

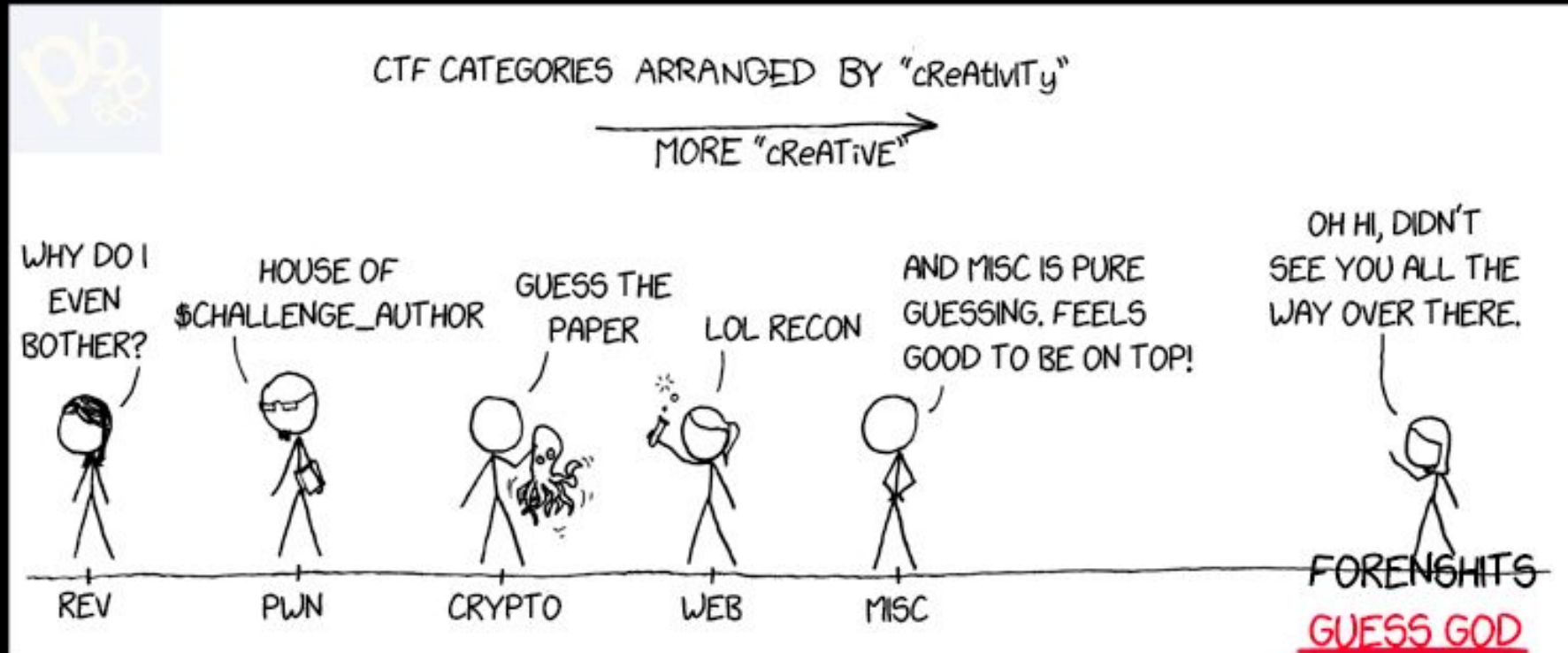
# Week 08

# Forensics

hidden things go brrr



# sigpwny{kiboff\_with\_your\_head}



# Announcements

3 Open Meeting Spaces!!!

Merch form but for real this time

halloween shenanigans this sunday yay



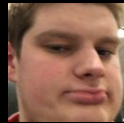
# What is forensics

- Analysis of computer systems information
  - Different from OSINT (Some of the info can be private)
  - Often after the fact to try and understand what happened.
- Types of Forensics
  - File forensics (metadata analysis, strings, grep, clear patterns)
  - Steganography (lsb, image and audio steg)
  - Memory forensics (ramdumps, cpu dumps etc)
  - Network Forensics
  - Systems / Org Forensics



# Forensics

- Forensics is a very wide field (just like security is a wide field)
  - We have some basic challenges here today
- Think about assumptions that you have about files
  - Is a PNG just a PNG, or is there hidden text in it.
  - PNG's can also be ZIPs
- Metadata
  - What information is attached to a file
  - Dates
  - Location
  - Everything Else
- Modified Files
  - Steganography :thomasoof:



# Basic Forensic Tools



# file

Determine the file type of a file (what it really is)

Is a file really what it says it is? Can a file be opened in a different way? Don't always trust the extension!



# strings

see what strings exist in a file

valuable when a file is a binary

- can give useful information about functions, variables, static values etc





# xxd

prints a hexdump of a file

Good to look for recognizable hex patterns (file headers).

```
00025a40: d508 de91 1600 65b9 c62a 9b8b ac88 d919 .....e.*.....
00025a50: 4f3b 881d 7db3 5f44 5df8 5b50 9dca 468c 0;...}_D].[P..F.
00025a60: 8a79 24f6 ac65 f0f4 f681 8301 28cf f10e .y$.e.....(...
00025a70: 723b d2df 7339 ad74 3c54 df6a 2aa3 134a r;...s9.t<T.j*..J
00025a80: a8bf 2e00 207f 2a85 6eae 4b98 9f73 2677 .... *.n.K..s&w
00025a90: 6587 24d7 b31d 325b 8244 8385 e76e 318a e.$...2[.D...n1.
00025aa0: 8e5b 2893 f773 c48c 0f4e 0722 856e c16e .[(...s...N."n.n
00025ab0: e78e 4aeb 2b0f 3214 639e 8475 f635 1cc9 ..J.+2.c..u.5..
00025ac0: 6aac d1dd 58c6 08ec 3230 6bd5 e7d0 ac2e j...X...20k.....
00025ad0: 6310 4702 c6cb cef1 eddb 3597 2784 6da4 c.G.....5.'m.
00025ae0: 712f 9ecc 641b 8871 8c13 44af d06a 299e q/..d..q..D..j).
00025af0: 4e6d 74f6 20c9 091e 841e 950b 5858 1001 Nmt. ....XX..
00025b00: 99a3 1eb8 cd7a 4bf8 30bc a434 db42 9c60 .....zK.0..4.B.`
00025b10: 6315 5ae3 c39f 67b9 fb3c 7961 b4b6 ec71 c.Z...g..<ya...q
00025b20: c569 cc4a a4cf 3e9f 488b cc1f 67b9 322e .i.J..>.H...g.2.
00025b30: 38ca e2a9 1d26 52a5 4b2b 919c 66bb 49ec 8....&R.K+..f.I.
00025b40: ae61 6cf9 7e62 0efd eb39 a326 4236 141d .a1.~b...9.&B6..
00025b50: f230 2ab9 d8a7 4dbd 9181 1e95 a8c4 108e .0*...M.....
00025b60: fd08 6aaf 3457 a1bc cdae ac9c 6715 d288 ..j.4W.....g...
00025b70: e577 f31b 2a07 0067 a8f5 a97c eda8 487c .w...*.g...|..H|
00025b80: 03c7 d6a1 c8c9 d267 2524 f76f f248 0918 .....g%$.o.H..
00025b90: e7e5 aaf9 ff00 63f4 aec6 4f99 3681 9350 .....c...0.6..P
00025ba0: 7952 ff00 cf31 f90a a524 4b8b 3fff d9 yR...1...$K?...?
```



# grep

Find text within files!

```
grep -r "text you want to find" .
```

```
grep -A -B -C -r "text you want to find"
```

```
cat <FILE> | grep
```



# Metadata

its data... but meta



# Metadata

Data... but meta (No not Facebook's new name)

Metadata is data about data

- When something happens, how big something is
- Statistics and relevant information that isn't the actual data, but may be critical to allowing the data to function (file size)
- Enough metadata put together can often re-create some amount of the real data.



# Metadata Tools

inode

exiftool

Image metadata tool



# Exiftool

View all the metadata of a thing

**Metadata:** Data about data

How big is this image?

When was it made?

Where was it taken?

```
smv@maskine:~/Downloads$ exiftool 20160730_205039.jpg
ExifTool Version Number      : 12.16
File Name                    : 20160730_205039.jpg
Directory                   : .
File Size                   : 2.8 MiB
File Modification Date/Time  : 2016:07:30 20:50:40+03:00
File Access Date/Time       : 2021:08:14 07:50:57+03:00
File Inode Change Date/Time  : 2021:08:14 07:50:57+03:00
File Permissions             : rwxrwxrwx
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
GPS Altitude Ref             : Above Sea Level
Camera Model Name           : LG-D855
Y Cb Cr Positioning         : Centered
Resolution Unit              : inches
Y Resolution                 : 72
Orientation                  : Horizontal (normal)
Color Space                  : sRGB
Create Date                  : 2016:07:30 20:50:39
F Number                     : 2.4
Focal Length                 : 4.0 mm
White Balance                : Auto
Exif Image Width             : 4160
Sub Sec Time                 : 773022
Metering Mode                : Center-weighted average
Date/Time Original          : 2016:07:30 20:50:39
Sub Sec Time Digitized      : 773022
Warning                      : Invalid EXIF text encoding for UserComment
User Comment                 : NightShot ProcInfo Gain=15,N_M=2,OBC=6,Y=1,C=1,Sharp=700,LuxM
ode=5,FaceNum=2 FocusArea=11111111
Components Configuration    : Y, Cb, Cr, -
Exif Image Height           : 2340
Flash                       : No Flash
Exif Version                 : 0220
Interoperability Index      : R98 - DCF basic file (sRGB)
Interoperability Version    : 0100
Exposure Compensation       : 0
ISO                          : 700
Flashpix Version            : 0100
Sub Sec Time Original       : 773022
Digital Zoom Ratio          : 1
Exposure Time               : 1/12
X Resolution                 : 72
Make                        : LG Electronics
Thumbnail Length            : 26617
```



# Steganography

oh god oh frick oh god oh frick oh god oh frick oh god oh frick oh god oh



# Steganography

- Hide data in other data
- Inherently guessy during CTFs
  - Try lots of ideas
  - Waste lots of time
  - Use statistical approaches if applicable



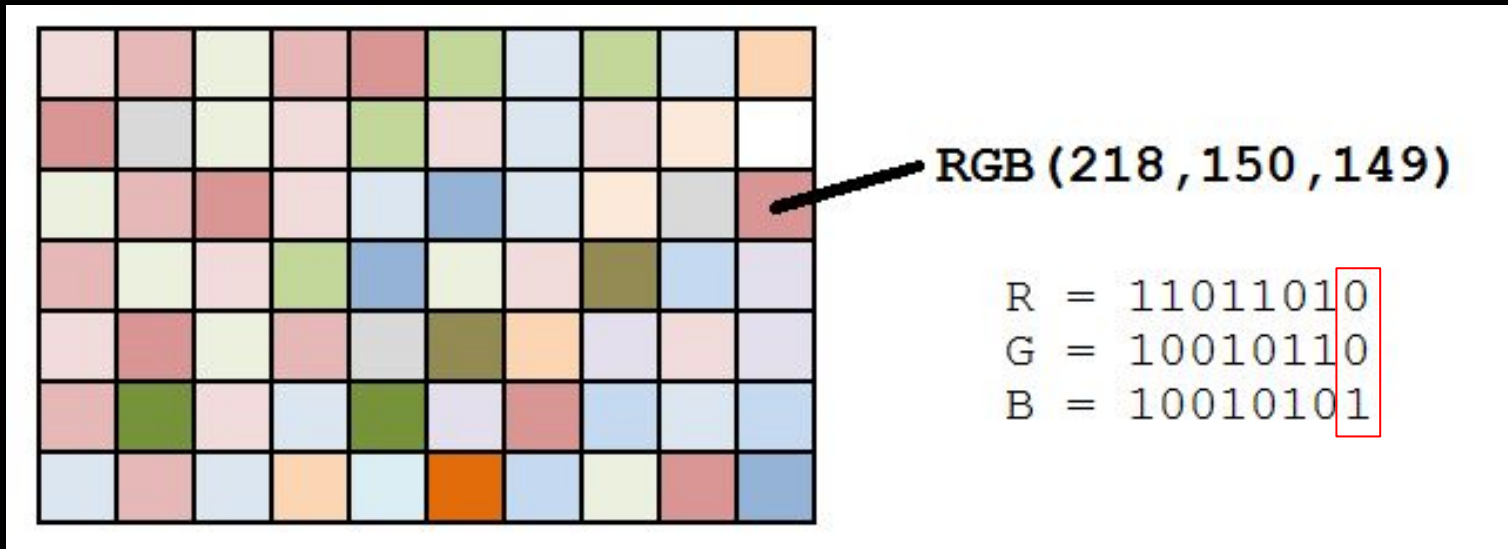


# Image Stego - LSB

- LSB (least significant bit) encoding
- Not really useful in the real world, but CTFs love it
- Take the least significant bit (last bit) of each color byte and concatenate all of them to form a message
- Image is mostly visibly unchanged



# Image Stego - LSB



Message =  $(R \& 1) \parallel (G \& 1) \parallel (B \& 1) = 001\dots$



# Can you tell the difference?



Original



LSB Encoded



# Other Stego

## Audio stego

- 90 % of the time it is a spectrogram
- The other 10% is either
  - SSTV
  - Some frequency modulation
  - Some other guessey home-brewed bullshit
- Most audio stego can be solved with tools



# Memory Forensics



# Memory Forensics

Looking at memory dumps to try to find valuable information.



# Foremost

Data recovery tool

Can recover deleted files from a mount

Can find hidden files inside a drive / file

Also use binwalk

```
Terminal - wikipedia@linux:~
File Edit View Terminal Go Help
wikipedia@linux:~$ foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w|-d] [-t <type>] [-s <blocks>] [-k <size>]
  [-b <size>] [-c <file>] [-o <dir>] [-i <file>]

-V - display copyright information and exit
-t - specify file type. (-t jpeg,pdf ...)
-d - turn on indirect block detection (for UNIX file-systems)
-i - specify input file (default is stdin)
-a - Write all headers, perform no error detection (corrupted files)
-w - Only write the audit file, do not write any detected files to the disk
-o - set output directory (defaults to output)
-c - set configuration file to use (defaults to foremost.conf)
-q - enables quick mode. Search are performed on 512 byte boundaries.
-Q - enables quiet mode. Suppress output messages.
-v - verbose mode. Logs all messages to screen
wikipedia@linux:~$
```



# Network Forensics





# Network Forensics

Looking at packet captures, network traffic.

Good to get an understanding of what happened within a network.



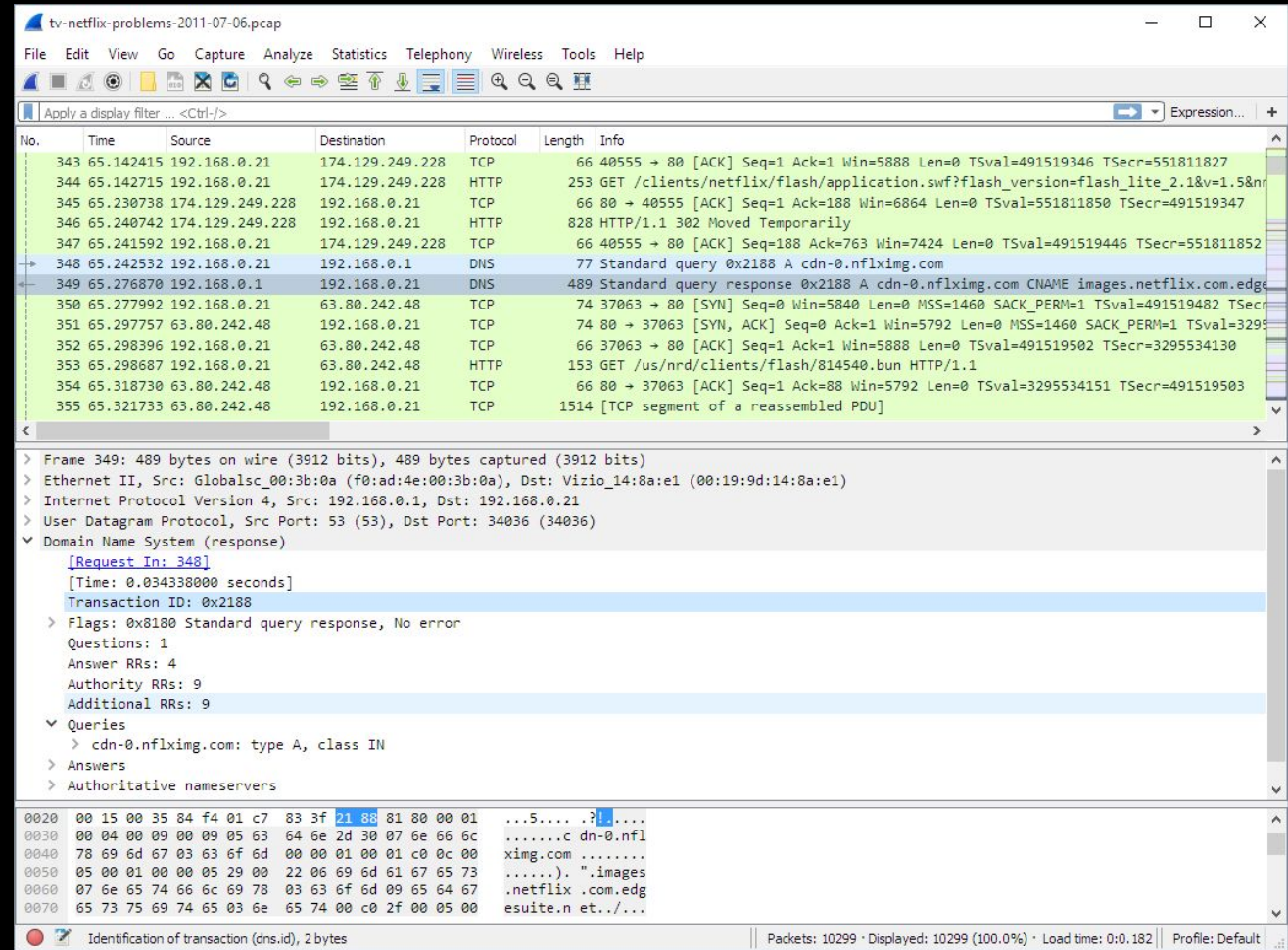
# Wireshark

Network packet analysis

Really good filtering

Can follow conversations and view individual packet values

Will do longer wireshark meeting later



The screenshot displays the Wireshark interface for a capture file named 'tv-netflix-problems-2011-07-06.pcap'. The main pane shows a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 349 is selected, showing a DNS Standard query response from 192.168.0.1 to 192.168.0.21. The packet details pane below shows the structure of the DNS response, including flags, questions, answer RRs, and authoritative nameservers. The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edg...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=329534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=329534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]



# Systems / Org Forensics

Kibana was interesting...



# Systems / Org Forensics

Forensics is really hard to do at scale

Enter: Org tools (many are expensive)

**EX:** Secconion, Kibana, Velociraptor, Akira/Akimba/A-something

Many cost a lot of money, but it's good to know they exist.

**TracerFIRE** coming to UIUC soon!



# Other Misc Forensics Tools

- Foremost - File Recovery
  - OutGuess
  - Wireshark
  - Exiftool
  - Like a bajillion steganography tools you can find & use online
  - Kibana :sadge:
  - Tons of stuff that are big expensive
- 
- Tons of CLI tools (strings, Grep, file etc).



# Next Meetings

## Weekend Seminar: Spooky SIGPwny Summary

- Who SIGPwny is
- What we do (all-in-all and this semester)
- What our plans are as we can be in more person (next semester/year)

## Thursday: The end game within security (The Jobs Meeting)

- End goals for security careers (CISO, Pentesting, gov, etc.)
- How to incorporate security into a non-security career.
- Likely longer form meeting
- **Might switch to OSINT if people want.**



# Specific Tools For Today's Challenges

- Wireshark
- binwalk
- strings
- file
- xxd
- Online LSB tool like <https://stegonline.georgeom.net/>

