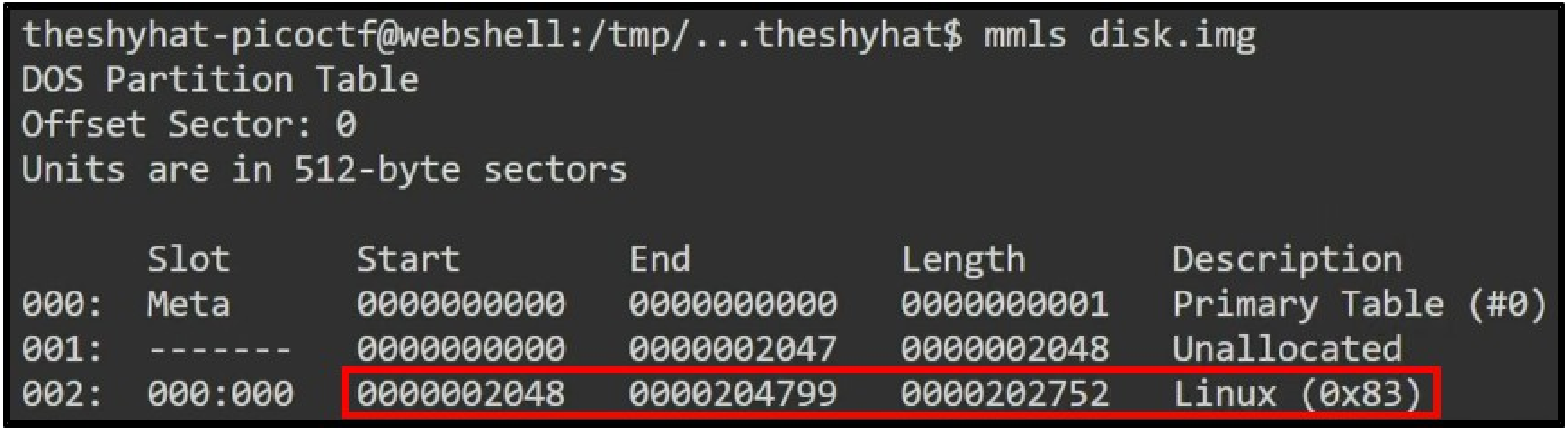


Let's review the digital forensics concepts we learned in this workshop:

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

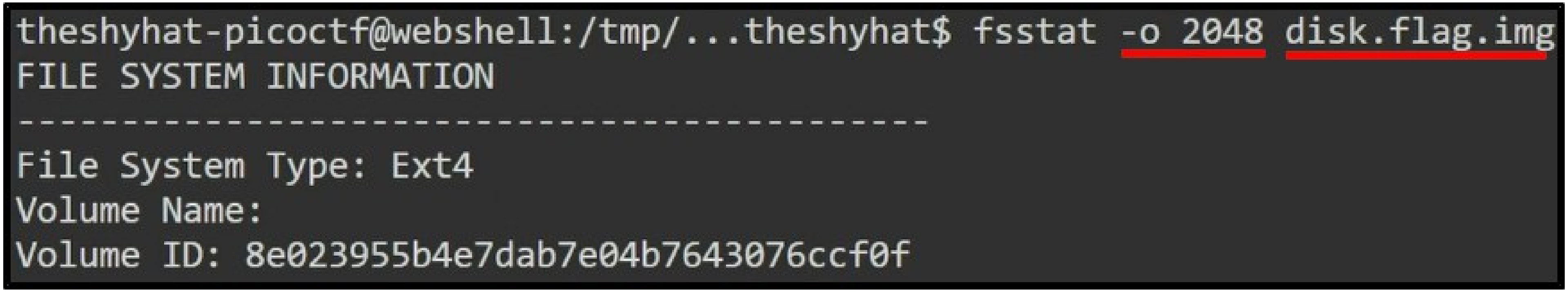


```
theshyhat-picoctf@webshell:/tmp/...theshyhat$ mmls disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      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-picoctf@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)

What's Next?

In the next HackerFrogs Afterschool digital forensics workshop, we'll use a different program to look at disk image files, in a more intuitive way!

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!