Wireshark Packet Analysis - Project Brief

What is Wireshark?

Wireshark is the most commonly used and world's foremost network protocol analyzer. It enables one to observe the network on a microscopic level and let's one analyze what is happening on the network. It is a standard tool used by many non-profit, educational and commercial organizations alike. The project was started by Gerald Combs in 1998 and is regularly contributed to by the volunteers and networking experts.

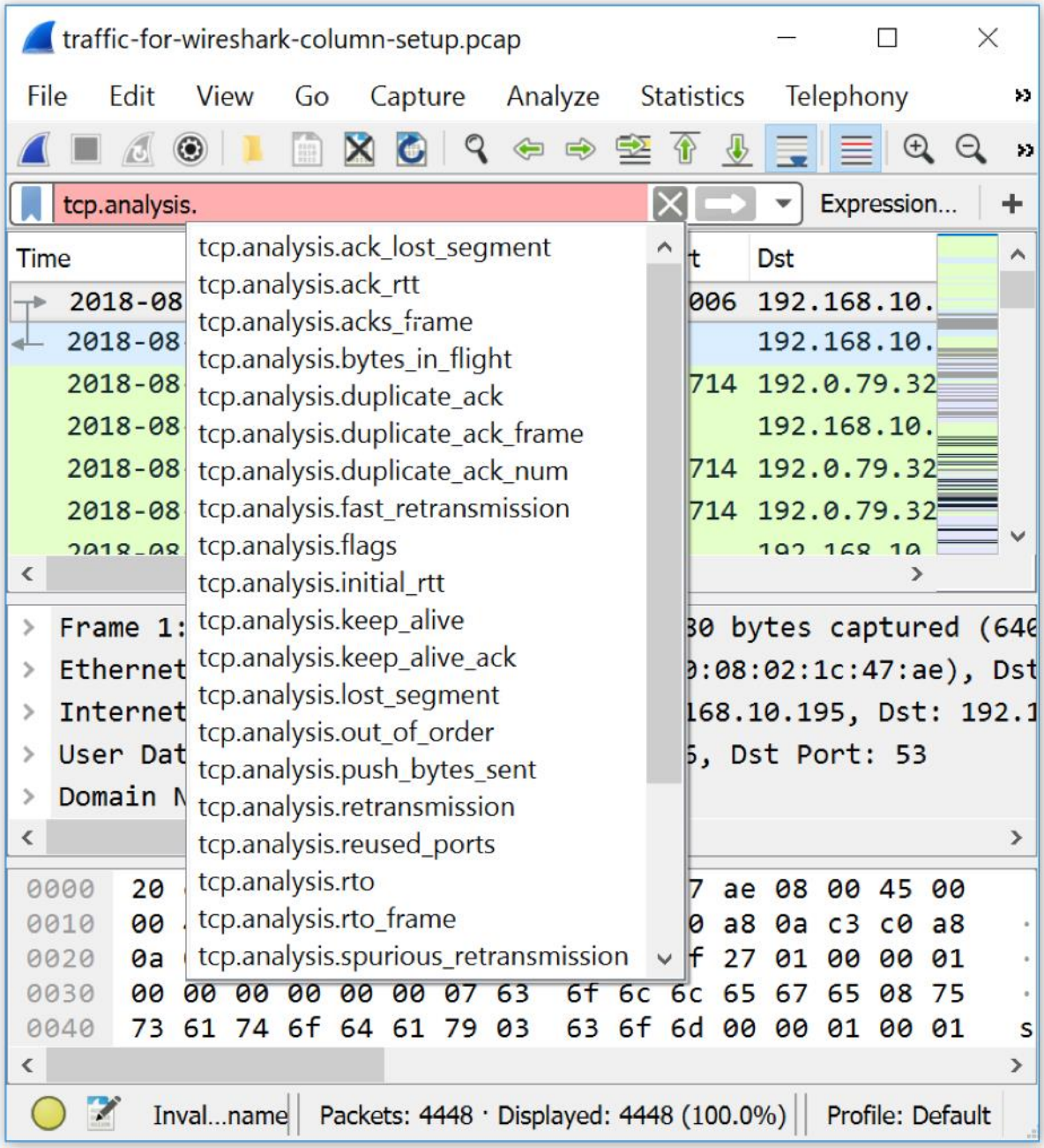
Features of Wireshark includes the following:

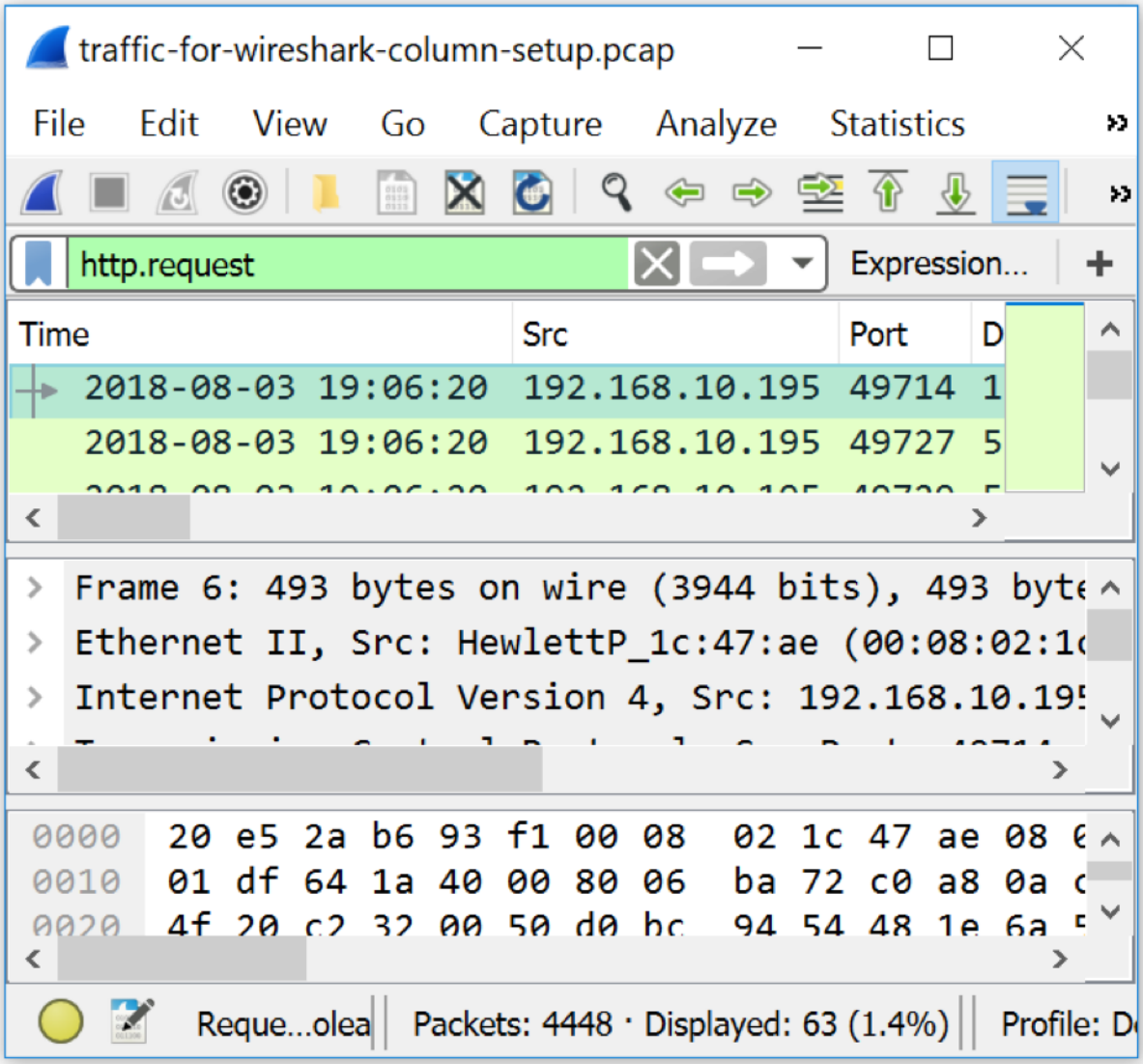
- Deep inspection of multiple protocols
- Live capture of network packets
- Offline analysis of the packets

What are display filters?

Filters are used to view packets that meet a specific criterion. During analysis, filters help to isolate a specific conversation. In the terminology used by Wireshark a conversation is the collection of packets exchanged between two computers.

Wireshark will provide a list of suggestions, once you start typing in the display filter, on the basis of the typed text. The entered expression has not been accepted if the display filter is heighted with a red color. The entered expression has been accepted and will work appropriately, if the color turns green. However, if the color turns yellow, it means that the expression is accepted but might not work as expected.





Boolean expressions are utilized in the display filter of Wireshark. This can help in specifying values and combining them. Most commonly used expressions are:

- **And:** && or and
- **Equals:** == or eq
- **Or:** || (double pipe) or or
-

Examples of these filter expressions follow:

```
➢ http.request || http.response
➢ ip.addr eq 10.0.2.1 and ip.addr == 10.0.2.2
➢ dns.qry.name contains example1 or dns.qry.name contains example2
➢ http.request && ip.addr == 10.0.2.2
```

Do not use the expression "!=" to exclude a value. For instance, if you want to indicate- all traffic that does not include IP address 10.0.2.1, use "!(ip.addr eq 10.0.2.1)" instead of "ip.addr != 10.0.2.1".

Reference: Complete list of display filters can be found here: https://www.wireshark.org/docs/dfref/

Project Overview

The project will help you to familiarize with the Wireshark tool. In this project, you would learn to analyze the HTTP traffic, identify a 3-way TCP handshake from packet captures and analyze DNS traffic. In this project you will perform hands-on tasks on Wireshark with capture filters, display filters and DNS filters.

Installing Wireshark on Windows:

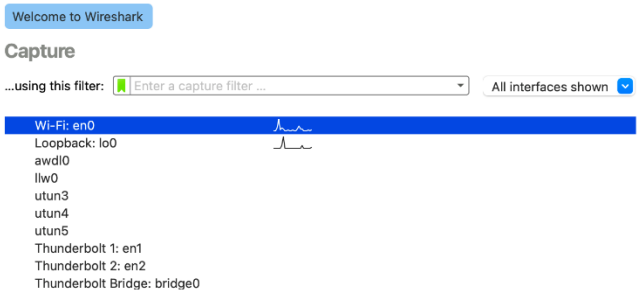
1. Go to the website- https://www.wireshark.org/download.html
2. Download the installer as per your systems configuration. (Windows/macOS and 32 bit/64 bit)
3. Locate the installer file of Wireshark you downloaded. Double-click on the file to open it.
4. On the User Account Control dialog box, select **Yes.** This will allow the program to make changes to your computer.
5. Select **Next >** to start the Setup Wizard.
6. If you agree with the licence agreement, select **Noted** to continue.
7. Select **Next >** to skip the Donate today Window
8. Select **Next>.** Leave the file components selected as it is.
9. Select the shortcuts that you want to create. Leave the file extensions selected. Select **Next >** to continue.
10. Select **Next >** to accept the default install location.
11. Click Install Npcap 1.71 and Select **Next >** to install NPcap.
12. Click Install USBPcap 1.5.4.0 and Select **Next >** to install USBPcap
13. Select **I agree** to begin installation
14. Select **Install** to initiate the installation process.
15. Click **I accept the terms of the Licence Agreement** to continue installation
16. Select **Next >** to select the location.
17. Select **Install >** to accept the default install location.

Installing Wireshark on MacOS:

1. Go to the **Official Wireshark** Website on a web browser.
2. Download the "**macOS intel 64-bit.dmg**" file.
3. Once the download is complete, go to the **Downloads** folder and Open "**Wireshark 4.0.2 Intel 64.dmg**". [Note that the downloaded version might be different]
4. Install **ChmodBPF.pkg**. Perform the installation by selecting the default options [You can choose to change the default locations] and clicking on "Continue". [Note that you would require Administrator privileges to perform the installation].

5. Install "**Add Wireshark to the system Path**" by following the instructions as prompted on the installation dialogue box.
6. To install Wireshark, drag the *Wireshark* application bundle to the *Applications* folder.

7. Go to the **Applications folder** and double click on the **Wireshark Icon** to launch it.
8. On the home page of the application, **double click on the network** you want to capture the packets for.



Note: Please ensure you watch the Demo on Wireshark before attempting the project tasks.

Questions:

Task 1 (10 points)

Your task is to analyze the packet capture from "capture_01.pcapng" file.

Instructions:

1. Download the capture_01.pcapng file from Olympus.
2. Open Wireshark as Admin.
3. Open the capture_01.pcapng file with Wireshark.
4. Identify the HTTP traffic in this capture file to spot the login attempt

Submission Details:
Once you find the packet that contains the username and password details, take a screenshot and submit the same. [Please make sure that the Frame No., Username and Password are clearly visible on the screenshot]

[Tip: Display filters will be your best friends.]

Task 2 (15 points)

During a network monitoring session, Ananth found a conversation between 172.25.10.13 & 52.111.240.3. This connection led to a data breach. As an investigator, your task is to spot the three-way TCP handshake and perform forensic investigations.

Instructions:

1. Download the capture_02.pcapng file from Olympus.
2. Open Wireshark as Admin.
3. Open the capture_02.pcapng file with Wireshark.
4. Determine the display filter that helps in isolating the traffic between the two IP address (mentioned above).
5. Spot the 3-way TCP handshake.

Submission Details:

1. Once you have spotted the conversation, take a screenshot of the 3-way TCP handshake. [Please ensure that the Frame No., Time, Source, Destination, Protocol, Length and Info details are visible in the screenshot].
2. Complete the following table:

	Frame No.	Source IP address	Source port number	Destination IP address	Destination port
SYN Packet					
SYN-ACK Packet					
ACK-Packet					

[Tip: Use the Info column in the packet list pane to spot the 3-way TCP handshake. Use the Packet details pane to complete the table]

Task 3 (15 points)

In this task, you will practice capture filters and then use display filters as well.

Instructions:

1. Start Wireshark as an admin.
2. Identify what capture filter is used for capturing only DNS traffic.
3. Use the capture filter for DNS and start capturing packets.
4. Open the command prompt.
5. Use the command- **ping shodan.io**.
6. Do you see DNS capture packets in your live capture?
7. Stop the Capture. Save the capture file on your computer. (*Save the file as "yourfirstname.pcap")*
8. Analyze the DNS traffic that you just captured. Identify the queries and the responses.
9. You would see your computer sending IPv4 (A record) and IPv6 (AAAA record) requests.
10. For this assignment, spot the IPv4 address that you received as the reply.

Submission details:

1. Screenshot of the DNS response containing the IPv4 address.
2. SHA-1 hash of the .pcap file that you saved. (Use the tool - https://emn178.github.io/online-tools/sha1_checksum.html to get the SHA-1 hash)
3. Upload the .pcap file on Olympus.

Note: Please use the Sample Report Format docx file (on Olympus) to submit the project report.

Project Support:

Q&A forum for offline support: Discussion board.

You can also post your queries on the discussion forums available on Olympus.