

CS 43: Computer Networks

Wireshark Introduction

Oct 9, 2020



Wireshark Start-up Screen (with X11)

The screenshot shows the Wireshark Network Analyzer interface. The title bar reads "The Wireshark Network Analyzer". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. Below the toolbar is a display filter input field with the text "Apply a display filter ... <Ctrl-/>".

The main area is titled "Welcome to Wireshark" and "Capture". It features a filter input field with the text "...using this filter: Enter a capture filter ..." and a dropdown menu set to "All interfaces shown". Below this is a list of interfaces and capture methods:

eth0	~
Loopback: lo	~
any	~
bluetooth-monitor	---
nflog	---
nfqueue	---
⊗ Cisco remote capture: ciscodump	---
⊗ DisplayPort AUX channel monitor capture: dpauxmon	---
⊗ Random packet generator: randpkt	---
⊗ systemd Journal Export: sdjournal	---
⊗ SSH remote capture: sshdump	---
⊗ UDP Listener remote capture: udpdump	---

A red arrow points to the "eth0" interface in the list. To the right of the arrow, the text "Choose eth0 to capture packets" is displayed.

At the bottom of the interface, there is a status bar with the text "Ready to load or capture", "No Packets", and "Profile: Default".

Wireshark Start-up Screen (local install)

Welcome to Wireshark

Capture

...using this filter: All interfaces shown

Wi-Fi: en0	
p2p0	---
awdl0	---
llw0	---
utun0	---
utun1	---
Loopback: lo0	
Thunderbolt Bridge: bridge0	---
Thunderbolt 1: en1	---
Thunderbolt 2: en2	---
Thunderbolt 3: en3	---
Thunderbolt 4: en4	---
gif0	---
stf0	---
ap1	---
<input checked="" type="radio"/> Cisco remote capture: ciscodump	---
<input checked="" type="radio"/> Random packet generator: randpkt	---
<input checked="" type="radio"/> SSH remote capture: sshdump	---
<input checked="" type="radio"/> UDP Listener remote capture: udpdump	---

Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.0.3 (v3.0.3-0-g6130b92b0ec6).

Ready to load or capture No Packets Profile: Default

Choose eth0 for
wired connections
or Wi-Fi en0 for
wireless
connections

Wireshark Step 2

(all steps here on shown for X11 but stay the same for local installs)

The screenshot shows the Wireshark interface with a live capture on the eth0 interface. The packet list pane displays a series of packets, including SSH and TCP traffic. A red arrow points to a specific packet in the list. The packet details pane shows the structure of the selected packet, including Ethernet II, ARP, and IP headers.

No.	Time	Source	Destination	Protocol	Length	Info
20744	9.780607031			SSH	22914	Server: Encrypted packet (len=22848)
20745	9.780627965			TCP	66	50159 → 22 [ACK] Seq=105553 Ack=93356325 Win=19233 Len=0 TSval=834077518 TSecr=2856176655
20746	9.780633220			TCP	66	50159 → 22 [ACK] Seq=105553 Ack=93359181 Win=19233 Len=0 TSval=834077519 TSecr=2856176655
20747	9.780641129			SSH	22914	Server: Encrypted packet (len=22848)
20748	9.780655536			TCP	66	50159 → 22 [ACK] Seq=105553 Ack=93370605 Win=19054 Len=0 TSval=834077519 TSecr=2856176655
20749	9.780665369			TCP	66	50159 → 22 [ACK] Seq=105553 Ack=93382029 Win=18876 Len=0 TSval=834077519 TSecr=2856176655
20750	9.780669598			TCP	66	50159 → 22 [ACK] Seq=105553 Ack=93386313 Win=18809 Len=0 TSval=834077519 TSecr=2856176655
20751	9.780674806			TCP	66	50159 → 22 [ACK] Seq=105553 Ack=93397737 Win=18630 Len=0 TSval=834077519 TSecr=2856176656
20752	9.780679757			TCP	66	50159 → 22 [ACK] Seq=105553 Ack=93409161 Win=18580 Len=0 TSval=834077519 TSecr=2856176656
20753	9.780683561			SSH	102	Client: Encrypted packet (len=36)
20754	9.780703681			TCP	66	50159 → 22 [ACK] Seq=105589 Ack=93412017 Win=19047 Len=0 TSval=834077519 TSecr=2856176656
20755	9.780710183			TCP	66	50159 → 22 [ACK] Seq=105589 Ack=93423441 Win=18869 Len=0 TSval=834077519 TSecr=2856176656
20756	9.780714481			TCP	66	50159 → 22 [ACK] Seq=105589 Ack=93424869 Win=18975 Len=0 TSval=834077519 TSecr=2856176656

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: HewlettP_4a:35:b2 (10:e7:c6:4a:35:b2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

You should see packets coming through across the network. (IP addresses blurred in image)

```
0000 ff ff ff ff ff 10 e7 c6 4a 35 b2 08 06 00 01 .....J5.....
0010 08 00 06 04 00 01 10 e7 c6 4a 35 b2 82 3a 44 8a .....J5...D...
0020 00 00 00 00 00 00 82 3a 44 3a 00 00 00 00 00 00 .....D:.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Wireshark Start-up Step 3

(2) Hit stop capture and continue without saving



(1) Type in dns to filter for dns traffic, and issue a dig query on the command line



No.	Time	Source	Destination	Protocol	Length	Info
42420	28.711995719	130.58.68.85	130.58.68.10	DNS	105	Standard query 0xaa68 A demo.cs.swarthmore.edu
42421	28.713289507	130.58.68.10	130.58.68.85	DNS	189	Standard query response 0xaa68 A demo.cs.swarthmore.edu

top third: list of traffic we have captured

Unsaved packets...

Do you want to save the captured packets before starting a new capture?
Your captured packets will be lost if you don't save them.

Save Continue without Saving Cancel

use bars to resize, sometimes the middle might not be visible without resizing



Wireshark Start-up Step 3

Hit stop capture
and don't save



Type in dns to filter for dns traffic, and issue a dig query on the command line



No.	Time	Source	Destination	Protocol	Length	Info
42420	28.711995719	130.58.68.85	130.58.68.10	DNS	105	Standard query 0xaa68 A demo.cs.swarthmore.edu
42421	28.713289507	130.58.68.10	130.58.68.85	DNS	189	Standard query response 0xaa68 A demo.cs.swarthmore.edu

```
squash[~]$ dig demo.cs.swarthmore.edu
```

top third: list of traffic we have captured

```
Frame 42420: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface eth0, id 0
Ethernet II, Src: HewlettP_64:55:a6 (84:a9:3e:64:55:a6), Dst: SuperMic_bb:67:f8 (00:25:90:bb:67:f8)
Internet Protocol Version 4, Src: 130.58.68.85, Dst: 130.58.68.10
User Datagram Protocol, Src Port: 38229, Dst Port: 53
Domain Name System (query)
```

middle: show all the encapsulated layers from ethernet -> application layer

use bars to resize, sometimes the middle might not be visible without resizing



```
0000  00 25 90 bb 67 f8 84 a9 3e 64 55 a6 08 00 45 00  %..g...>dU...E.
0010  00 5b 79 34 00 00 40 11 74 8a 82 3a 44 55 82 3a  [y4..@.t...DU..
0020  44 0a 95 55 00 35 00 47 8d 2c aa 68 01 20 00 01  D..U.5.G.,.h...
0030  00 00 00 00 00 01 04 64 65 6d 6f 02 63 73 0a 73  ....d emo.cs.s
0040  77 61 72 74 68 6d 6f 72 65 03 65 64 75 00 00 01  warthmor e.edu...
0050  00 01 00 00 29 10 00 00 00 00 00 00 0c 00 0a 00  ....).....
0060  08 d7 cb d6 d6 83 98 53 2d                      .....S-
```

bottom: shows you the entire packet in hex. representation.

Wireshark tries to also show you a text-based interpretation. But if the protocol is not text-based except where ASCII characters appear everything else will be gibberish.