Shaheed Zulfikar Ali Bhutto Institute of Science & Technology

COMPUTER SCIENCE DEPARTMENT

Total Marks: _____

Obtained Marks: _____

CNDC

Lab Task 6-7

Submitted To: Sir Ammad Noor

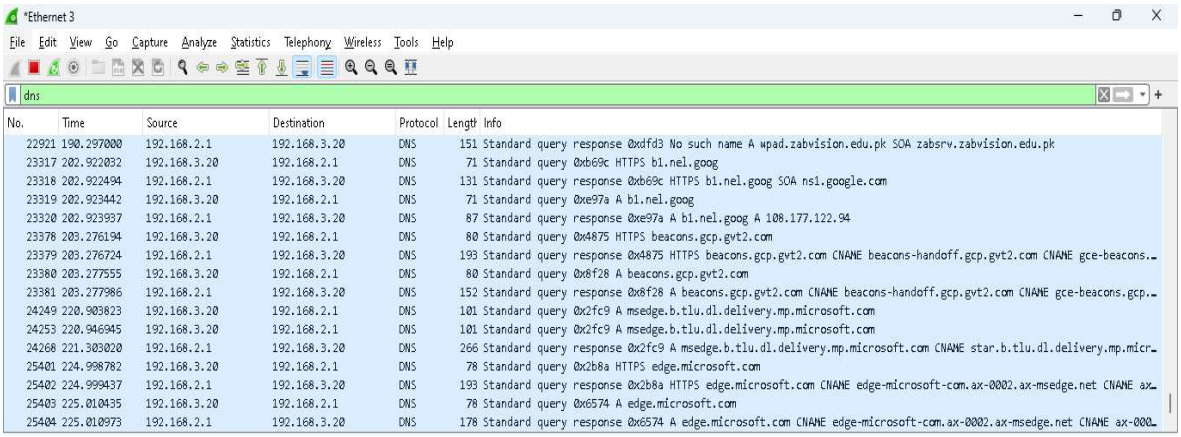
Student Name: Ubaid Bin Waris

Reg Number: 2212416

1. **Task 1: IP Header Analysis**
2. Version: 4 (IPv4 packet)
3. Header Length: 20 bytes (standard, no options)
4. Total Length: 345 bytes (IP header + UDP + DNS payload)
5. Identification: 0x688c (26764) – unique number for fragmentation
6. TTL: 128 – maximum hops for packet
7. Protocol: UDP (17) – carries UDP segment
8. Source IP: 192.168.2.1 – DNS server/router
9. Destination IP: 192.168.3.20 – client PC

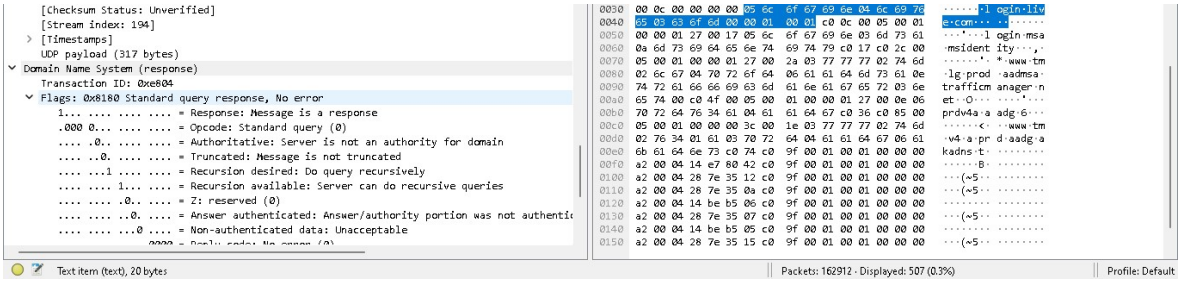
Task 2: UDP Header Examination

1. Source Port: 53 – DNS server port (response)
2. Destination Port: 49655 – ephemeral port on client PC
3. Length: 325 bytes (UDP header + payload)
4. Checksum: 0x5655 [unverified] – error checking
5. UDP Payload Size: 317 bytes (325 − 8)
6. Significance of port 53: Standard port used for DNS queries/responses



Task 3: DNS Query Breakdown

1. Transaction ID: 0xe804 – matches request and response
2. Flags: 0x8180 – standard query response, recursion available, no error
3. Questions: 1 – number of domain queries
4. Answer RRs: 12 – number of answers in response
5. Authority RRs: 0 – none
6. Additional RRs: 0 – none
7. Domain Name Queried: login.live.com, type A, class IN



1. **Task 4: Relationship Between IP → UDP → DNS**
2. Encapsulation: IP Header → UDP Header → DNS Response Data
3. Why DNS uses UDP:
   - Faster than TCP
   - No handshake
   - Less overhead
   - Most DNS queries fit in one UDP packet

1) **Task 5: Response Tracking in Wireshark**
2) "Request In": 2911 – the request frame for this response
3) Linking query and response helps:
   a) Confirms server replied
   b) Matches Transaction ID
   c) Allows analysis of response time/errors
4) Comparison:
   a) Transaction ID: 0xe804 (request & response same)
   b) Domain Name: live.com (same)
   c) Flags: request = 0x0100 (query), response = 0x8180 (response)
   d) Answers: request = 0, response = 12
5) Response time: 0.051 seconds

Shaheed Zulfikar Ali Bhutto Institute of Science & Technology

COMPUTER SCIENCE DEPARTMENT