CS 43: Computer Networks

Wireshark Introduction

Oct 9, 2020
Wireshark Start-up Screen (with X11)

Choose eth0 to capture packets
Wireshark Start-up Screen (local install)

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)

You should see packets coming through across the network.
(IP addresses blurred in image)
(1) Type in `dns` to filter for DNS traffic, and issue a `dig` query on the command line:
```
squash[~]$ dig demo.cs.swarthmore.edu
```

(2) Hit stop capture and continue without saving.

Top third: list of traffic we have captured.

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:
```
squash~$ dig demo.cs.swarthmore.edu
```

**Top third:** list of traffic we have captured

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

**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.