



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

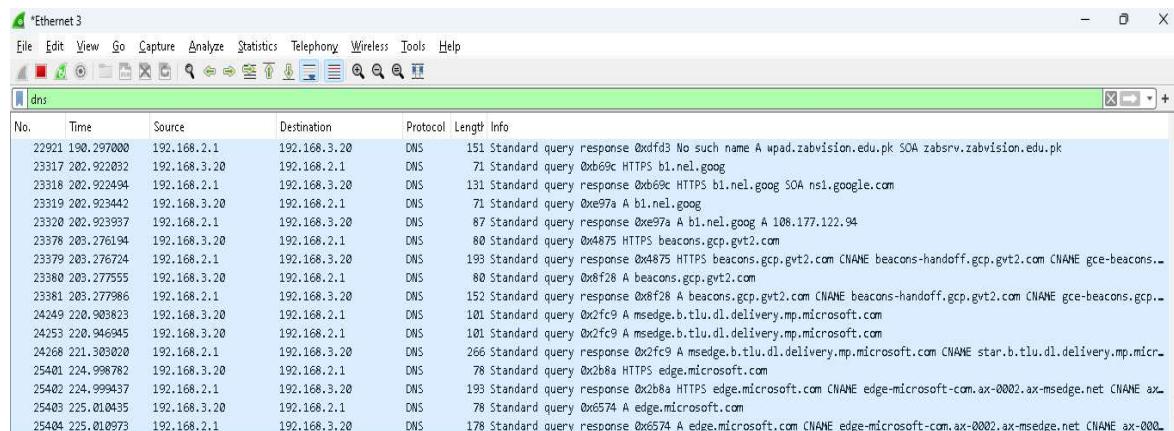
Reg Number: 2212416

COMPUTER SCIENCE DEPARTMENT

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



No.	Time	Source	Destination	Protocol	Length	Info
22921	190.297000	192.168.2.1	192.168.3.20	DNS	151	Standard query response 0xdfd3 No such name A wpad.zabvision.edu.pk SOA zabsrv.zabvision.edu.pk
23317	202.922032	192.168.3.20	192.168.2.1	DNS	71	Standard query 0xb69c HTTPS b1.nel.goog
23318	202.922494	192.168.2.1	192.168.3.20	DNS	131	Standard query response 0xb69c HTTPS b1.nel.goog SOA ns1.google.com
23319	202.923442	192.168.3.20	192.168.2.1	DNS	71	Standard query 0xe97a A b1.nel.goog
23320	202.923937	192.168.2.1	192.168.3.20	DNS	87	Standard query response 0xe97a A b1.nel.goog A 108.177.122.94
23378	203.276194	192.168.3.20	192.168.2.1	DNS	80	Standard query 0x4875 HTTPS beacons.gcp.gvt2.com
23379	203.276724	192.168.2.1	192.168.3.20	DNS	193	Standard query response 0x4875 HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com CNAME gce-beacons..
23380	203.277555	192.168.3.20	192.168.2.1	DNS	80	Standard query 0x8f28 A beacons.gcp.gvt2.com
23381	203.277986	192.168.2.1	192.168.3.20	DNS	152	Standard query response 0x8f28 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com CNAME gce-beacons.gcp..
24249	220.903823	192.168.3.20	192.168.2.1	DNS	101	Standard query 0x2fc9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
24253	220.946945	192.168.3.20	192.168.2.1	DNS	101	Standard query 0x2fc9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
24268	221.303024	192.168.2.1	192.168.3.20	DNS	266	Standard query response 0x2fc9 A msedge.b.tlu.dl.delivery.mp.microsoft.com star.b.tlu.dl.delivery.mp.microsoft.com
25401	224.998782	192.168.3.20	192.168.2.1	DNS	78	Standard query 0x2b8a HTTPS edge.microsoft.com
25402	224.999437	192.168.2.1	192.168.3.20	DNS	193	Standard query response 0x2b8a HTTPS edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME ax..
25403	225.010435	192.168.3.20	192.168.2.1	DNS	78	Standard query 0x6574 A edge.microsoft.com
25404	225.010973	192.168.2.1	192.168.3.20	DNS	178	Standard query response 0x6574 A edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME ax-000..

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



Shaheed Zulfikar Ali Bhutto Institute of Science & Technology

COMPUTER SCIENCE DEPARTMENT

	[Checksum Status: Unverified]	[Stream index: 194]	[Timestamps]	[Plcsoft-liv]
> [Timestamps]				1.0 1.0 1.0 1.0 1.0
UDF payload (317 bytes)				1.0 1.0 1.0 1.0 1.0
Domain Name System (response)				1.0 1.0 1.0 1.0 1.0
Transaction ID: 0xe6e4				1.0 1.0 1.0 1.0 1.0
Flags: 0x8180 Standard query response, No error				1.0 1.0 1.0 1.0 1.0
..... = Response: Message is a response				1.0 1.0 1.0 1.0 1.0
..000 0... = Opcode: Standard query (0)				1.0 1.0 1.0 1.0 1.0
..0. = Authoritative: Server is not an authority for domain				1.0 1.0 1.0 1.0 1.0
....0. = Truncated: Message is not truncated				1.0 1.0 1.0 1.0 1.0
....1. = Recursion desired: Do query recursively				1.0 1.0 1.0 1.0 1.0
....1. = Recursion available: Server can do recursive queries				1.0 1.0 1.0 1.0 1.0
....0. = Reserved (0)				1.0 1.0 1.0 1.0 1.0
....0. = Z: Reserved (0)				1.0 1.0 1.0 1.0 1.0
....0. = Answer authenticated: Answer/authority portion was not authentic				1.0 1.0 1.0 1.0 1.0
....0. = Non-authenticated data: Unacceptable				1.0 1.0 1.0 1.0 1.0
....0. = RCODE: code= No error (0)				1.0 1.0 1.0 1.0 1.0
0x0300 00 0c 00 03 00 00 05 6f 5f 67 69 6c 05 6c 00 76				1.0 1.0 1.0 1.0 1.0
0x0400 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 01				1.0 1.0 1.0 1.0 1.0
0x0500 00 00 01 27 08 17 05 6c 6f 67 69 6e 09 6d 73 61				1.0 1.0 1.0 1.0 1.0
0x0600 08 6d 73 69 64 65 6d 74 69 74 79 c0 17 c0 2c 00				1.0 1.0 1.0 1.0 1.0
0x0700 05 00 01 00 02 01 27 08 2a 03 77 77 77 02 74 6d				1.0 1.0 1.0 1.0 1.0
0x0800 02 6c 67 04 70 72 6f 6d 06 61 64 6d 73 61 0e				1.0 1.0 1.0 1.0 1.0
0x0900 74 72 61 66 69 63 6d 61 6e 67 65 72 03 0e				1.0 1.0 1.0 1.0 1.0
0x0a00 65 74 00 02 04 0f 00 00 02 01 00 00 01 27 00 0e				1.0 1.0 1.0 1.0 1.0
0x0b00 70 72 64 76 34 61 01 61 64 67 00 36 00 85 00				1.0 1.0 1.0 1.0 1.0
0x0c00 05 00 01 00 00 00 3c 00 18 03 77 77 77 02 74 6d				1.0 1.0 1.0 1.0 1.0
0x0d00 02 76 61 64 65 6d 74 69 74 79 c0 17 c0 2c 00				1.0 1.0 1.0 1.0 1.0
0x0e00 04 6e 67 04 70 72 6f 6d 06 61 64 6d 73 61 0e				1.0 1.0 1.0 1.0 1.0
0x0f00 02 00 04 14 7c 80 42 00 0f 00 01 00 01 00 00 00				1.0 1.0 1.0 1.0 1.0
0x1000 02 00 04 28 7e 35 12 00 0f 00 01 00 01 00 00 00				1.0 1.0 1.0 1.0 1.0
0x1100 02 00 04 28 7e 35 03 00 0f 00 01 00 01 00 00 00				1.0 1.0 1.0 1.0 1.0
0x1200 02 00 04 14 0b b5 00 00 0f 00 01 00 01 00 00 00				1.0 1.0 1.0 1.0 1.0
0x1300 02 00 04 28 7e 35 07 00 0f 00 01 00 01 00 00 00				1.0 1.0 1.0 1.0 1.0
0x1400 02 00 04 14 be b5 00 00 0f 00 01 00 01 00 00 00				1.0 1.0 1.0 1.0 1.0
0x1500 02 00 04 28 7e 35 15 00 0f 00 01 00 01 00 00 00				1.0 1.0 1.0 1.0 1.0

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

Task 5: Response Tracking in Wireshark

“Request In”: 2911 – the request frame for this response

Linking query and response helps:

 - a) Confirms server replied
 - b) Matches Transaction ID
 - c) Allows analysis of response time/errors

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

Response time: 0.051 seconds



Shaheed Zulfikar Ali Bhutto Institute of Science &
Technology

COMPUTER SCIENCE DEPARTMENT