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!

```
00000080: b172 be7b cebc 173b 77ee ac
00000090: 7903 8072 145b 24ca 4455 00c8
Screenshots    xxd pgodultimate.png | head
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452   .PNG........IHDR
00000010: 0000 0154 0000 0078 0806 0000 00ad 8b0a   ...T...x........
00000020: 4c00 000c 2569 4343 5049 4343 2050 726f   L...%iCCPICC Pro
00000030: 6669 6c65 0000 4889 9597 0754 5349 17c7   file..H....TSI..
00000040: e795 2424 24b4 4028 5242 6f82 f42a bd46   ..$$$.@(RBo..*.F
00000050: 1090 2ad8 0849 20a1 8410 082a 7674 5181   ..*..I ....*vtQ.
00000060: b5a0 62c1 8aae 8ad8 d602 c8a2 2216 2c2c   ..b........".,,
00000070: 820d fb82 888a b22e 166c a87c 9304 d075   .........l.|...u
         bf72 be7b cebc f73b 77ee dcf9 dff7 e6cd   r.{..;w.......
```

Macintosh HD   Mac

pgodultimate.png   Open with Preview

PGODULTIMATE
Jugando a **God**

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

File   Analyse

Red plane 0
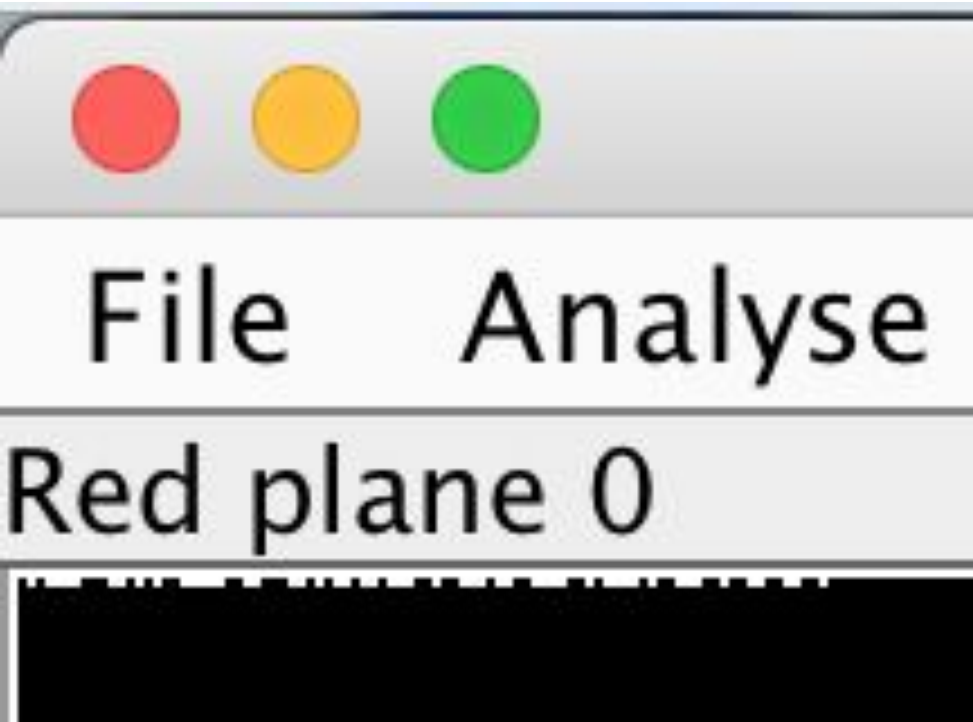
- RGB: LSB of an image
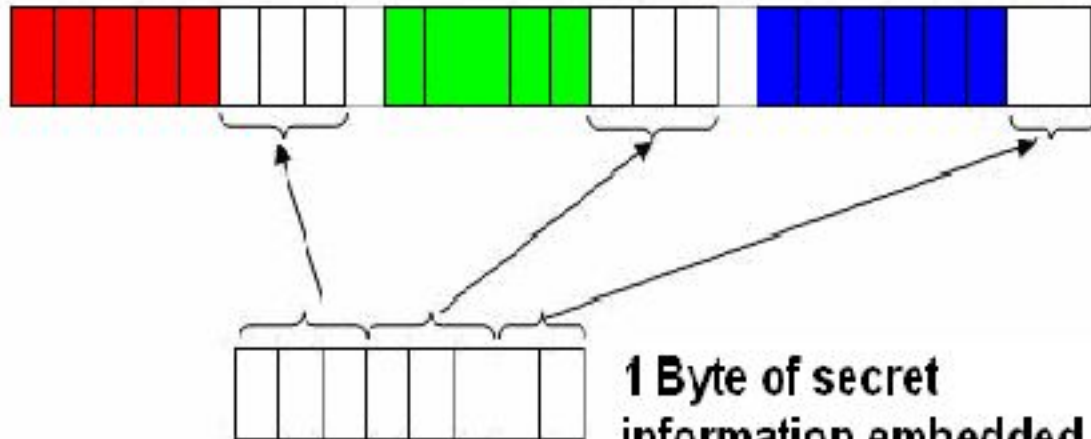- sometimes you have to hunt for the right tool, sometimes you have to write your own

< stegsolve

Steganography : hiding things in files

RGB Pixel of Cover Image

1 Byte of secret information embedded in 3,3,2 bit positions of LSB of RGB respectively of the

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

No.	Time	Source	Destination	Protocol	Length	Leftover Capture Data
7	0.004708	192.168.3.129	192.168.3.128	TCP	66	
8	0.004782	192.168.3.128	192.168.3.129	HTTP	2354	

Filter field: http

Adminpanel.pcap challenge!

Sign in

https://courses.engr.illinois.edu

Username

Password
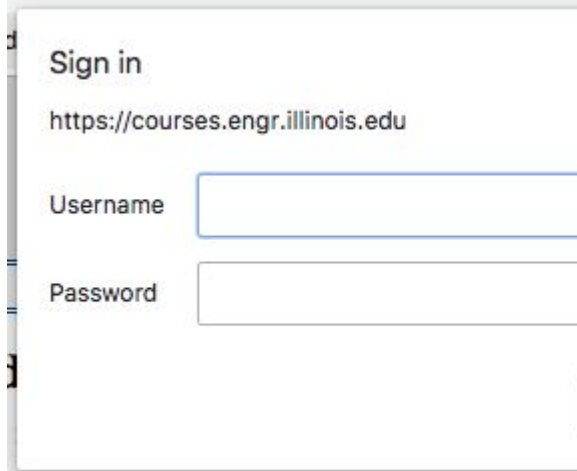
Step 3: Look at useful info and read!

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

```
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   er=admin &passwor
0200  64 3d 70 69 63 6f 43 54  46 7b 6e 30 74 73 33 63   d=picoCT F{n0ts3c
0210  75 72 33 5f 31 33 35 39  37 62 34 33 7d            ur3_1359 7b43}
```

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](#)