Intro Forensics

Pranav & Ian “it’s still halloween in some time zones” Klatzco, challenges & slides borrowed from friends @ UW (Batman’s Kitchen)

DOWNLOAD THESE FILES

Things we'll cover

concepts:

- file formats
- network protocols
- steganography

tools:

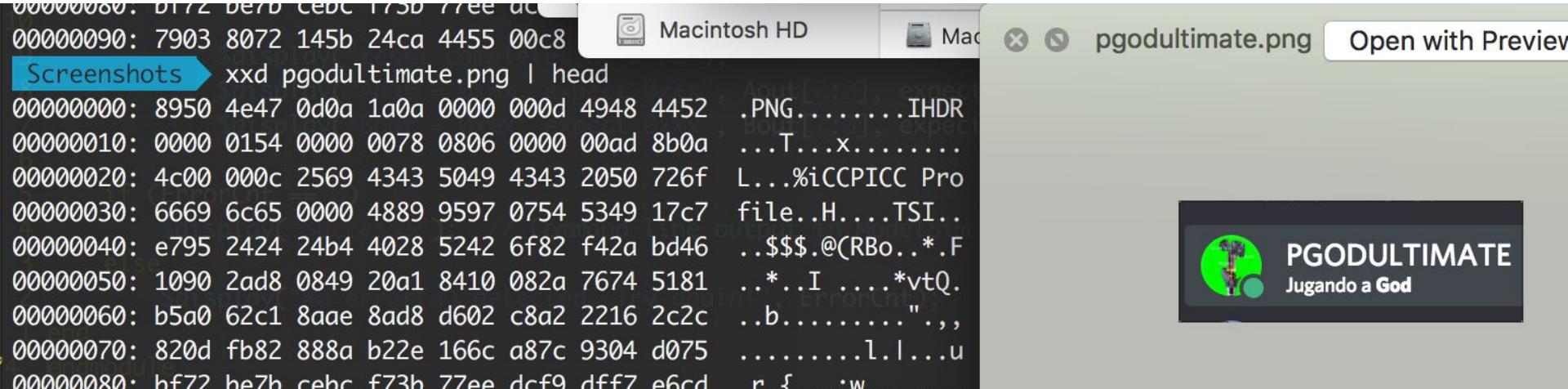
- foremost
- wireshark
- stegsolve

Jobs in this field that use forensics skills

- Incident Response - looking at things post-hack
- Malware Analysis - obfuscated exfiltration methods
- These skills are general and make you better at using a computer (but that’s true about pretty much anything you learn so...)
- I don’t really know! Feel free to DM me / throw out suggestions.

Magic Number

- File formats usually start with a sequence of bytes
- how does the **file** utility work? usu. by checking magic #s
- you can check with: **xxd filename | head**
- This is useful for identifying files!

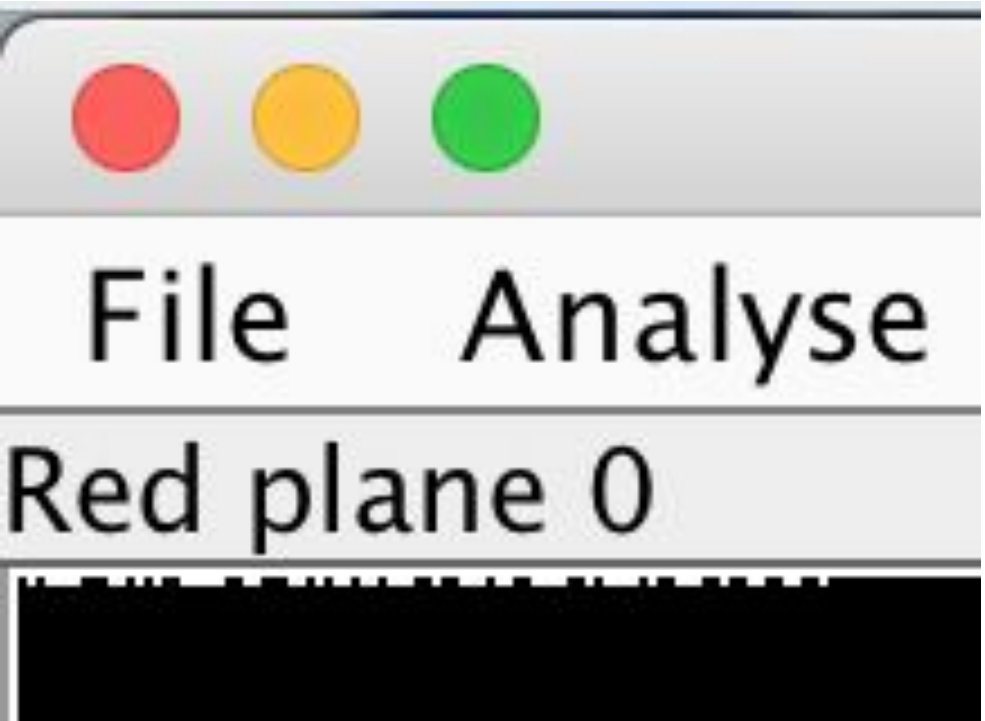


Foremost quick usage:

- It is a “file carver” — used for recovering files from disk images
- looks for headers (magic numbers, footers, data structures)
- **apt-get install foremost** or **pip install foremost**
- foremost -i input_file # will create output/ with results, if any

Try: animals.dd challenge

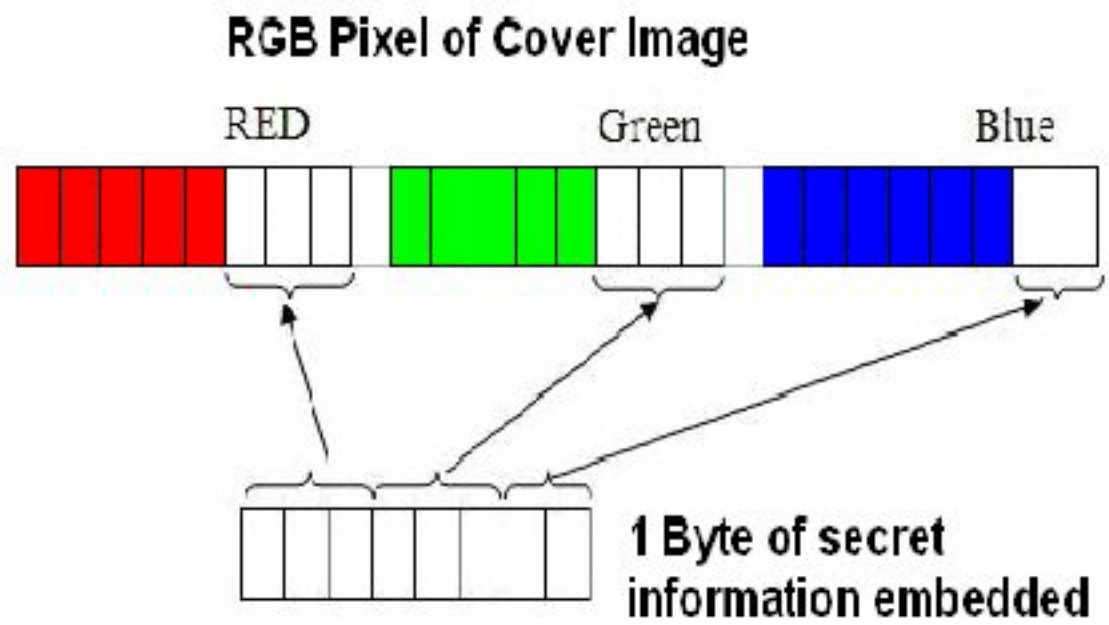
Steganography: hiding things in files



- RGB: LSB of an image
- sometimes you have to hunt for the right tool, sometimes you have to write your own

< stegsolve

Steganography: hiding things in files

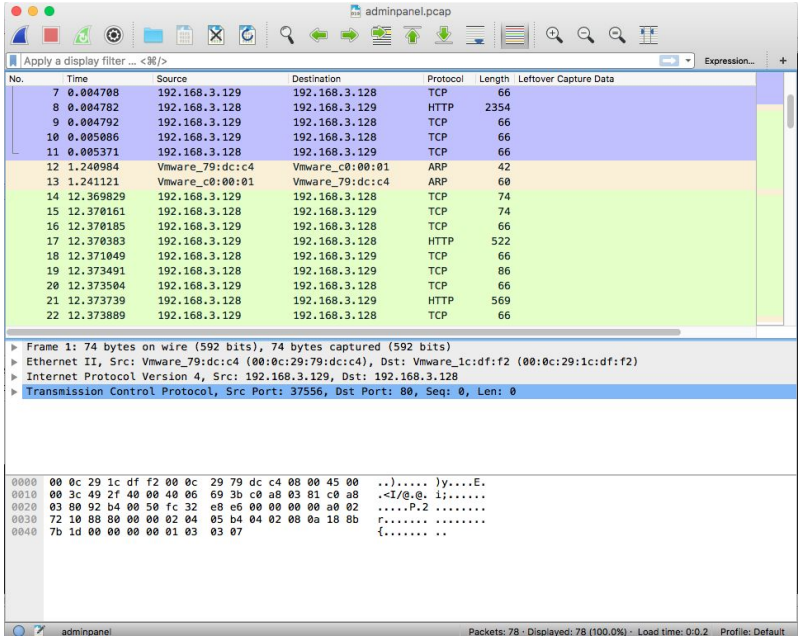


Wireshark

- tool for analyzing network protocols
- very useful for day-to-day
- fun with wireshark: finding 0days @ DEF CON CTF

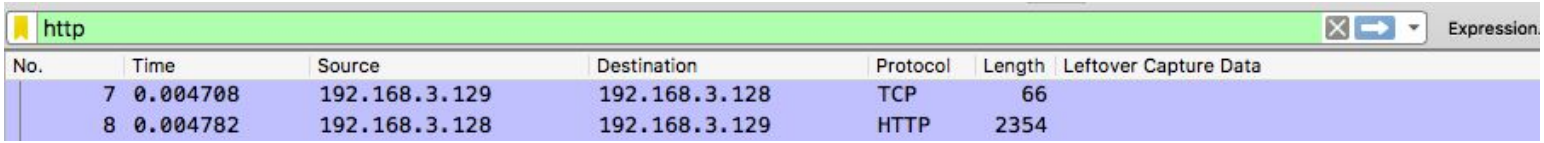
Adminpanel.pcap challenge!

Step 1: open wireshark with data

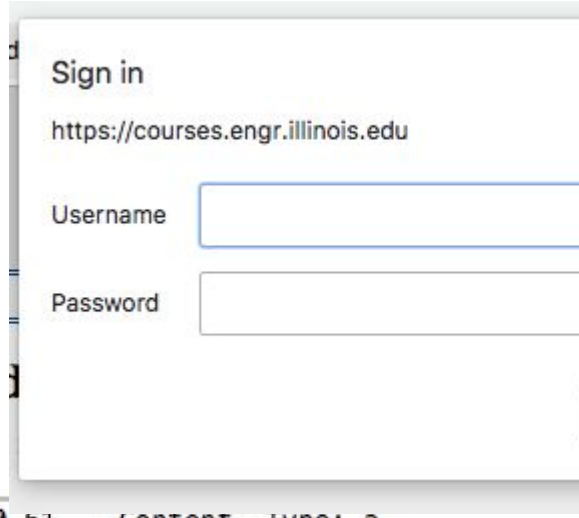


Adminpanel.pcap challenge!

Step 2: Filter relevant data



Adminpanel.pcap challenge!



Step 3: Look at useful info and read!

Info
GET / HTTP/1.1
HTTP/1.0 200 OK (tex
POST /login HTTP/1.1
HTTP/1.0 302 FOUND (
GET /admin HTTP/1.1
HTTP/1.0 200 OK (tex
GET /logout HTTP/1.1
HTTP/1.0 302 FOUND (
GET / HTTP/1.1
HTTP/1.0 200 OK (tex
POST /login HTTP/1.1
HTTP/1.0 200 OK (tex

```
0170  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 61   .Content -Type: a
0180  70 70 6c 69 63 61 74 69  6f 6e 2f 78 2d 77 77 77   pplicati on/x-www
0190  2d 66 6f 72 6d 2d 75 72  6c 65 6e 63 6f 64 65 64   -form-ur lencoded
01a0  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ..Conten t-Length
01b0  3a 20 35 33 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   : 53..Co nnection
01c0  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 55 70   : keep-a live..Up
01d0  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
01e0  65 71 75 65 73 74 73 3a  20 31 0d 0a 0d 0a 75 73   equests:  1....us
01f0  65 72 3d 61 64 6d 69 6e  26 70 61 73 73 77 6f 72
0200  64 3d 70 69 63 6f 43 54  46 7b 6e 30 74 73 33 63
0210  75 72 33 5f 31 33 35 39  37 62 34 33 7d
```

Can't just give you the answer lol

ext-super-magic.img

- ext2 is a filesystem
- it has “superblocks” that contain metadata about files
- Something has happened to one of the superblock fields!
- could it be.... the magic number????
- more info: this GNU spec or this page from OSdev wiki
- you can mount filesystems using the mount command

Get started!

DOWNLOAD THESE FILES

Flags are up on sigpwny.com