| 1403/11/17 | 4001830235 | محمد مهدی رسول امینی |
|---|---|---|

## UDP Packet Analysis Using Wireshark

## Introduction

In this lab, we analyze the UDP transport protocol using Wireshark. By executing an `nslookup` command to resolve the IP address of `digikala.com`, we capture UDP packets and study their structure, fields, and characteristics.

---

## Packet Capture and Analysis

### Step 1: Capturing UDP Packets

1. Open **Wireshark** and start a packet capture on the active network interface.
2. Execute the following command in the terminal or command prompt:
```
nslookup digikala.com
```
4. Stop the packet capture after receiving a response.
5. Apply the following filter in Wireshark to isolate UDP packets:
```
udp
```

### Step 2: Extracting UDP Packet Details

- The first UDP segment found in the trace file is **Packet #25**.
- The application-layer protocol encapsulated in this packet is **DNS (Domain Name System)**.
- Expanding the UDP header in Wireshark reveals four fields:
    1. **Source Port:** 49512
    2. **Destination Port:** 53 (DNS Server)
    3. **Length:** 50 bytes
    4. **Checksum:** Computed value

### Step 3: UDP Header Field Sizes

Each field in the UDP header has a fixed size:

- **Source Port:** 2 bytes (16 bits)
- **Destination Port:** 2 bytes (16 bits)
- **Length:** 2 bytes (16 bits)
- **Checksum:** 2 bytes (16 bits)
- **Total UDP Header Size:** 8 bytes

**Step 4: Interpreting the Length Field**

- The value in the **Length field** represents the total size of the UDP segment, including both the **header and the payload**.
- For the DNS request, the **length is 50 bytes**, confirming:
- `UDP Header (8 bytes) + DNS Query Data (42 bytes) = 50 bytes`

**Step 5: Maximum UDP Payload Size**

- The maximum possible UDP segment size is **65535 bytes** (due to the 16-bit Length field).
- Deducting 8 bytes for the UDP header, the **maximum UDP payload is 65527 bytes**.

**Step 6: Maximum Source Port Number**

- The UDP port field is 16-bit, allowing a maximum **port number of 65535**.

**Step 7: UDP Protocol Number in IP Header**

- In the IP header, UDP is identified by **Protocol Number 17 (decimal).**

---

## UDP Request-Response Analysis

We analyze the request-response exchange between the client and the DNS server:

**First UDP Packet (DNS Query from Client)**

- **Packet Number:** 25
- **Source Port:** 49512
- **Destination Port:** 53 (DNS Server)

**Second UDP Packet (DNS Response from Server)**

- **Packet Number:** 26
- **Source Port:** 53 (DNS Server)
- **Destination Port:** 49512

**Port Number Relationship**

- The **source port** of the first packet becomes the **destination port** in the response packet, and vice versa.
- This confirms a proper **request-response exchange** between the client and DNS server.

---

## Graphical Analysis Using Wireshark

### 1. UDP Packet Count Over Time

- **Path:** `Wireshark → Statistics → I/O Graphs`
- **Filter:** `udp`
- **Graph Representation:** UDP packets per second over time.

### 2. Flow of UDP Packets Between Client and Server

- **Path:** `Wireshark → Statistics → Flow Graph`
- **Visual Representation:** Sequence of UDP packet exchanges.

---

## Conclusion

- The `nslookup digikala.com` command successfully generated UDP packets captured in Wireshark.
- The DNS request and response exchanged between **port 49512 (client) and port 53 (DNS server)** were observed.
- The UDP header fields, their sizes, and maximum capacity constraints were verified.
- The **Wireshark graphical tools provided a clear visualization** of UDP packet activity.
- This experiment demonstrates how **UDP functions as a lightweight, connectionless protocol**, ideal for **fast, low-overhead data transmission** such as DNS queries.
-