That’s not a packet tracer... This is a packet tracer! An introduction to Wireshark

by

Maurice Cronin

Background

- Left CIT with a BSc in Analytical Chemistry
- Worked in various labs
- Building work
- Tool hire
- Coring and chasing
- Small engine repair
- Back to CIT for the first year of the H. Dip in Cloud Computing
- Software QE at EMC

What we’ll cover tonight

- What/What/Why/Where
- Capturing traffic
- Promiscuous Mode
- Examining a packet
- Filters - Capture & Display
- Following a stream
- Re-creating a file from a stream

What is Wireshark?

- Wireshark a type of tool called a network protocol analyzer or packet analyzer.
    - Also refered to as a packet sniffer or tracer
- Log and browse network traffic.
- A network protocol defines rules and conventions for communication between network devices.

What would you use Wireshark for?

- Examine the traffic on your network
- Great way to learn more about networking as it provides a method to watch network operations in progress.
- Can be used to detect malicious/unwanted traffic

Why use Wireshark?

- Very powerful tool
- Cross platform – Linux, Windows, MacOS, FreeBSD and more
- Open source
- Free
- Easy to use
- Supports a huge range of protocols
- Captures from multiple types of network interface

Where do I get Wireshark?

- https://www.wireshark.org/download.html
- Found in many Linux repositories
- Installation varies by platform, so not covering that tonight.
- Wirehshark home page also has lots of detail on various filters, captures of various traffic types and lots more.

Setup

- 4 VMs for tonight’s demonstration
- Kali VM (192.168.1.202)
- Mint 18.3 Jack (192.168.1.120) – Webserver
- Mint 18.3 Bob (192.168.1.102) - Client
- Router running OpenWRT