

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

No.	Time	Source	Destination	Protocol	Length	Info
210	25.292629	10.159.74.218	10.159.0.49	TCP	176	8009 → 58685 [PSH, ACK] Seq=551 Ack=661 Win=537 Len=11
211	25.292735	10.159.0.49	10.159.74.218	TCP	66	58685 → 8009 [ACK] Seq=661 Ack=661 Win=4092 Len=0 TSva
212	25.391970	10.159.0.49	129.174.253.66	DNS	74	Standard query 0x9071 A www.google.com
213	25.397397	129.174.253.66	10.159.0.49	DNS	338	Standard query response 0x9071 A www.google.com A 172.
214	25.399047	10.159.0.49	172.217.5.228	UDP	1392	49418 → 443 Len=1350

Authority RRS: 0
Additional RRs: 0

Queries

▼ www.google.com: type A, class IN

Name: www.google.com

[Name Length: 14]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Wireshark Packet Analysis

Raw
Bytes

0000	00 08 e3 ff fd e0 b8 f6 b1 1b b9 13 08 00 45 00E.
0010	00 3c 37 94 00 00 40 11 b9 5c 0a 9f 00 31 81 ae	<7...@. \...1..
0020	fd 42 dd 10 00 35 00 28 79 7e 90 71 01 00 00 01	.B...5.(y~.q....
0030	00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6cw ww.googl
0040	65 03 63 6f 6d 00 00 01 00 01	e.com... ..

Bytes in ASCII

Wireshark 101



- Apply filters (or just right-click)

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

Wireshark 101



- Apply filters

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

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™