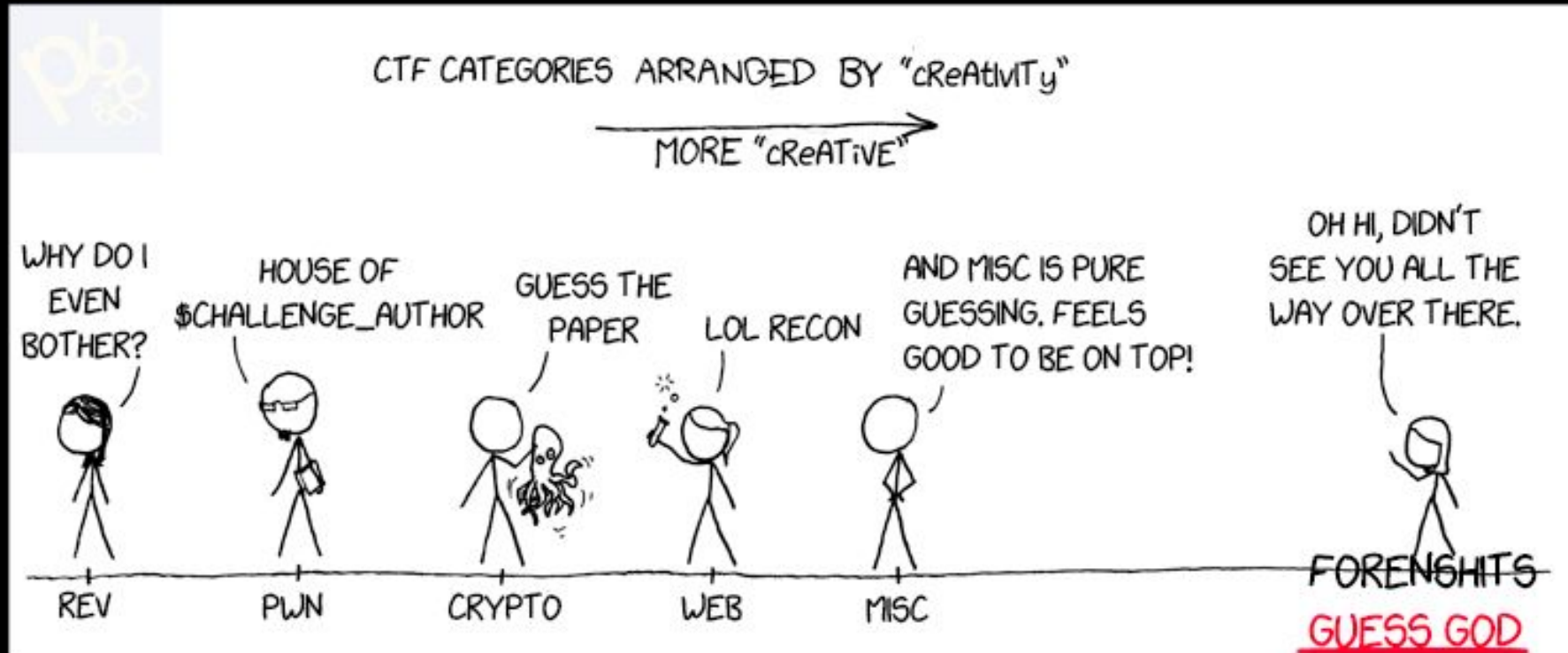# Week 08
# Forensics

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 is 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).

# 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=111111111
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
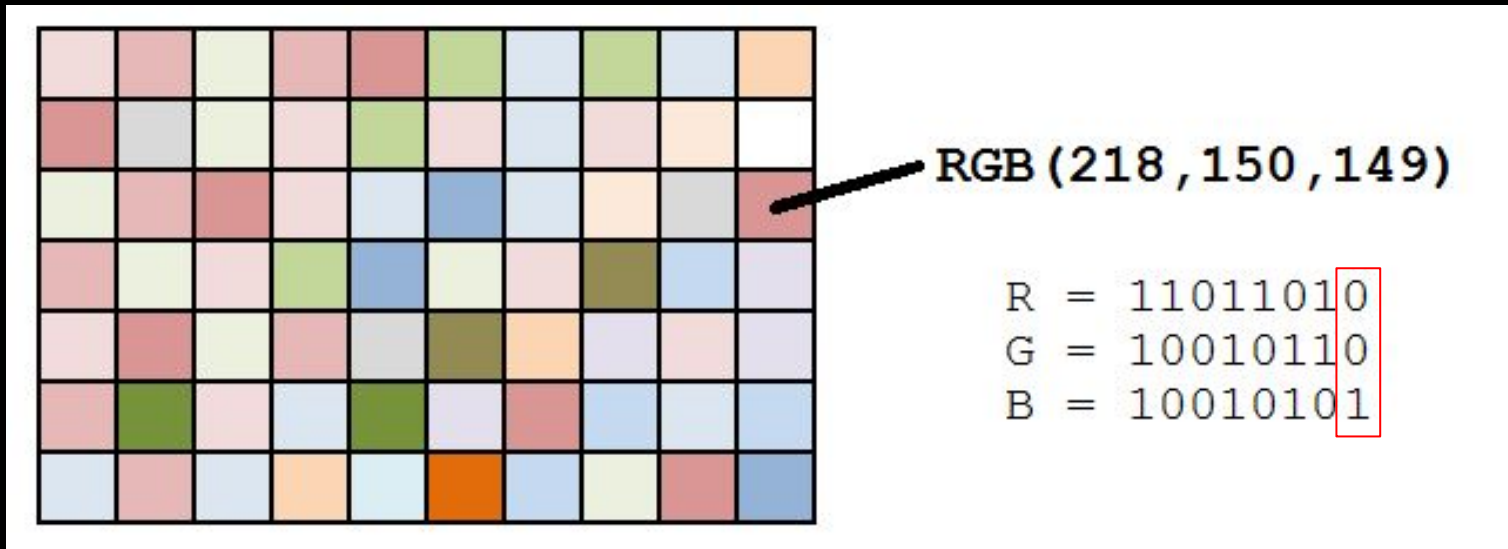  - Use statistical approaches if applicable

# 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



RGB(218,150,149)

R = 11011010
G = 10010110
B = 10010101

Message = (R & 1) || (G & 1) || (B & 1) = 001...

# 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 guessy 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.
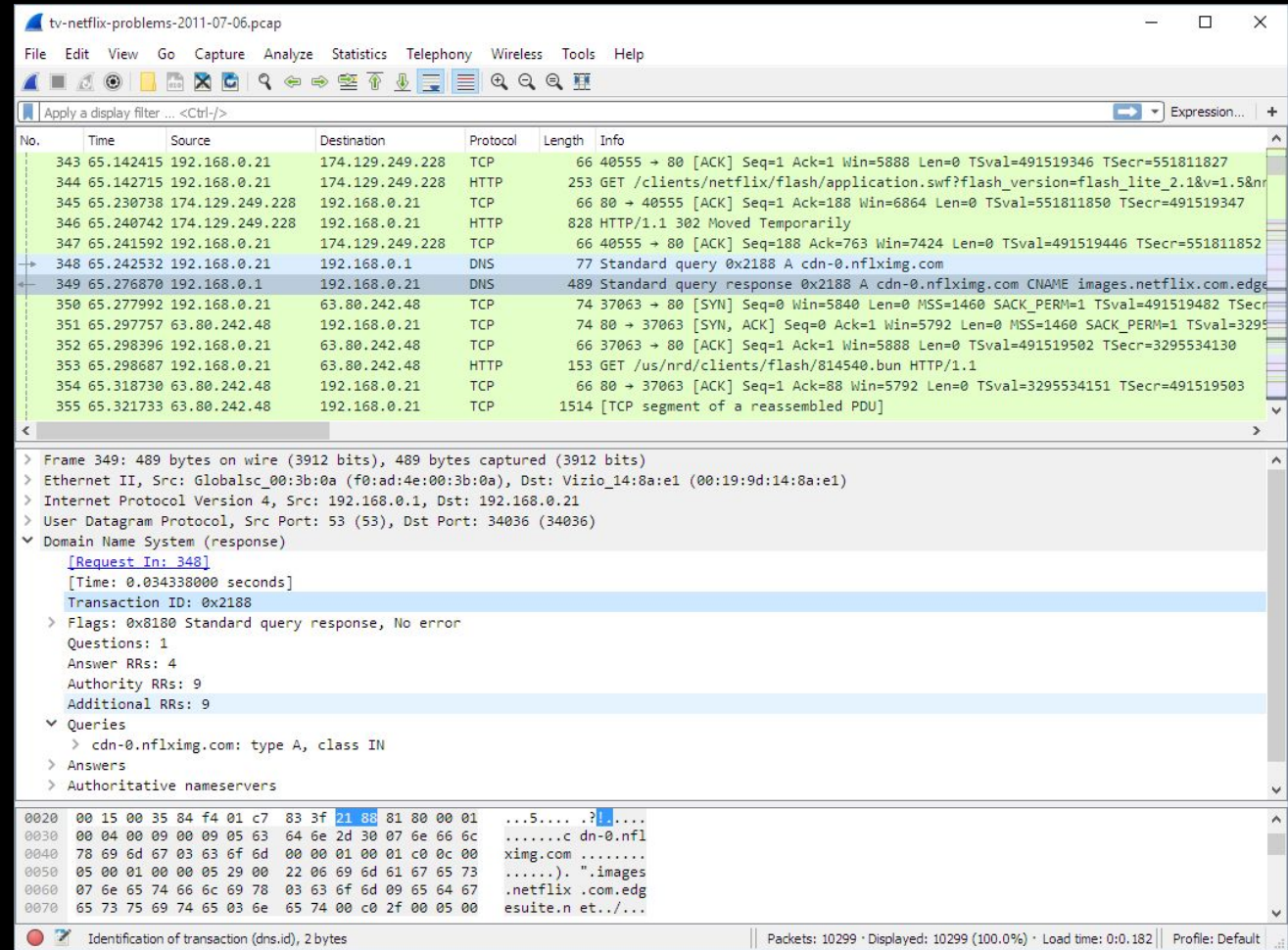
# Wireshark

Network packet analysis

Really good filtering

Can follow conversations and view individual packet values

Will do longer wireshark meeting later

# Systems / Org Forensics

Kibana was interesting...

# Systems / Org Forensics

Forensics is really hard to do at scale

Enter: Org tools (many are expensive)

**EX:** Seconion, 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/