

Basic Wireshark Intro

Debug Project 1 by capturing and analyzing packets



Administrivia

- HW2 is released on Gradescope
 - Due on Monday April 26
- Project 1 due on Monday
 - Today: a short section followed by additional office hours

Wireshark

Download: <https://www.wireshark.org/download.html>

- Also available in most Linux package managers

User's Guide: https://www.wireshark.org/docs/wsug_html_chunked/

What is Wireshark

It's a tool that captures and analyzes packets sent over the network

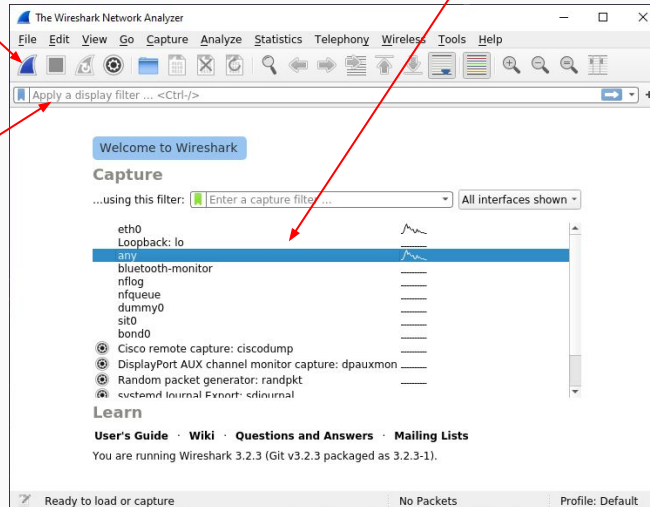
- Very commonly used in Network Forensics
- Captures all packets through a network interface (ethernet, WiFi)
 - Can capture packets on all network interfaces at the same time
- Analyzes packets and decodes raw data if the protocol is recognized
- Filters packets based on user's input

Wireshark Interface

Start Packet Capture

Interface Selection

Display filter for captured packets



Debugging P1 with Wireshark

Lots of packets are being sent while your computer is connected to a network.

- *Filtering packets to/from **attu's IP address***
 - How to find the IP address of attu?
 - Run `ifconfig` on attu (through SSH)
 - `nslookup attu2.cs.washington.edu` (from any computer)
 - `traceroute` will print out the IP address as well
 - `ip.addr == 128.208.1.138`
- *Filtering on the **port number***
 - `udp.port == 12235`
 - `tcp.port == portNumber`
- *Applying boolean logic to combine filters: `==`, `&&`, `||`, `!`*
 - `ip.addr == 128.208.1.138 && udp.port == 12235`
 - Will only show packets to/from attu2 on udp port 12235

Wireshark Captured Packets Interface

Captured packets

Hexadecimal data contained in the UDP packet

ASCII Decoding of data

Copy data value as hexadecimal string

The screenshot displays the Wireshark interface with a filter set to `ip.addr == 128.208.1.138 && udp.port == 12235`. The packet list shows two captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
776	8.752599900	172.22.203.88	128.208.1.138	UDP	68	58726
777	8.818393900	128.208.1.138	172.22.203.88	UDP	72	12235

The details pane for the selected packet (No. 776) shows the following structure:

- Frame 776: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 172.22.203.88, Dst: 128.208.1.138
- User Datagram Protocol, Src Port: 58726, Dst Port: 12235
- Data (24 bytes)

The data field is expanded to show hexadecimal and ASCII representations:

```
0000 00 04 00 01 00 06 00 15 5d 59 7c e1 ef ff 08 00 .....|Y|.....
0010 45 00 00 34 a9 al 80 00 40 11 97 4e ac 16 cb 58 E:4:3|@-N--X
0020 80 d0 01 8a e5 66 2f cb 00 20 f9 fa 00 00 0c .....f|.....
0030 00 00 00 00 00 01 03 cb 68 65 6c 6c 6f 20 77 6f .....hello wo
0040 72 6c 64 00 .....rld.
```

The packet bytes pane shows the hexadecimal string: `0000000c00000000000103cb68656c6f20776f726c6400`. A context menu is open over this pane, with the 'Copy' option selected. The 'Copy' submenu is also visible, showing options like 'Copy', 'Show Packet Bytes...', 'Export Packet Bytes...', 'Wiki Protocol Page', 'Filter Field Reference', 'Protocol Preferences', 'Decode As...', 'Go to Linked Packet', and 'Show Linked Packet in New Window'. The 'Copy' option is highlighted, and the 'Copy' submenu is open, showing options like 'All Visible Items', 'All Visible Selected Tree Items', 'Description', 'Field Name', 'Value', 'As Filter', 'Copy Bytes as Hex + ASCII Dump', '...as Hex Dump', '...as Printable Text', '...as a Hex Stream', '...as Raw Binary', and '...as Escaped String'.

