**EXPERIMENT NUMBER 7**

| Name of Student: Sangeet Agrawal | PRN: 21070122140 | Section: CS-B3 |
| --- | --- | --- |

**Title:** Understand Network monitoring tool

**Aim:** Study and demonstrate Wireshark for packet capturing and monitoring

**Objective:** To make students learn and demonstrate Wireshark as network monitoring tool

**Theory: [Source -** <https://www.wireshark.org/docs/wsug_html_chunked/index.html>**]**

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

**Here are some reasons to use Wireshark:**

* Network administrators use it to troubleshoot network problems
* Network security engineers use it to examine security problems
* QA engineers use it to verify network applications
* Developers use it to debug protocol implementations
* People use it to learn network protocol internals

**The following are some of the many features Wireshark provides:**

* Available for UNIX and Windows.
* Capture live packet data from a network interface.
* Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
* Import packets from text files containing hex dumps of packet data.
* Display packets with very detailed protocol information.
* Save packet data captured.
* Export some or all packets in a number of capture file formats.
* Filter packets on many criteria.
* Search for packets on many criteria.
* Colorize packet display based on filters.
* Create various statistics.

**Here are some things Wireshark does not provide:**

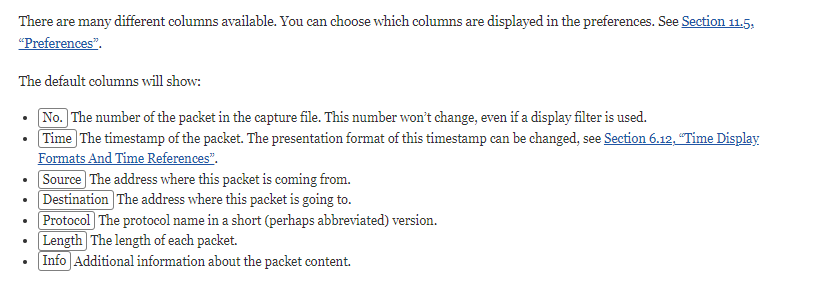
* Wireshark isn’t an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
* Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn’t send packets on the network or do other active things (except domain name resolution, but that can be disabled).

## A Brief History Of Wireshark

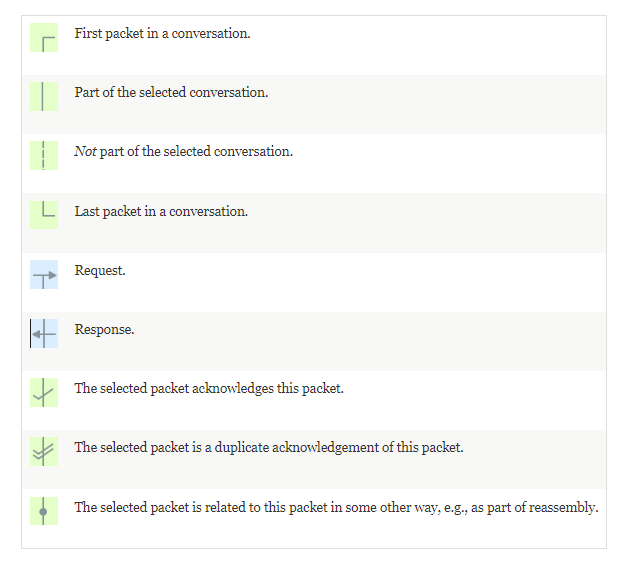
In late 1997 Gerald Combs needed a tool for tracking down network problems and wanted to learn more about networking so he started writing Ethereal (the original name of the Wireshark project) as a way to solve both problems. Ethereal was initially released after several pauses in development in July 1998 as version 0.2.0. Within days patches, bug reports, and words of encouragement started arriving and Ethereal was on its way to success.

In October, 1998 Guy Harris was looking for something better than tcpview so he started applying patches and contributing dissectors to Ethereal. In late 1998 Richard Sharpe, who was giving TCP/IP courses, saw its potential on such courses and started looking at it to see if it supported the protocols he needed. While it didn’t at that point new protocols could be easily added. So he started contributing dissectors and contributing patches. In 2006 the project moved house and re-emerged under a new name: Wireshark.

In 2008, after ten years of development, Wireshark finally arrived at version 1.0. This release was the first deemed complete, with the minimum features implemented. Its release coincided with the first Wireshark Developer and User Conference, called Sharkfest. In 2015 Wireshark 2.0 was released, which featured a new user interface. In 2023 Wireshark moved to the [Wireshark Foundation](https://wiresharkfoundation.org/), a nonprofit corporation that operates under section 501(c)(3) of the U.S. tax code. The foundation provides the project’s infrastructure, hosts [SharkFest](https://sharkfest.wireshark.org/), our developer and user conference, and promotes low-level network education.



**Related packet symbols**



**Tools for Study:**

1. WinPcap
2. Wireshark

**Reference web links:**

1. <https://www.winpcap.org/>
2. <https://www.wireshark.org/>
3. <https://www.imperva.com/learn/ddos/high-orbit-ion-cannon/>
4. <https://www.kali.org/tools/hping3/>
5. <https://www.wireshark.org/docs/wsug_html_chunked/index.html>

**Theory question:**

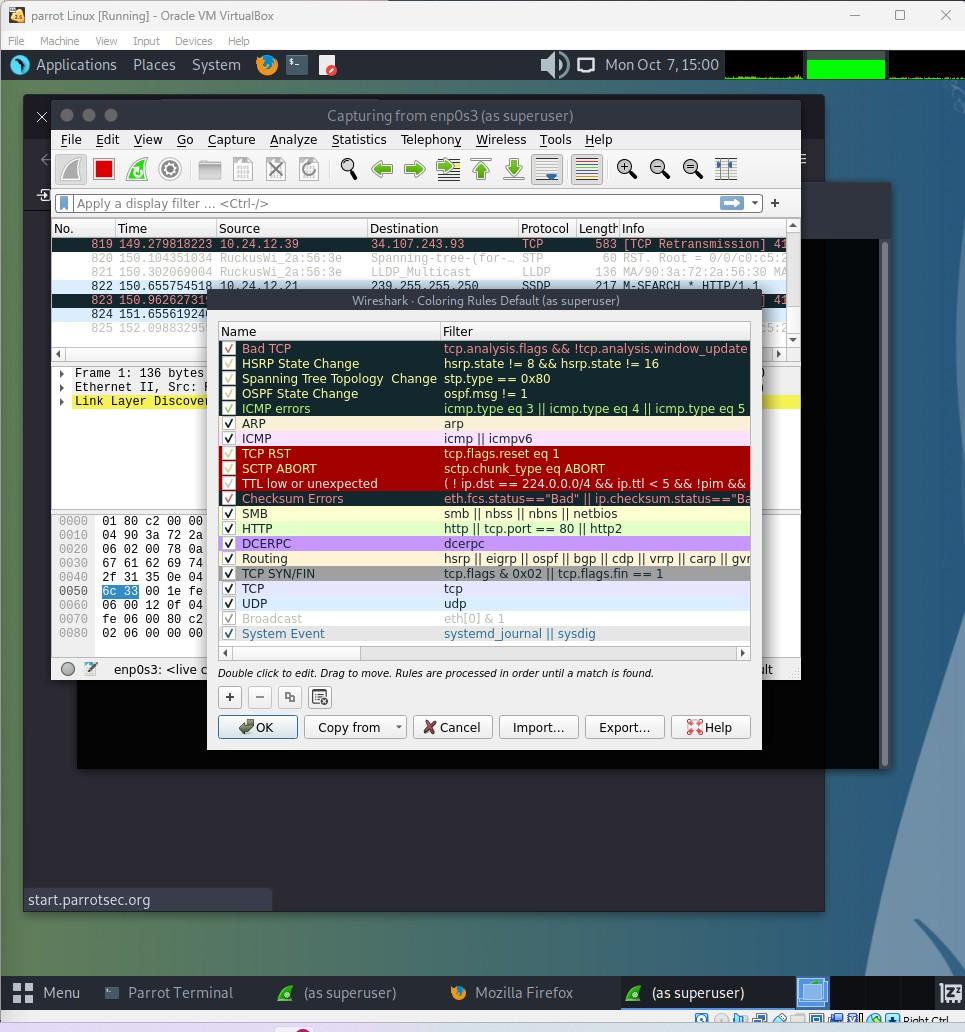
1. Differentiate between HOIC and LOIC

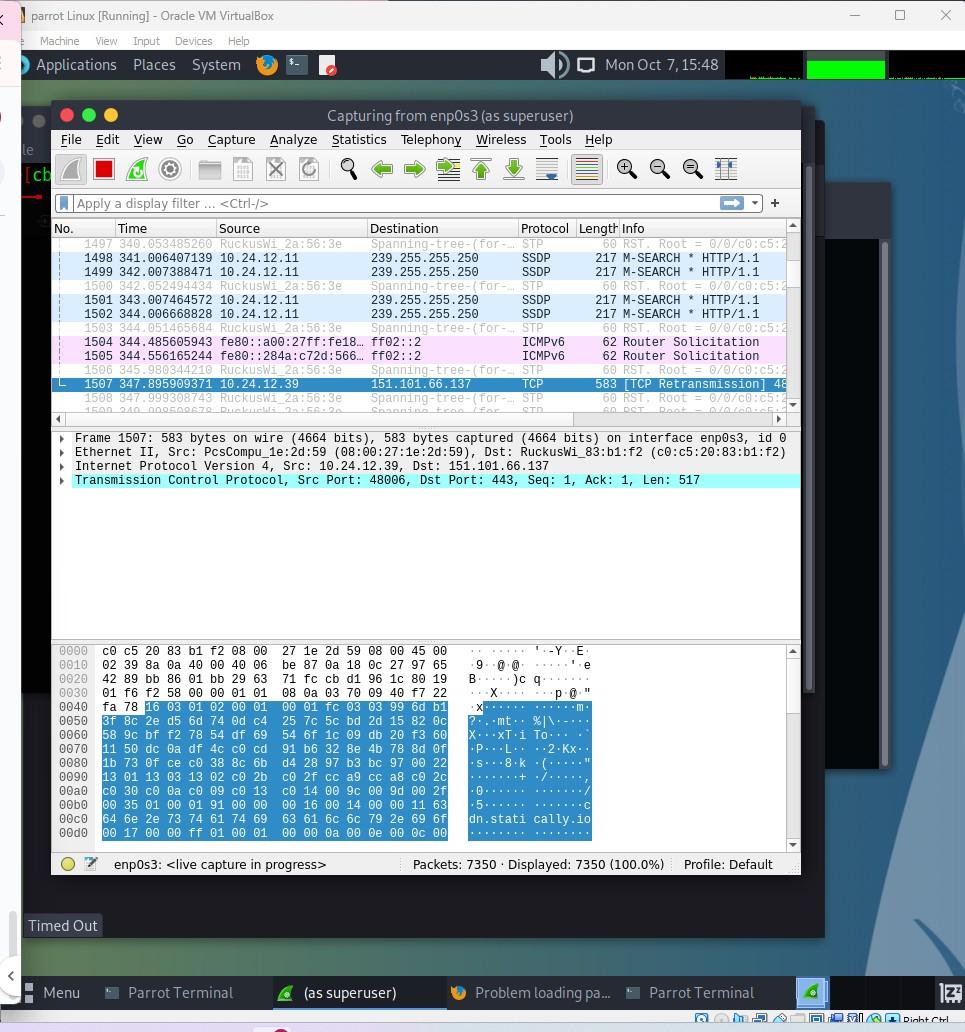
| **Aspect** | **HOIC (High Orbit Ion Cannon)** | **LOIC (Low Orbit Ion Cannon)** |
| --- | --- | --- |
| **Attack Type** | HTTP-based DoS/DDoS | TCP/UDP/ICMP DoS/DDoS |
| **Targeting** | Multi-threaded, can target multiple URLs | Single-target at a time |
| **Usability** | More advanced, requires configuration | Simple and user-friendly |
| **Power** | More powerful, harder to mitigate | Less powerful but still dangerous |
| **Usage** | Used in larger-scale DDoS attacks | Commonly used in basic DDoS attacks |
| **Anonymity** | Requires proxy for anonymity | No built-in anonymity features |

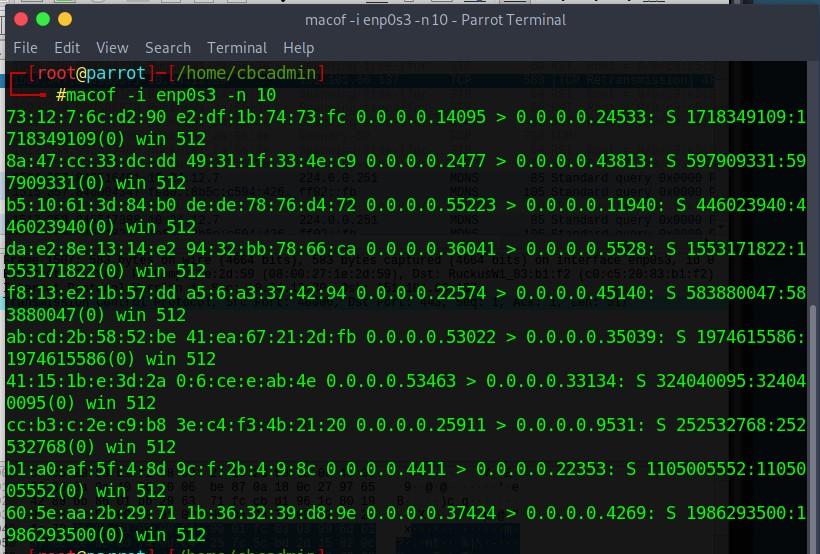
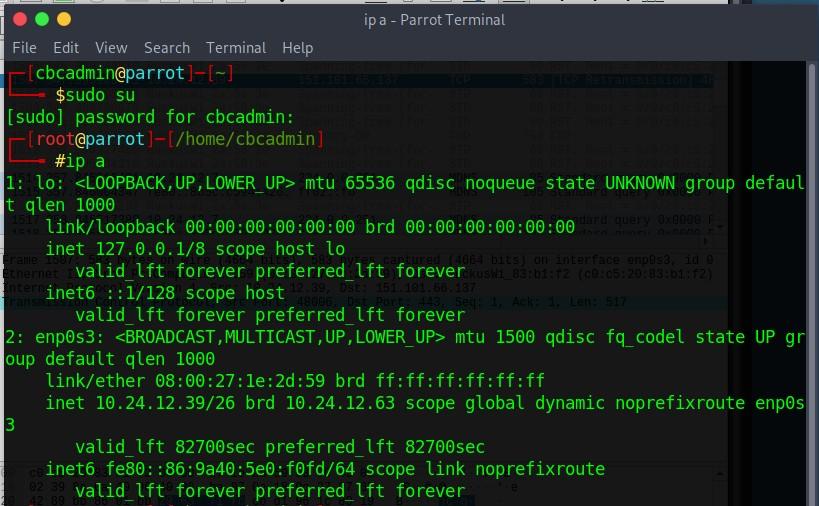
1. Differentiate between Winpcap and Wireshark

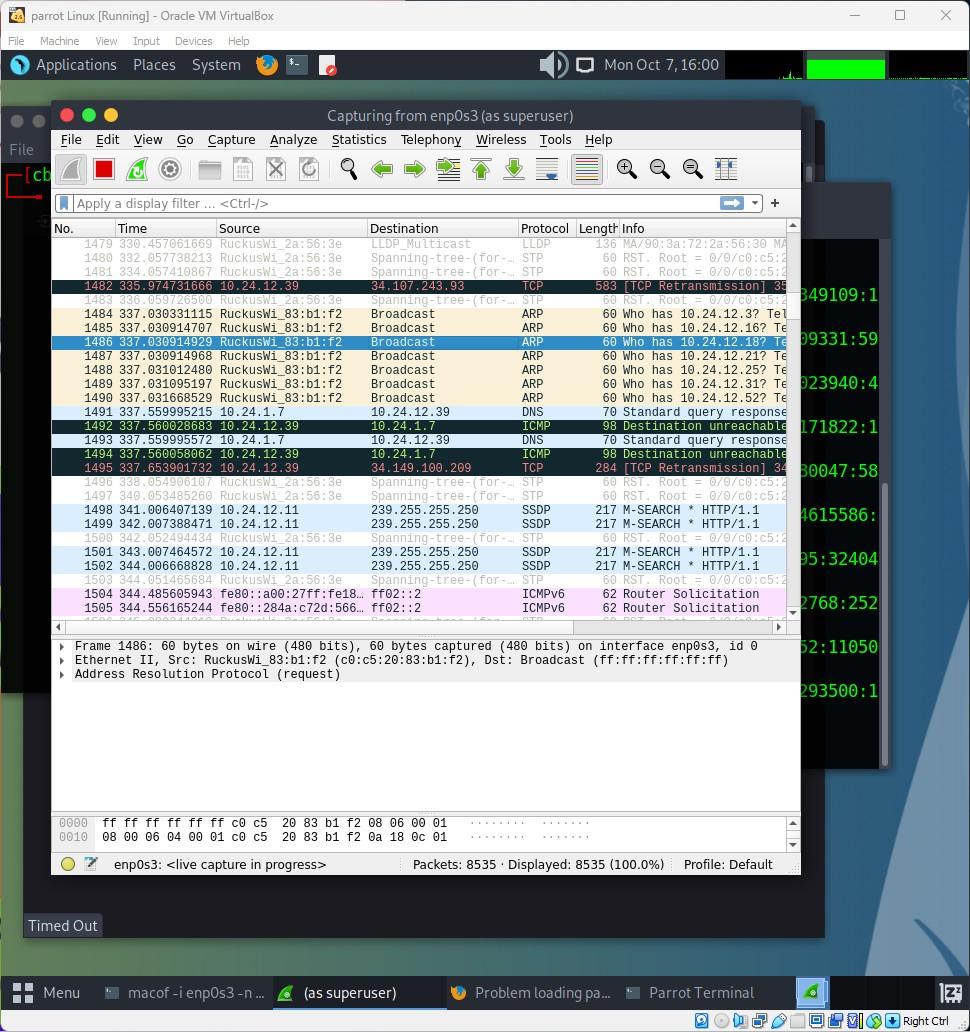
| **Aspect** | **WinPcap** | **Wireshark** |
| --- | --- | --- |
| **Functionality** | Packet capture library (API) | Full packet capture and analysis tool |
| **Role** | Backend for packet capturing | Frontend for packet analysis |
| **Operating Environment** | CLI/Programmatic use | GUI-based interface |
| **Platform Dependency** | Windows-only | Cross-platform (Windows, macOS, Linux) |
| **Usage** | Used by apps like Wireshark for capturing | Complete tool for capturing and analyzing packets |
| **Replacement** | Deprecated (replaced by Npcap) | Actively maintained and updated |

1. Perform DoS/DDoS attack using any open source tool of Kali OS or Windows OS and capture the packets during attack using wireshark.









1. Explain important details about the packets captured in the previous question.
2. Source and Destination IPs:
   * The source IP represents the machine from which the attack originated or appeared to originate. In a DoS attack, this is typically the IP address of the targeted system.
   * The destination IP refers to the IP address of the machine being targeted by the attack.
3. Types of Packets:
   * Depending on the nature of the attack, packets may include ICMP (used in ping floods), TCP SYN (used in SYN floods), or UDP packets.
   * For HTTP floods, a large number of HTTP GET or POST requests are typically observed.
4. Packet Volume and Frequency:
   * A DoS attack is characterized by a high frequency of identical or nearly identical packets, usually transmitted in rapid succession, as seen in attacks like ICMP or SYN floods.
5. Flags (in TCP packets):
   * In TCP-based attacks, such as SYN floods, multiple TCP packets with the SYN flag are transmitted, indicating repeated attempts to establish connections without completing them.
   * The targeted server may respond with SYN-ACK packets, but the attacker fails to complete the handshake.
6. Packet Size:
   * Packet sizes may vary depending on the tools used. For instance, UDP floods may include large packets to maximize bandwidth consumption, while ICMP floods typically involve uniform packet size.

**Note:** Students are suggested to use Linux OS-based tools or free Windows OS-based tools.

**Conclusion:** We have successfully implemented Wireshark for packet capturing and network monitoring. This study provided students with hands-on experience in analyzing network traffic, enhancing their skills in detecting patterns and identifying potential threats effectively.