Sam Hobbs

UoG Applicant Day

A guide to Wireshark

16/03/2024-23/03/2024

Contents

[What is Wireshark? 2](#_Toc191473118)

[Features 2](#_Toc191473119)

[The Wireshark GUI 2](#_Toc191473120)

[Packet Colours 3](#_Toc191473121)

[Common Packet Filtering Commands 3](#_Toc191473122)

[Following ‘streams’ 4](#_Toc191473123)

[Packet Reassembly (for Bonus Challenge) 6](#_Toc191473124)

[CHALLENGES 6](#_Toc191473125)

[BONUS CHALLENGE 7](#_Toc191473126)

# What is Wireshark?

Wireshark is a popular tool used in the world of Ethical Hacking and cyber security, and it is used to analyse any traffic over a network. It provides lots of information about network traffic, such as source/destination IP addresses, devices, protocols and many more. It has become the industry standard tool for network traffic analysis.

# Features

* Ability to capture network traffic in real-time over any network.
* Allows for offline analysis as well (previously captured packets).
* Cross-platform, can run on Windows, macOS and Linux.
* Features many powerful display filters to analyse packets more closely.
* GUI-based, but data can also be viewed in a command line interface too.
* Support for hundreds of different networking protocols.

# A screenshot of a computer Description automatically generatedThe Wireshark GUI

Packet Info

Packet Viewer

HEX data

Each section of the Wireshark UI has a very specific, and useful, purpose. The packet viewer is the main section of the UI, and is where you can see all of the traffic on the network, and information like protocols and addresses. The packet info section contains some additional information about different packet. The HEX data section provides an overview of a particular packet’s data in a readable format (on the right), along with the hexadecimal format on the left.

# Packet Colours

Wireshark uses different colours to represent different packet types. Below is a table you can use as a reference point:

|  |  |
| --- | --- |
| **Colour** | **Meaning/Type** |
| **Light Purple** | TCP (Transmission Control Protocol) |
| **Light Blue** | UDP (User Datagram Protocol) or DNS |
| **Black** | Packets that contain errors. |
| **Light Green** | HTTP (Hypertext Transfer Protocol) |
| **Yellow** | Packet Routing |
| **Dark Gray** | SYN/FIN/ACK traffic. |
| **Purple** | RPC call. |
| **Red** | Potentially dangerous packets. |
| **White** | Ethernet packets. |

The packet colours you see in a file will depend on the type of traffic being sent over the network at the time of the capture taking place.

# Common Packet Filtering Commands

Ip.addr == (ip) – Filter by IP address  
ip.dest == (ip) - Filter by destination IP  
ip.src == (ip) – Filter by source IP  
ip.addr >= (ip) and ip.addr <= (ip) – Filter by range  
ip.addr == (ip) and ip.addr == (ip) – Filter by multiple IPs.  
tcp.port == (port) - Filter by port  
http.host == “host name” – Filter by URL  
frame.time >= “date/time” – Filter by time stamp  
eth.addr == (MAC) – MAC address filter  
ip.host = hostname – Host name filter  
tcp.flags.reset == 1 – RST flag filter

These commands are entered into the ‘Apply a display filter’ section at the top of the UI.

# Following ‘streams’

A screenshot of a computer

Description automatically generatedFollowing a stream of data from packet is a useful method of gathering information from packets, such as URLs, system information and other data. Here is a simple guide on how to do this from the UI:  
  
1 – Find any packet from the capture file (highlighted in blue in the below picture)

A screenshot of a computer program

Description automatically generated  
2 - Right-click the packet.

3 – On the menu that pops up, hover over the ‘Follow’ section.

A screenshot of a computer

Description automatically generated

4 – When a sub-menu appears, click on whatever option appears (TCP Stream, UDP Stream etc).

A screenshot of a computer

Description automatically generated

5 – A new window should appear, with data being displayed in either red or blue. Red data is client data, and blue is server data.

# A screenshot of a computer Description automatically generatedCHALLENGES

* In the packet named ‘msnms.pcap’, try and find the unencrypted conversation. (We will do this one together).
* Look for the small conversation in ‘nb6-https.pcap’, along with the hashed data.