# Hack the planet:

## Digital Forensics

# Topics

- Kali
- Bash
- Filesystems
    - ext, fat, ntfs
- Challenges
- Network monitoring
- Memory forensics

# Getting Kali Linux working

If you haven't already, download virtualbox:

- http://www.virtualbox.org/wiki/Downloads
- (using other versions of linux is fine, just install tools as needed)

Get Kali:

- https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

Download challenges:

- Download challenges: https://goo.gl/jN5o2B

# Getting Kali working

- Start virtualbox

- File > Import Appliance > Kali.ova > continue with default options

- Start the virtual machine

https://goo.gl/jN5o2B

# What is digital forensics?

- What it is
  - Collecting evidence for use in court in criminal cases
  - Not tampering with evidence (being careful to not modify it in any way)
  - Incident response (CCDC)
- Network monitoring, detection of malware and breaches

- Typical CTF challenges:
  - recover deleted file/partition
  - examine dumped memory
  - figure out what format a file is or what it does
  - examine network traffic

# Bash

Basic shell commands:

- ls : show directory contents
- cd : change directory
- file : get file information
- cat : print file contents
- man : get a manual for a command (q to quit)
- Ctrl+c : stop execution
- (covered grep, nc last time)

(check out The Linux Command Line by William Shotts)

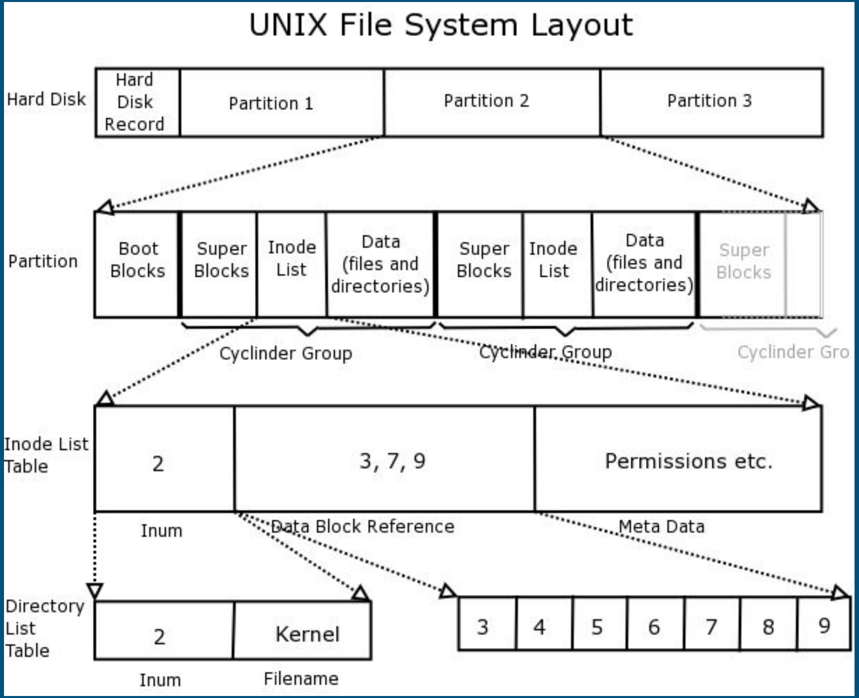
$ man cat

https://goo.gl/jN5o2B

# Basic filesystems

- Layers of operation:
  - Data layer
  - Metadata layer
  - Filename layer

- Different formats:
  - ext2, ext4, NTFS, FAT32



https://goo.gl/jN5o2B

# Ext2/Ext4 - extended file system

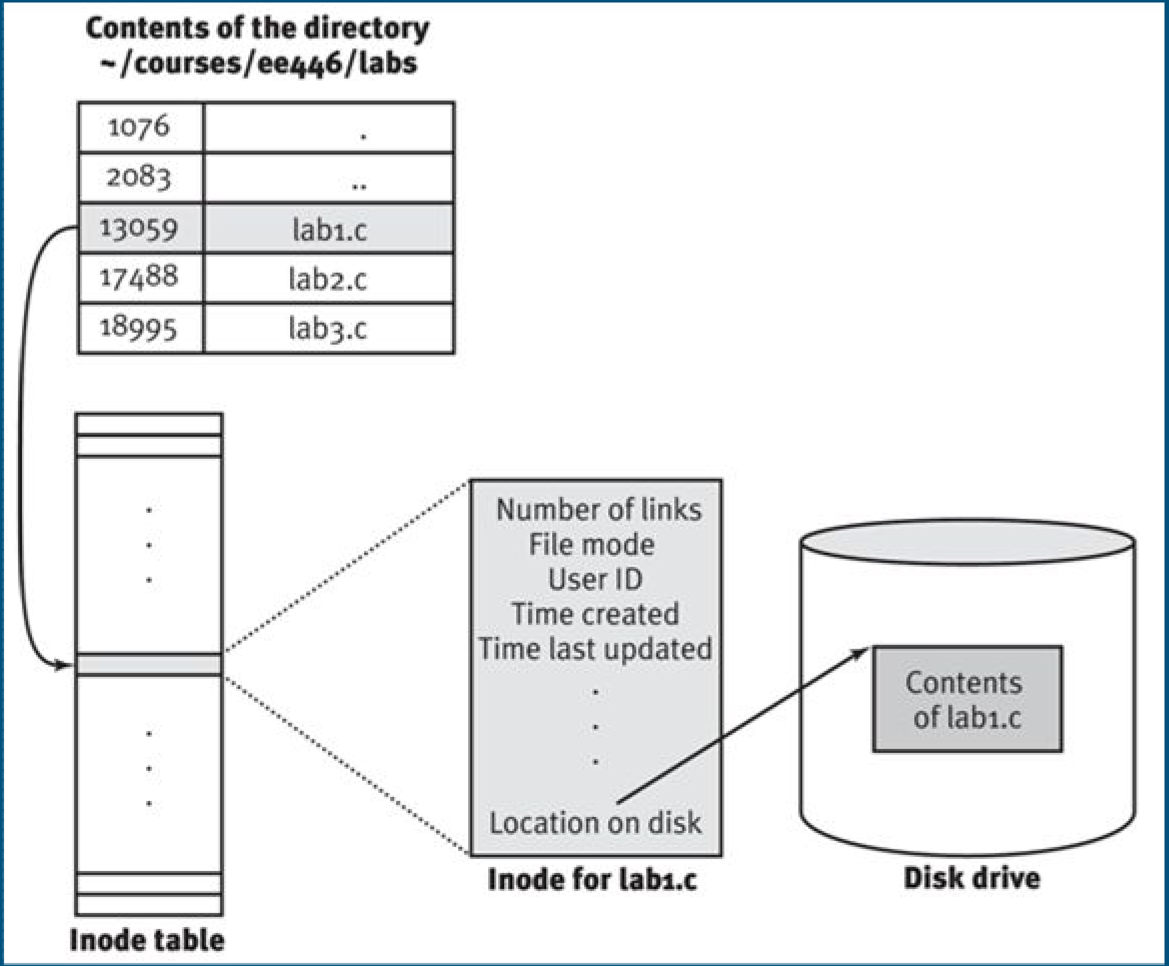
- Smallest unit is a block - 4 KB
- Each file has a corresponding inode

(containing metadata: allocated, block size, owner, permissions, number of links)

- Directory: a file containing a mapping of filename to inode
- Everything in linux is a file, even memory

- Interacting with files: stat

https://goo.gl/jN5o2B



Contents of the directory
~/courses/ee446/labs

|  |  |
|---|---|
| 1076 | . |
| 2083 | .. |
| 13059 | lab1.c |
| 17488 | lab2.c |
| 18995 | lab3.c |

Number of links
File mode
User ID
Time created
Time last updated
.
.
.
Location on disk

Inode for lab1.c

Contents of lab1.c

Disk drive

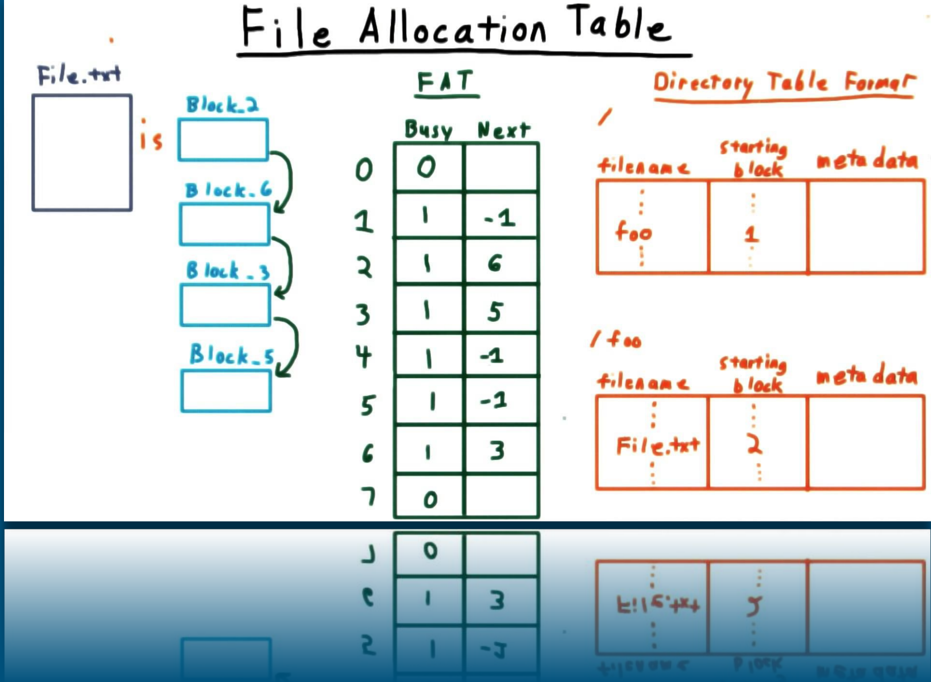
Inode table

https://goo.gl/jN5o2B

# FAT - File Allocation Table

- Smallest unit is a *cluster* (16/32 bit)
- Partition contains File Allocation Table then data
- Files are linked lists
- FAT is a lookup table
- Directory files help with lookup

- Deleted files are renamed with 0xE5 prefix and marked unallocated



FAT

|  | Busy | Next |
|---|---|---|
| 0 | 0 |  |
| 1 | 1 | -1 |
| 2 | 1 | 6 |
| 3 | 1 | 5 |
| 4 | 1 | -1 |
| 5 | 1 | -1 |
| 6 | 1 | 3 |
| 7 | 0 |  |

/

| filename | starting block | meta data |
|---|---|---|
| foo | 1 |  |

/foo

| filename | starting block | meta data |
|---|---|---|
| File.txt | 2 |  |

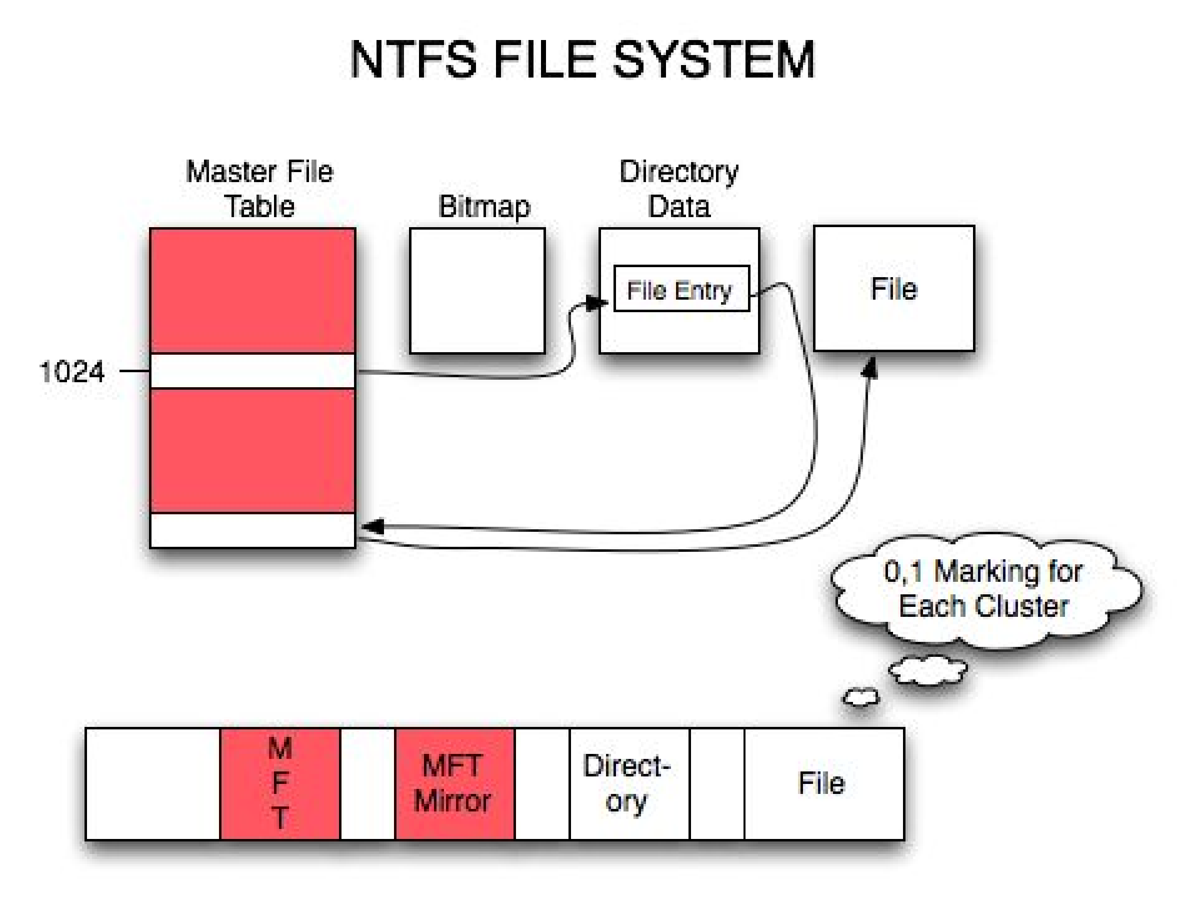
Nice youtube video: https://youtu.be/V2Gxqv3bJCk

# NTFS

- Journaling filesystem: changes are logged before being written
- Master File Table (MFT):
  - Stores metadata for each file (filename, attribute (stores a small file up to 1024 bytes), allocation status)
  - Bitmap file keeps track of which clusters are used
- Cluster sizes vary: 512 bytes to 64 KB

- After deletion, if the MFT record still exists, the clusters can be traced
- Otherwise, some information can still be recovered

https://goo.gl/jN5o2B



https://goo.gl/jN5o2B

# Tools to explore/examine filesystems

- dd - bitstream copy
- FTK Imager : examine filesystem dumps, take memory dumps
- **Autopsy/The Sleuth Kit**

- EnCase Forensics : examine MBR (master boot record), usual examination tools (paid software)

# Recovering deleted files

Idea:

- deleted files are just unlinked from the filesystem
- If you can find the right blocks, you can read file contents

Using TSK (sleuth kit):

| | |
|---|---|
| fsstat [image] | : get filesystem type |
| fls -f [type] [image] | : like ls, but shows deleted files beginning with a * |
| icat -f [type] [image] [inode #] | : cat, using the inode number |

https://goo.gl/jN5o2B

# File Carving

File signatures, magic numbers

xxd/hexdump

Tools: foremost, binwalk

syntax:

```
foremost  [file]
binwalk    [file]              : lists file types found
binwalk -e [file]              : extracts files
```

(demo: file carving from challenge 1)

https://goo.gl/jN5o2B

# Submitting corrupted homework

Hint: documents are just zip files

Check man page for zip

# Network monitoring

- Packet captures
- Live network monitoring

- Play with wireshark, monitoring your own traffic (demo)

https://goo.gl/jN5o2B

# Memory dumps

- Memory dumps are more complex

- LiME : linux memory extractor -- load lime module and it dumps memory
- Use Volatility to analyze memory dumps

- Cold booting (see extra challenge)
    - https://citp.princeton.edu/research/memory/

https://goo.gl/jN5o2B

# Guide to volatility

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

Usage: vol.py -f [filename] *command*

- imageinfo : inspects the image for a known operating system
- pslist : list processes on the process tree
- psscan : similar to psscan, but finds unlinked or inactive processes

Check registry options on the reference page

> Come to Sieg/ask on slack if you're interested in this kind of thing and get stuck/want more information

# Misc challenges / Resources

- Many ctfs have miscellaneous categories
- Often involve guessing, but past knowledge is useful
- Audio captures - look for patterns, maybe decoding/denoising
- Keyboard captures - key presses and releases correspond to events with codes (see http://www.usb.org/developers/hidpage/Hut1_12v2.pdf pages 53-55)
- Mobile forensics (ask Nick/Carson, they’re pros)
- Also check out http://www.forensicswiki.org
  and https://sift.readthedocs.io/en/latest/cheatsheet/

# Questions?

- Try more challenges, in the additional-chals/ directory
    - Do it yourself before checking solutions

https://goo.gl/jN5o2B

# Solutions

Filesystem:

```
fls -f ntfs 1-partition-lost.img
icat -f ntfs 1-partition-lost.img 29-128-1
```

Carving: https://github.com/CombustibleLemonsCTF/CAMS-CTF-2015-writeups/tree/master/carve

Corrupted doc:

https://github.com/ctfs/write-ups-2015/tree/master/icectf-2015/forensics/document-troubles

Network:

Follow tcp stream (yes, it’s that simple)