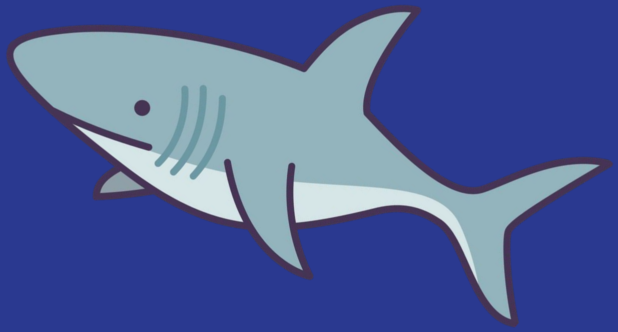
Wireshark Tool Talk

By Aya the Awesome



If you have wireshark installed, you can follow along :)

Let’s get something cleared up

- I first used wireshark 4 years ago
  - So you may think I’m a pro
  - You are so wrong
  - I’m more like a mediocre amatuer
- My goal is to get ***you*** to the point of mediocre amatuer in the span of 1 hour instead of 4 years

Contents

1. Network interfaces
2. Collecting packet data
3. Filtering packet data
4. Reading a packet
5. Solving a foreverCTF problem

Network Interfaces

What are You Sniffing?

- Common interfaces to connect to
    - Ethernet (may see as “eno1”)
    - Wifi (may see as “wlo1”)
    - Loopback
        - Localhost (so just what you’re sending yourself)
        - Great for debugging stuff you self-host
- Default is to only listen to traffic going to/from your device
    - Can also listen to all traffic on a local network
        - Requires promiscuous mode

A Note About What is OK

Basically: ask for permission, not forgiveness

✓

- Sniffing your own traffic
- Sniffing other people's traffic on a network where you have permission to do so

?

- Sniffing other people's traffic on a network where you never really asked but they might be cool with it…?
  - You should ask for permission

✗

- Sniffing other people's traffic on a network where you don't have permission
  - Seriously, what have I been saying about asking for permission

Collecting Data

- Start capture
  - Don’t have to press the first time
  - Wireshark starts collecting data as soon as you pick an interface
    - Need to have special privileges for wireshark to let you collect packet data
- Stop capture
  - Will have to save packet data before starting again or will lose it
- Restart capture
  - Again, have to save packet data or will lose it

Filtering Data

Common ways to filter data

- By IP address
  - ip.addr/ip.src/ip.dst == [ip address]
- By packet protocol
  - just use protocol name (ex: tcp, udp, tls)
- Specific keywords
  - [protocol name] contains [string/bytes searching for]
- By streams (specific “conversation”)
  - [protocol name].stream == [stream #]
  - Right click -> “Follow”
- **COLORS! :D**

Filtering Data, cont.

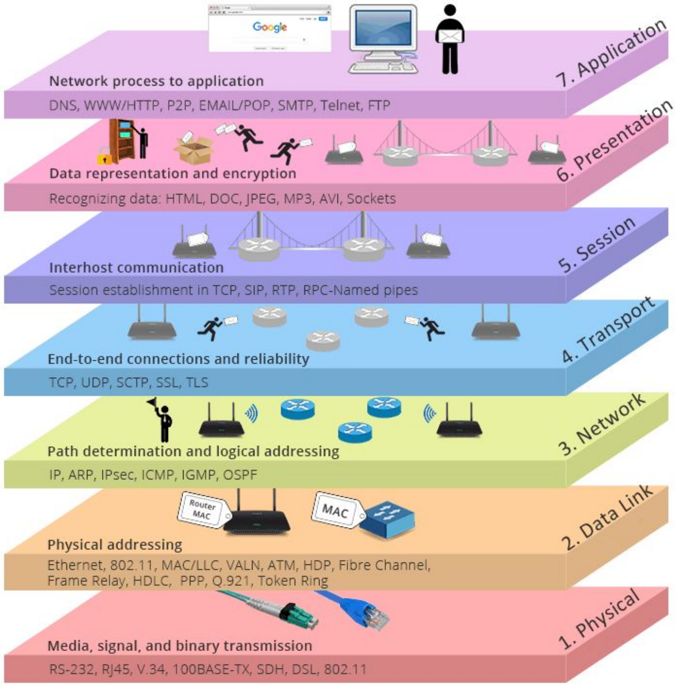
But how do you know?

- How do you remember/figure out what the filter commands are?
  - Strategy 1: read the docs
  - Strategy 2: just guess and hope wireshark autofill figures it out for you
    - My personal go-to strategy

Reading Packets

Ok, I got a specific packet…now what?

- Wireshark is good about breaking up packet into its “layers”
  - Drop downs
  - Highlighting
    - correlate description with raw data
- This is a ***very helpful tool, but not a replacement for actual knowledge of networking***



7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP

6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets

5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes

4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS

3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF

2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring

1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

foreverCTF Problem!

Go to “Wireshark” problem on forever.isss.io.

If you feel comfortable with that one, try “HTTP Object” next.