

Intro To Forensics & Incident Response

UMass Cybersecurity Club



What is Forensics and Incident Response (IR)?

Forensics: finding out *what happened, how it happened, and who did it**.

Forensics and incident response mean basically the same thing.

- Forensics focuses on figuring out who did it, and is usually done by law enforcement.
- Incident response focuses on recovering from an attack, usually done by enterprise security teams.



Don't you need a warrant for that?

Forensics in particular uses a lot of legal theory when done in practice.

This is a workshop (~~and we assume you don't care~~), so we won't go too in depth.

For more information take:

- CS 365 (Digital Forensics)
- CS 363 (Computer Crime Law)
- CS 563 (Internet Law and Policy)

This workshop is **mostly** going to cover some introductory techniques you would see in CTFs and the like. **You don't have to worry about how everything works**—we're just showing you what's available!



Disclaimer:

Don't mess with anything you don't own.

(We're not responsible for you if you do.)

Common Use Cases and Techniques I

- Most computers log addresses constantly (IPs, MACs, GPS locations)
 - a. Can use this to recover **where** a device was and **who** it was with
 - b. **Wireshark** let's us capture all network traffic, tracking down criminals or locating C2 servers
- Filesystems are very lazy, they don't actually delete your files!
 - a. Can use tools like The Sleuth Kit (tsk) to recover deleted files to find malware, evidence of a crime, or restore deleted files



UMASS
CYBERSEC
CLUB

- [illegible]

Trial by fire

Forensics is best learned through practice, so let's practice!

1. We'll walk you through the scenario
2. Give you a simple goal
3. Some time to figure it out on your own
4. And then show the solution



Some context: Wireshark

- Many devices, including routers and computers, can perform what is called a “packet capture”.
 - A detailed record of all packets sent over a network that were seen by the device.
- Wireshark is a tool that allows us to inspect and analyze packet captures
 - great insight into what was going on at a specific time on your network

Legal caveat: capturing packets on your *own network* is perfectly fine and legal.

The Global Internet Is Being Attacked by Sharks, Google Confirms

By Will Oremus



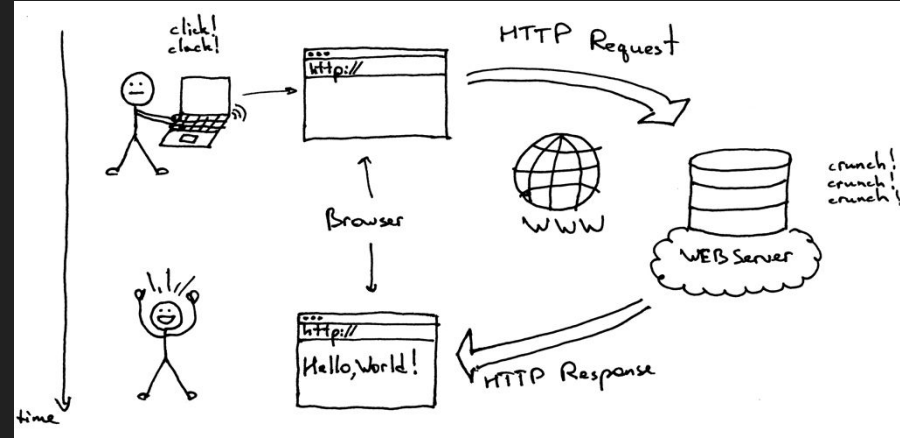
17.2k 6k 34



More context: Client-Server Model (Web Workshop)

- **Client:** System/program that connects to a remote server to retrieve content
 - For most users: the browser
- **Server:** A local or remote system that provides data to a user
 - Can be local or remote
- Different protocols (types of messages) for different purposes

A packet capture is a record of the messages being sent to and from the machine!



Challenge #1 (intro-pcap)

- Your coworker has bet that you can't see what they just downloaded over the Internet.
- Little did they know you were actively recording packets from their machine the entire time, because you're the network administrator.
- What did they download?
- (Hint: You access websites using HTTP)



Flag format: MINUTEMAN{__flag__text__here__}

<https://training.umasscybersec.org/challenges>

OK, now you know a little about network forensics. But what about physical data?

Image analysis

- One of the most common tasks for a forensic analyst is to make virtual images of physical evidence.
- This is often accomplished with a specialized software for phones, or through the use of a “drive toaster” for a computer.



Filesystems: How are files stored?

Different file systems have different standards for where and how data is retrieved/stored. Usually (but not always) tied to your OS:

- NTFS (Windows)
- ext4 (Linux)
- FAT32 (cross-platform)

If this looks like nonsense, don't worry!

We'll look at an abstraction of a file system in the next slide.

Where are your files, really?

Process 1
File descriptor table

fd	flags
0	- ①
1	-
2	-
3	O_CLOEXEC ②
9	- ③

Process 2
File descriptor table

fd	flags
0	- ④
1	-
2	- ⑤
3	O_CLOEXEC ⑥

Open file description table
(system wide)

position	status flags
0	- ⑧
239	O_APPEND, O_SYNC ⑨
32	O_DIRECT
9301	-
0	-

inodes
(system wide)

inode	path (for simplicity) ⑦
3	/dev/pts/0
31031	/var/lib/file.db
4	/dev/pts/1
89085	/tmp/out.log

Let's say you delete this file.

What happens here?

Data can be stored in disk, RAM....

The Sleuth Kit

- One of the better command line programs for disk image analysis is called The Sleuth Kit.
- The Sleuth Kit can read file system information from a disk, and display it to you without the need to boot the disk up.
- We'll (potentially) go over a few of it's tools - mmls, fls, and icat - in future talks.



Image Analysis: some resources

Making images of devices you don't own is... questionable. Good thing knowledge is free.

There are **many** images and practice materials available for you to practice:

- [Digital Corpora](#) has a *ton* of different scenarios and some walkthroughs.
- [PicoCTF](#) for more general forensics and smaller images
- Also consider taking CS365 Digital Forensics

Metadata



- Sometimes the facts *about* your data are more important than the actual contents.
- A **lot** of valuable information comes from the “data about the data” you want to analyze
 - Metadata and data might not be stored in the same place!
- For example: images!
 - Location data
 - Camera information
 - Author/owner
 - Timestamp

Another scenario (minute-meta)

- Your programmer friend who *just* learned how to use `exiftool` has sent you an image.
- Apparently there's a message for you in it, somewhere...

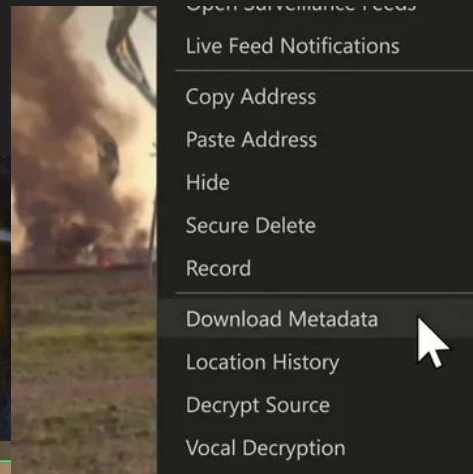
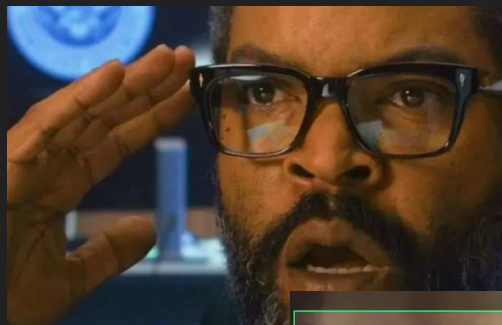
Open a terminal!

Linux: `apt install exiftool`

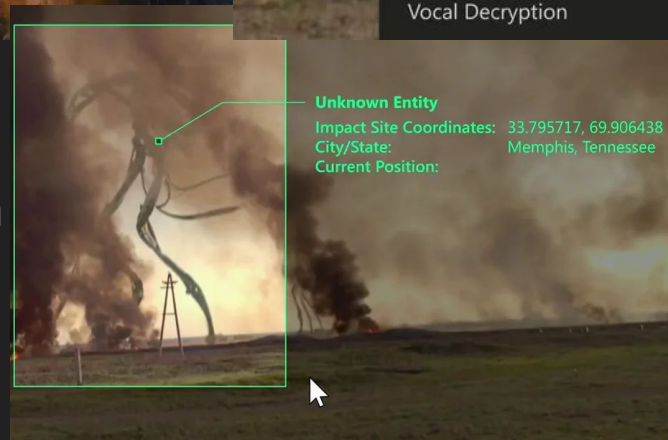
Windows:

<https://exiftool.org/index.html>

Flag format: `UMASS[__flag__text__here__]`



100%
realistic
depiction



Binwalk & magic numbers

- Binwalk is a general purpose file extraction tool
- Every file on a computer has what's called a "magic number" at it's beginning. It functions as a file signature so the computer knows how to process the file when it reads it.
- Binwalk scans a file for other internal file signatures, then extracts the files if they match the format indicated by the magic numbers.
- Binwalk is incredibly useful - it can be used to perform full filesystem extractions, find hidden information, and more.



Linux commands

- Linux has a command called `file` that can tell you information about a file based on its magic numbers.
- The command `ls -lah` will tell you information about when a file was created. The information can be changed easily though, and should only be relied on to confirm something you already suspect.
- Both are pre-installed on most Linux distributions



An aside on CTF Forensics: Steganography

- Steg is essentially the practice of “security through obscurity”
 - Hiding data in seemingly mundane data (usually in an image)
 - can be super duper obscure or really easy depending on your approach

There are a litany of tools you can chuck at a CTF steg challenge:

- binwalk (for finding hidden file signatures)
- exiftool (for parsing image metadata)
- [stegsolve](#), zsteg
- strings

However, more complex problems require you to know either a) *how* the data was hidden or b) be *really* familiar with the structure of certain files.

Thanks for coming!

Now for some advertisements...

Women in Cybersecurity (WiCyS)

- National Organization that aims to uplift and encourage minorities in cybersecurity especially women
- **Scholarships** for members/special conferences from parent organization
- Opportunities for **free** certifications!



NECCDC Applications open soon!

If you're interested in blue teaming, this is a competition where you defend a simulated corporate network against industry professional hackers!

- Fill out our interest form!
- Application materials will be released next week.

Interest form



Join us on Friday for a CTF!

Play an international CTF alongside the team, or get guided practice on our training platform!

Friday, 9/26 | 4-7 PM | LGRC A104

(Rootkit Part 2 Delayed)



You thought
we were the
only club?

PIT
event
alert!

THE DIGITAL WALLET INSECURITY



Professor Taqi Raza



Wednesday, 24th September 2025



6PM - 7PM, Rm A104 (Makerspace) LGRC



Free Dunkin' Donuts!!

Questions?

How do I learn more?

How can I get involved?

When are you guys available?

Come Up & Ask!

Resources Posted in Discord

Newsletter



Discord



Twitter



Website



CTF Demo Time!