

# Mason Competitive Cyber

## Networking



# News since last meeting



- Apple patched WPA2 Krack attacks
- Georgia elections = sketchy af
  - Lawsuit filed. Trying to annul June special election & investigate evidence of election hacking
  - Election server and backups immediately wiped
  - FBI maybe has image of server
- Controlled Folder Access
  - New Windows update to prevent ransomware
  - Restricts programs from modifying folders

# Upcoming CTFs & Events

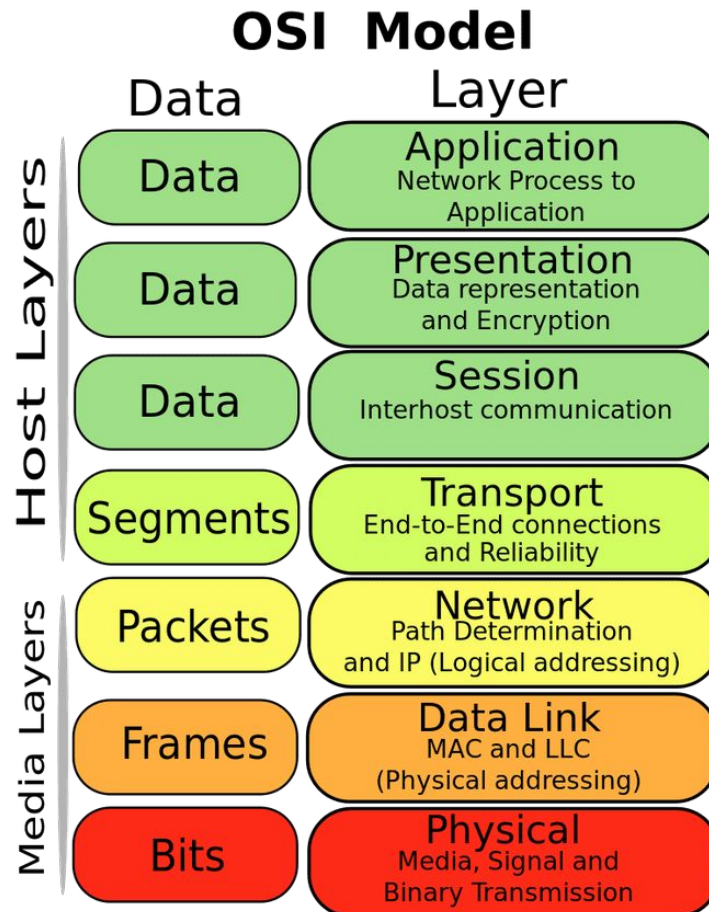


- HITCON CTF Quals
  - November 3rd 10pm - November 5th 10pm
  - Online
  - Finals in Taiwan

# Networking

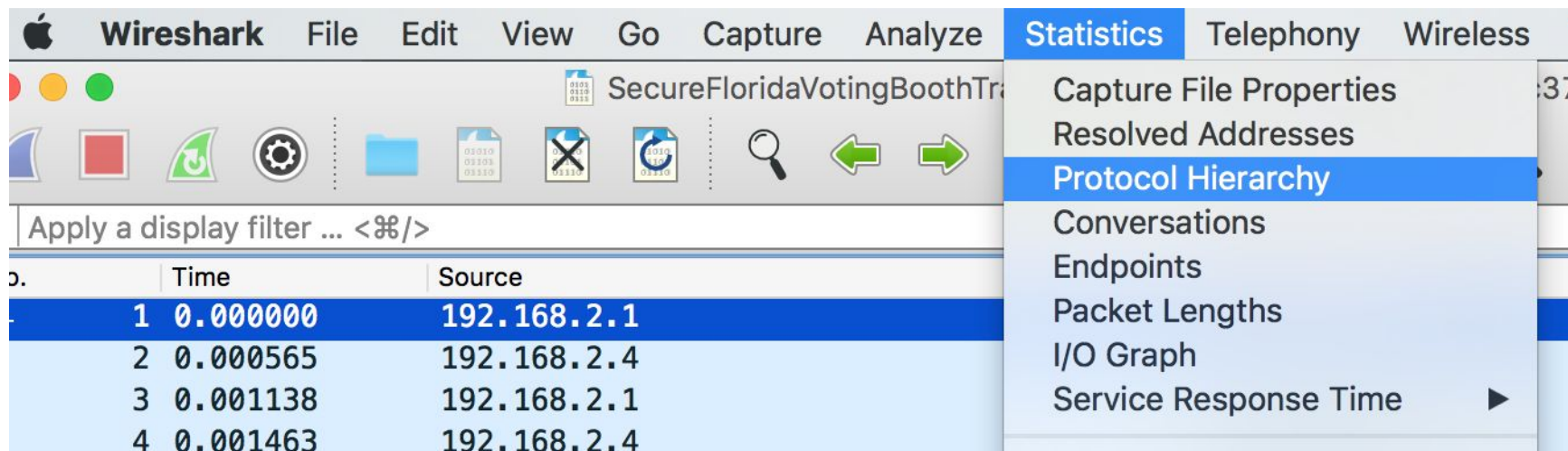


- How computers communicate with one another
  - Not going over theory of networking



# Networking in CTFs

- 1) `strings file.pcap | grep -i flag`
- 2) Open pcap with wireshark
- 3) Statistics -> Protocol Hierarchy

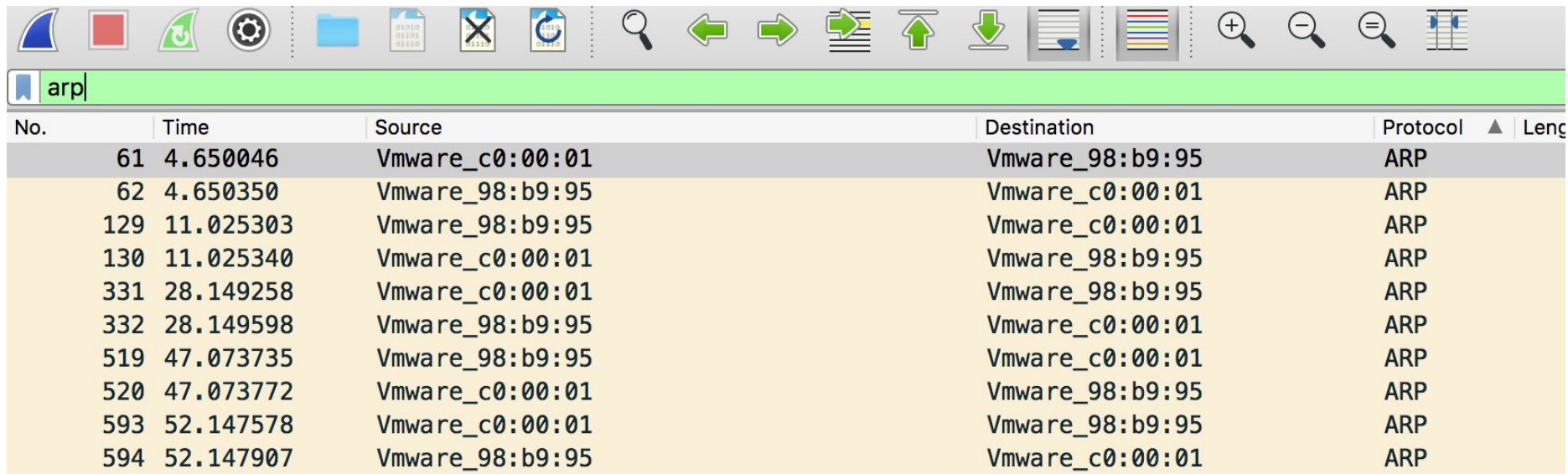




# Networking in CTFs



- Wireshark filter by protocol



The image shows a screenshot of the Wireshark network protocol analyzer. The top toolbar contains various icons for file operations, navigation, and analysis. Below the toolbar, a green filter bar contains the text 'arp'. The main display area shows a list of captured packets, filtered to show only ARP traffic. The table has columns for packet number, time, source and destination MAC addresses, and protocol type. The packets are numbered 61, 62, 129, 130, 331, 332, 519, 520, 593, and 594, all showing ARP traffic between VMware interfaces.

No.	Time	Source	Destination	Protocol	Length
61	4.650046	Vmware_c0:00:01	Vmware_98:b9:95	ARP	
62	4.650350	Vmware_98:b9:95	Vmware_c0:00:01	ARP	
129	11.025303	Vmware_98:b9:95	Vmware_c0:00:01	ARP	
130	11.025340	Vmware_c0:00:01	Vmware_98:b9:95	ARP	
331	28.149258	Vmware_c0:00:01	Vmware_98:b9:95	ARP	
332	28.149598	Vmware_98:b9:95	Vmware_c0:00:01	ARP	
519	47.073735	Vmware_98:b9:95	Vmware_c0:00:01	ARP	
520	47.073772	Vmware_c0:00:01	Vmware_98:b9:95	ARP	
593	52.147578	Vmware_c0:00:01	Vmware_98:b9:95	ARP	
594	52.147907	Vmware_98:b9:95	Vmware_c0:00:01	ARP	

icmp and ip.src==192.168.50.10

# Networking in CTFs



## Types of Challenges:

- File in a packet (zip, png, jpeg)
- Encoded text in a packet (base64)
- Audio in multiple packets

# Networking in CTFs



- 1) `strings file.pcap | grep -i flag`
- 2) Open pcap with wireshark
- 3) Statistics -> Protocol Hierarchy

.  
. .

## Types of Challenges:

- File in a packet (zip, png, jpeg)
- Encoded text in a packet (base64)
- Audio in multiple packets



# Networking in CTF Tricks



- Right Click interesting packet -> TCP -> Follow Stream
- File -> Export Objects -> HTTP -> Save all
- ngrep

# Practical Challenges & TCTF



- [malware-traffic-analysis.net](https://malware-traffic-analysis.net)
- New challenges at [tctf.competitivecyber.club](https://tctf.competitivecyber.club)
  - Networking category
  - Web challenge
  - Crypto challenge

MasonCC Training CTF

[Web1](#)

[Teams](#)

[Scoreboard](#)

[Challenges](#)

[Admin](#)

[Team](#)

[Profile](#)

[Logout](#)

## Challenges

### Networking

Jaws

50

VOIP

100

usb

250

#голос

500

# Proud Sponsors



Thank you to these organizations who give us their support:

***BATTELLE***

**It can be done™**