# Wireshark Packet Capture and Analysis

**Lab 1**

**Telecommunication Software**

**Submitted by**
ABDUL HAYEE
[241AME011]

**Submitted to:**
TIANHUA CHEN

**FACULTY OF COMPUTER SCIENCE, INFORMATION TECHNOLOGY AND ENERGY**
INSTITUTE OF PHOTONICS, ELCTRONICS AND ELECTRONIC COMMUNICATIONS
RIGA TECHNICAL UNIVERSITY

[8th December ,2024]

**SUPERVISOR SIGNATURE: ____________________**

**CANDIDATE SIGNATURE: ____________________**

# LAB WORK REPORT

## Lab Work 06 Report:
## Wireshark. Network Traffic Capture and Analyze.

| Student Name Surname: | Student ID: | Date: |
|---|---|---|
| Abdul Hayee | 241AME011 | 8th December, 2024 |

### 3.1. Capture File Properties

Fill in the table. For initial data use the **Statistics/Capture File Properties**.

| Nr | Parametr | Value |
|---|---|---|
| 1 | Time of capture, min | 14.761 seconds |
| 2 | Packets | 7417 |
| 3 | Bytes, MiB | 7459324 bytes |
| 4 | Average packet size, B | 1006 |
| 5 | Average packets per seconds, pps | 505 k |
| 6 | Average bytes per seconds, B/s | 4042 k |

7. Total Traffic = 7,459,324 bytes
Time of capture (T) = 14.761 seconds
Bandwidth = 100 Mbits/sec

Conversion steps:

Convert bytes to Mbits:
7,459,324 bytes ÷ (8 * 1,000,000) = 0.0597 Mbits
Calculate network load:
L = (0.0597 Mbits / 14.761 sec) / (100 Mbits/sec)
L = 0.00405 / 100
L = 0.00405%

### 3.2. Ethernet Traffic Distribution by Protocols

Fill in the table. For initial data use the **Statistics/Protocol Hierarchy**.

| Nr | Protocol | Traffic, MiB | Traffic, % |
|---|---|---|---|
| 1 | IPv6 | 240 bytes, 130 bits/sec | 0.1% |
| 2 | IPv4 | 144400 bytes, 78k/sec | 97.3% |
| 3 | --UDP | 54920 bytes, 29k bits/sec | 92.6% |
| 4 | --TCP | 7212 bytes, 3908 bits/sec | 4.8% |
| 5 | --ICMP | 140 bytes, 75 bits/sec | 0.1% |
| 6 | ARP | 4959 bytes, 2685 bits/sec | 2.4% |
| 7 | 802.1X | 75 bytes, 40 bits/sec | 0.2% |
| | **SUMM** | | **100** |

8. In this network capture, the absence of service protocol packets creates a mathematical anomaly. The ratio of application to service protocols becomes undefined because division by zero is mathematically impossible. Technically, this means the ratio would approach infinity, indicating an extremely one-sided network communication dominated by application-layer traffic with no observable service protocol interactions.
This suggests an unusual network scenario where only application-level communications were captured, without any of the typical background network management and service protocols typically seen in normal network traffic.

## 3.3. Ethernet Traffic Distribution by Nodes

Fill in the table (for the 5 most active network nodes by Bytes). For initial data use the **Statistics/Endpoints/Ethernet**.

| Nr | MAC-address | IP- address | Traffic | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Rx input | | Tx output | | Overall | |
| | | | MiB | % | MiB | % | MiB | % |
| 1. | 54:ab:3a:04:85:88 | | 7MB | | 200kb | | 7MB | |
| 2. | bc:ea:fa:13:20:8d | | 198kb | | 7MB | | 7MB | |
| 3. | ff:ff:ff:ff:ff:ff | | 13kb | | 0 bytes | | 13kb | |
| 4. | 09:00:09:09:13:a6 | | 900 bytes | | 0 bytes | | 900 bytes | |
| 5. | 33:33:00:00:00:16 | | 450 bytes | | 0 bytes | | 450 bytes | |
| | | **SUM** | | **100** | | **100** | | **100** |

6. Which IP nodes are the most loaded, given the direction of traffic?
Incoming – Address: 78.154.135.49 Packets load: 6053 Total size 7MB
Outgoing Address: 31:13:72:52 Packet load: 5742 Packet size 6MB

Overall: 7MB

## 3.5. Network Problem Analyze

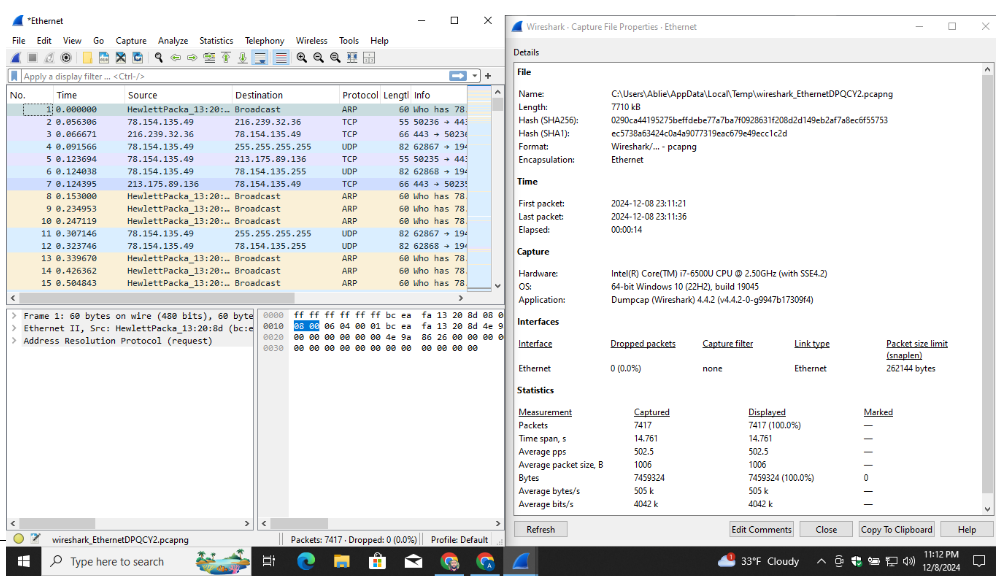
Analyze the 5 note/warning/error problems existing on the network. Find and read information about network problems on the Internet.
For initial data use the **Analyze/Expert Information**.

| Nr | Expert Information | Severity | Your Short Description (Problem Analyse) |
|---|---|---|---|
| 1 | Connection reset (RST) | Warning | Protocol TCP, Sequence group, Number of Count 1 |
| 2 | Failed to decrypt handshake | Warning | Protocol QUIC, Decryption group, Number of Count 90 |
| 3 | Inaccurate Padding Identification | Note | Protocol Ethertype, Group Protocol, Number of Count 13. |
| 4 | The legacy version field must be ignored. | Chat | Protocol TLS, Group Deprecated, Number of count 34. |
| 5 | NIL | Error | No error found in the connection. |
| | | | |

## 3.4. Display Filters

5 simple search filters (Display Filters) using AND, OR, NO to display packets from (to) a specific node generated by ICMP, DNS, ARP requests (responses) when accessing any server of your choice.

| Nr | Display Filter | Description |
|---|---|---|
| 1 | dns | Displays all DNS packets, including requests and responses |
| 2 | icmp \|\| dns | Displays packets that are either ICMP or DNS |
| 3 | icmp && !(arp) | Displays ICMP packets but excludes ARP packets. |
| 4 | arp.opcode == 1 | isplays all ARP requests. ARP requests have an opcode value of 1. |
| 5 | tcp | Displays all TCP used protocol. |



Output:

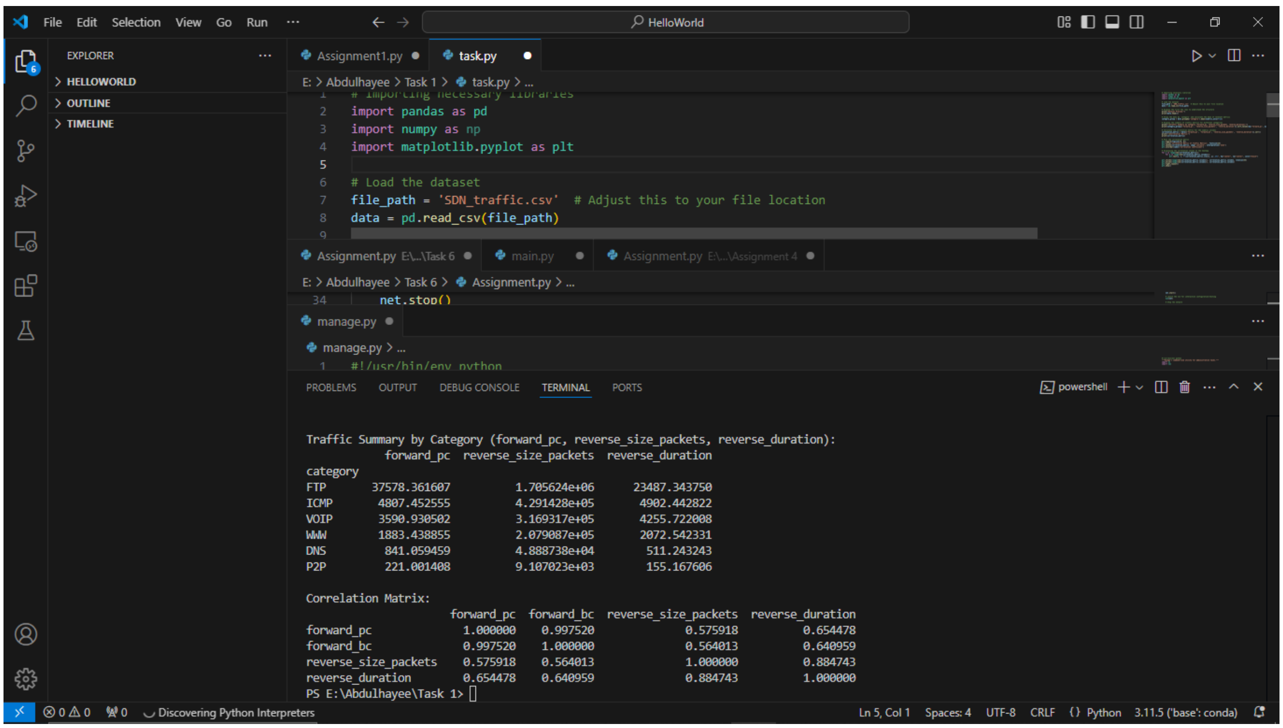
PS E:\Abdulhayee\Task 1> ls
    Directory: E:\Abdulhayee\Task 1

| Mode | LastWriteTime | Length | Name |
|---|---|---|---|
| -a---- | 12/9/2024 12:04 AM | 7709840 | Abdul Hayee.pcapng |
| -a---- | 9/17/2024 7:20 PM | 2233 | Assignment1.py |
| -a---- | 9/18/2024 12:46 PM | 1706 | task.py |
| -a---- | 12/8/2024 11:18 PM | 7578020 | wireless_connection.pcap |

**TASK 2:**

**Python, Numpy, Pandas and Matplotib**

Code:




Output:

PS E:\Abdulhayee\Task 1> python .\task.py runserver
Dataset Preview:

```
                          id_flow        nw_src  tp_src        nw_dst  ...  reverse_duration  reverse_size_packets  reverse_size_bytes  category
0  b2bb77a570fcfa9325eb9e51b6116d2a  172.16.25.104   41402  34.107.221.82  ...               121                    15                1114       WWW
1  f07977b0d1d6645c4fe1e9efea080ff3  172.16.25.104   41406  34.107.221.82  ...               121                    15                1114       WWW
2  e4026ba9b6c1957516e92bdd0d04878f  172.16.25.104   38232    52.84.77.43  ...                91                     9                 540       WWW
3  e2d747932e41500b1463fe8ae4299ecb  172.16.25.104   38234    52.84.77.43  ...                91                     9                 540       WWW
4  56325703391225ad65e013e7a2b02fac  172.16.25.104   60166    52.32.34.32  ...                31                     4                 265       WWW
```

```
[5 rows x 65 columns]

Traffic Summary by Category (forward_pc, reverse_size_packets, reverse_duration):
          forward_pc  reverse_size_packets  reverse_duration
category
FTP       37578.361607         1.705624e+06      23487.343750
ICMP       4807.452555         4.291428e+05       4902.442822
VOIP       3590.930502         3.169317e+05       4255.722008
WWW        1883.438855         2.079087e+05       2072.542331
DNS         841.059459         4.888738e+04        511.243243
P2P         221.001408         9.107023e+03        155.167606

Correlation Matrix:
                      forward_pc  forward_bc  reverse_size_packets  reverse_duration
forward_pc              1.000000    0.997520              0.575918          0.654478
forward_bc              0.997520    1.000000              0.564013          0.640959
reverse_size_packets    0.575918    0.564013              1.000000          0.884743
reverse_duration        0.654478    0.640959              0.884743          1.000000
```

## Dataset overview

The dataset contains various metrics related to telecommunication traffic, such as:

Source (nw_src) and destination (nw_dst) IP addresses

Source (tp_src) and destination (tp_dst) ports

Traffic characteristics like packet counts (forward_pc), packet sizes, and inter-arrival times (piat).

Category labels (e.g., WWW, FTP, VOIP).

## Traffic Summary by Category

By grouping the data by category, we analyzed average traffic metrics for different traffic types. Key insights include:

FTP traffic generates the largest number of forward packets and has the highest reverse size and duration, indicating it handles large volumes of data.

ICMP and VOIP traffic show high packet and size metrics but are smaller compared to FTP.

WWW traffic is moderate in terms of packet count and size, while DNS and P2P have relatively smaller traffic. Here’s a summary of the most relevant metrics:

| Category | Forward Packet | Reverse Size Packets | Reverse Duration |
|---|---|---|---|
| FTP | 37578.36 | 1.7 million | 23487.34 |
| ICMP | 4807.45 | 429k | 4902.44 |
| VOIP | 3590.93 | 316k | 4255.72 |
| WWW | 1883.44 | 208k | 2072.54 |
| DNS | 841.06 | 48k | 511.24 |
| P2P | 221.00 | 9k | 155.16 |

## Correlation Analysis

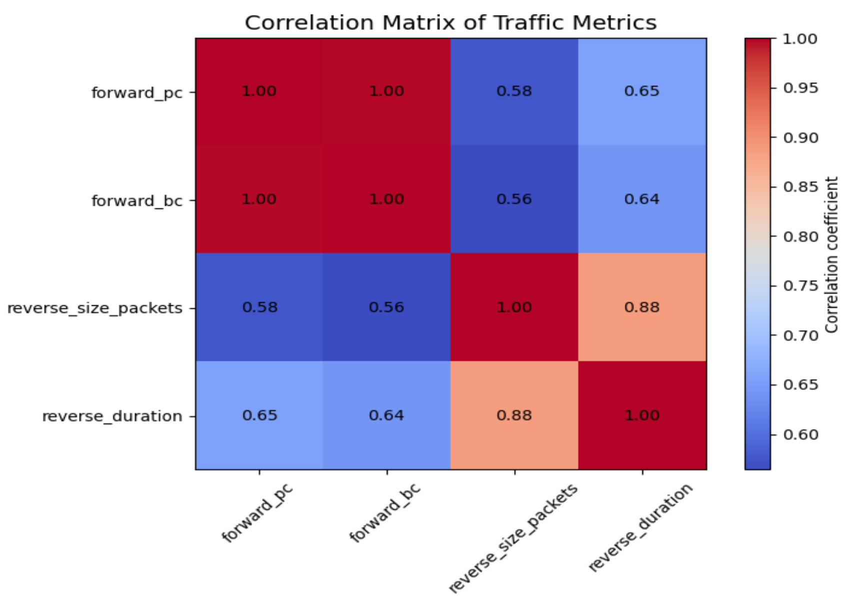
Using a correlation matrix, we analyzed the relationship between various traffic metrics:

Metrics like forward packet count (forward_pc) and reverse packet size show moderate to high correlation, implying that an increase in forward traffic is often matched by increased reverse traffic. Forward byte count (forward_bc) shows a strong positive correlation with forward packet count, suggesting that higher packet counts naturally lead to a higher volume of bytes transmitted.

## Visualization

A heatmap was generated to visually represent the correlation between metrics, with values ranging from -1 to 1. Strong correlations are indicated by colors on the scale, highlighting key relationships between traffic metrics.

This analysis provides a clear understanding of how different types of telecommunication traffic behave in terms of data transfer, packet sizes, and durations, with correlations showing how these metrics are interrelated.



**Conclusion:**

The lab work conducted a comprehensive analysis of network traffic through Wireshark packet capture and advanced data analysis techniques, revealing intricate details about network communication and performance. The Wireshark packet capture demonstrated a network environment predominantly characterized by IPv4 traffic, with UDP protocols accounting for a significant 92.6% of the total network communication. This analysis uncovered a nuanced network topology with multiple nodes and varying traffic patterns, highlighting the complex interactions between different network endpoints.

The Python-based data analysis provided deeper insights into the telecommunication traffic, categorizing and quantifying different types of network interactions. Notably, FTP traffic emerged as the most data-intensive category, generating the largest number of forward packets and exhibiting the highest reverse size and duration. This suggests that file transfer protocols play a crucial role in the network's data exchange, handling substantial volumes of information compared to other traffic types like ICMP, VOIP, and web traffic.

Correlation analysis revealed fascinating interconnections between various network metrics, demonstrating that forward packet counts strongly correlate with byte counts, and reverse packet sizes show significant relationships with traffic duration. These findings provide valuable insights into network behavior, showing how different traffic types interact and how metrics are fundamentally linked. The analysis not only quantifies network performance but also offers a nuanced understanding of the underlying communication patterns.

The minor network issues detected, such as TCP connection resets and QUIC handshake decryption challenges, suggest areas for potential network optimization. While these problems were not critical, they indicate the complexity of modern network communications and the importance of continuous monitoring and analysis. The comprehensive approach taken in this lab working combining packet capture, statistical analysis, and detailed categorization—provides a robust methodology for understanding network performance and identifying potential areas of improvement.