Mason Competitive Cyber

Wireshark and PCAP 101

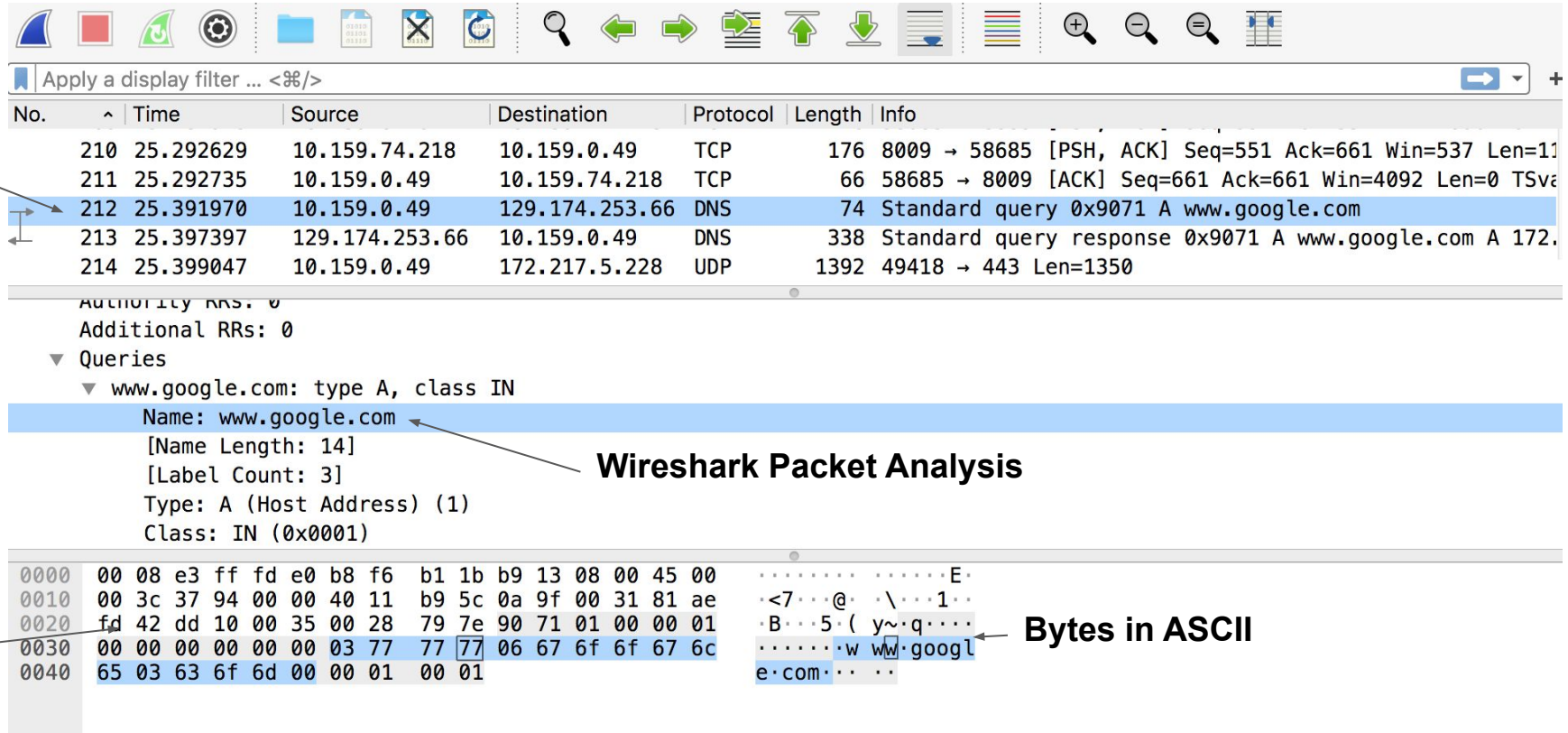
Upcoming Competitions

- National Cyber League Spring
  - Occurs throughout Spring semester
- NeverLAN (online)
  - February 8-11
  - Really great beginner CTF
- CyberFusion State Cup (Team already full)
  - February 22-23
  - Take the crown back from UVA
- VT Summit
  - March 28
- DawgCTF
  - April 11
- UMDCTF
  - April 18

Packet Captures

- Lots of CTFs have network/forensics challenges which involve .pcap files
- Typically, the Wireshark packet analyzer is the tool used to inspect these file
- Common challenges
  - Find various connection properties
  - Finding exfiltrated data
  - Capturing a file sent over the network

Wireshark Interface Basics



Packets

Wireshark Packet Analysis

Raw Bytes

Bytes in ASCII

Wireshark 101

- Apply filters (or just right-click)

Usage	Filter syntax
Wireshark Filter by IP	ip.addr == 10.10.50.1
Filter by Destination IP	ip.dest == 10.10.50.1
Filter by Source IP	ip.src == 10.10.50.1
Filter by IP range	ip.addr >= 10.10.50.1 and ip.addr <= 10.10.50.100
Filter by Multiple Ips	ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100
Filter out IP address	!(ip.addr == 10.10.50.1)
Filter subnet	ip.addr == 10.10.50.1/24
Filter by port	tcp.port == 25
Filter by destination port	tcp.dstport == 23
Filter by ip address and port	ip.addr == 10.10.50.1 and Tcp.port == 25

Wireshark 101

- Apply filters

Usage	Filter syntax
Filter by URL	http.host == “host name”
Filter by time stamp	frame.time >= “June 02, 2019 18:04:00”
Filter SYN flag	tcp.flags.syn == 1
	tcp.flags.syn == 1 and tcp.flags.ack == 0
Wireshark Beacon Filter	wlan.fc.type_subtype = 0x08
Wireshark broadcast filter	eth.dst == ff:ff:ff:ff:ff:ff
Wireshark multicast filter	(eth.dst[0] & 1)
Host name filter	ip.host = hostname
MAC address filter	eth.addr == 00:70:f4:23:18:c4
RST flag filter	tcp.flags.reset == 1

Wireshark 101

- Follow streams
  - Listen in to one particular conversation between two endpoints on the network
  - Right-click -> Follow -> Stream
- Use the statistics tab
  - Statistics -> Protocol Hierarchy; provides a good place to start looking for key streams

Listening to Streams

- Lots of low-point CTF problems simply require following the write conversation stream
  - Look for unencrypted connections
- The flag will be in the stream somewhere

Finding Exfiltrated Data

- If the goal of an attacker is to steal data from a network, then the attacker needs to exfiltrate data out to their command-and-control server somehow
  - Look for places where data leaves the network in big chunks
  - Usually involves a little bit of cryptography/steganography because attackers like to be sneaky
- See “Zaine’s Forensics” in TCTF
  - “whisper” is fairly straightforward

Files

- Lots of CTF problems deal with retrieving a file in the network traffic
- File -> Export Objects -> Usually HTTP
- Requires knowledge of file headers (aka magic bytes) to know what kind of file was transmitted
- See “Forensics” in TCTF
  - “USB” is a file challenge

Other Tools

- TCPdump - Command line interface packet capture analyzer
- Tshark - Wireshark CLI
- Zeek (Bro) - Open-source network security monitor tool with nice tutorial site at try.bro.org
  - Gives all of the network metadata
  - Will be the subject of later talks
- Splunk - Data enrichment center for your network logs

Challenges to Try

- NCL Qualifier - Terrible Little Security (TLS)
- Forensics - USB
- Zaine’s Forensics - Whisper

tctf.competitivecyber.club

Proud Sponsors

CACI

EVER VIGILANT

BATTELLE

It can be done™

CRYPSIS™