



Faculty of Engineering

Department of computer and Electrical Engineering

Data Com Lab

"Lab(03)"

Submitted By:

Musab Alaswed

No:120221213

Submitted To:

Eng.Abdullah Ouda

Lab_work 1

dns use 5 layer (application layer)

The screenshot shows a Wireshark capture of DNS traffic. The packet list on the left shows a standard query (No. 9) and a standard query response (No. 10) for config.edge.skype.com. The packet details pane on the right shows the structure of the DNS message, including the query type (A) and the response (A). The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.009982	fd7f:c411:7178:0:a9...	fd7f:c411:7178::1	DNS	101	Standard query 0xf510 A config.edge.skype.com
10	0.010307	fd7f:c411:7178:0:a9...	fd7f:c411:7178::1	DNS	101	Standard query response 0x6e09 HTTPS config.edge.skype.com

arp use 3 layer (Network layer)

The screenshot shows a Wireshark capture of ARP traffic. The packet list on the left shows an ARP request (No. 1026) and an ARP response (No. 1027) for 10.10.8.17. The packet details pane on the right shows the structure of the ARP message, including the source and destination IP addresses and the hardware type (Ethernet II). The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1026	5.072624	52:ff:e0:2b:fd:87	Broadcast	ARP	60	who has 10.10.8.17 Tell 10.10.8.70
1027	5.072624	52:ff:e0:2b:fd:87	Broadcast	ARP	60	who has 10.10.8.17 Tell 10.10.8.70

tcp use 4 layer (Transport layer)

Wireshark packet capture showing TCP traffic. The packet list shows a sequence of TCP segments. The packet details pane shows the structure of a TCP segment, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Frame 1879: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF...
Ethernet II, Src: Routerboard_e3:af:27 (c4:ad:34:e3:af:27), Dst: AzureIaveTec_e0:9d:e5 (34:6f:24:e0:9d:e5)
Destination: AzureIaveTec_e0:9d:e5 (34:6f:24:e0:9d:e5)
Type: IPv4 (0x0800)
[Stream index: 0]
Padding: 000000000000
Internet Protocol Version 4, Src: 216.239.32.223, Dst: 10.10.8.71
Transmission Control Protocol, Src Port: 443, Dst Port: 50038, Seq: 4697, Ack: 50087, Len: 0

Lab_work 2

Login | Personal Contacts Manager v1.0

Email*

dadad@gmail.com

Password*

.....

☐ Remember me

Submit

Dashboard | Personal Contacts Manager v1.0

Add New Contact Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	myname	jenefy	9898989898	admin@gmail.com	
102391	Danish	Shaikh	9012365487	danishshaikh@gmail.com	Edit
102392	Shahzan	Mehdi	9555034298	mehdishahzan78@gmail.com	Edit
102393	iconic	doremon	8198985856	dora@gmail.com	Edit
102394	Anuraag	bheem	09619910186	bheem@gmail.com	Edit
102395	Avaan	doremon	8198985856	dora@gmail.com	Edit
102396	Soham	Sawant	9819123373	sohamded@gmail.com	Edit
102397	I Love you	raj	95036052025	admin@google.com	Edit
102398	Aa	y	8995412377	yca@gmail.com	Edit
102399	tasneem	rami	059*****	tttora2017@gmail.com	Edit
102400	uuuuuu	oooooooo	059*****	tttora2017@gmail.com	Edit
102401	uuuuuu	oooooooo	059*****	tttora2017@gmail.com	Edit
102402	uuuuuu	oooooooo	059*****	tttora2017@gmail.com	Edit
102403	aa	dd	0598521475	anas_aldeeb@gmail.com	Edit
102404	mm	dd	54789	ash@gmail.com	Edit
102405	qq	ww	78965412	awd@gmail.com	Edit

Total Records Count: 16

Wireshark packet capture showing HTTP traffic. The packet list shows a GET request to /index.php. The packet details pane shows the reassembled TCP segments and the HTTP request structure. The packet bytes pane shows the raw data.

Frame 8199: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits) on interface 'Device'...

Internet Protocol Version 4, Src: 217.174.153.53, Dst: 10.10.8.71

Transmission Control Protocol, Src Port: 80, Dst Port: 50220, Seq: 1461, Ack: 500, Len: 676

Hypertext Transfer Protocol

Line-based text data: text/html (22 lines)

Frame (730 bytes) Reassembled TCP (2136 bytes)

Packets: 9074 - Displayed: 22 (0.2%) - Dropped: 0 (0.0%)

http use 5 layer (application layer)

Add post

Wireshark packet capture showing HTTP traffic. The packet list shows a POST request to /index.php. The packet details pane shows the reassembled TCP segments and the HTTP request structure. The packet bytes pane shows the raw data.

Frame 998: 780 bytes on wire (6240 bits), 780 bytes captured (6240 bits) on interface 'Device'...

Internet Protocol Version 4, Src: 10.10.8.71, Dst: 217.174.153.53

Transmission Control Protocol, Src Port: 50286, Dst Port: 80, Seq: 1, Ack: 1, Len: 726

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

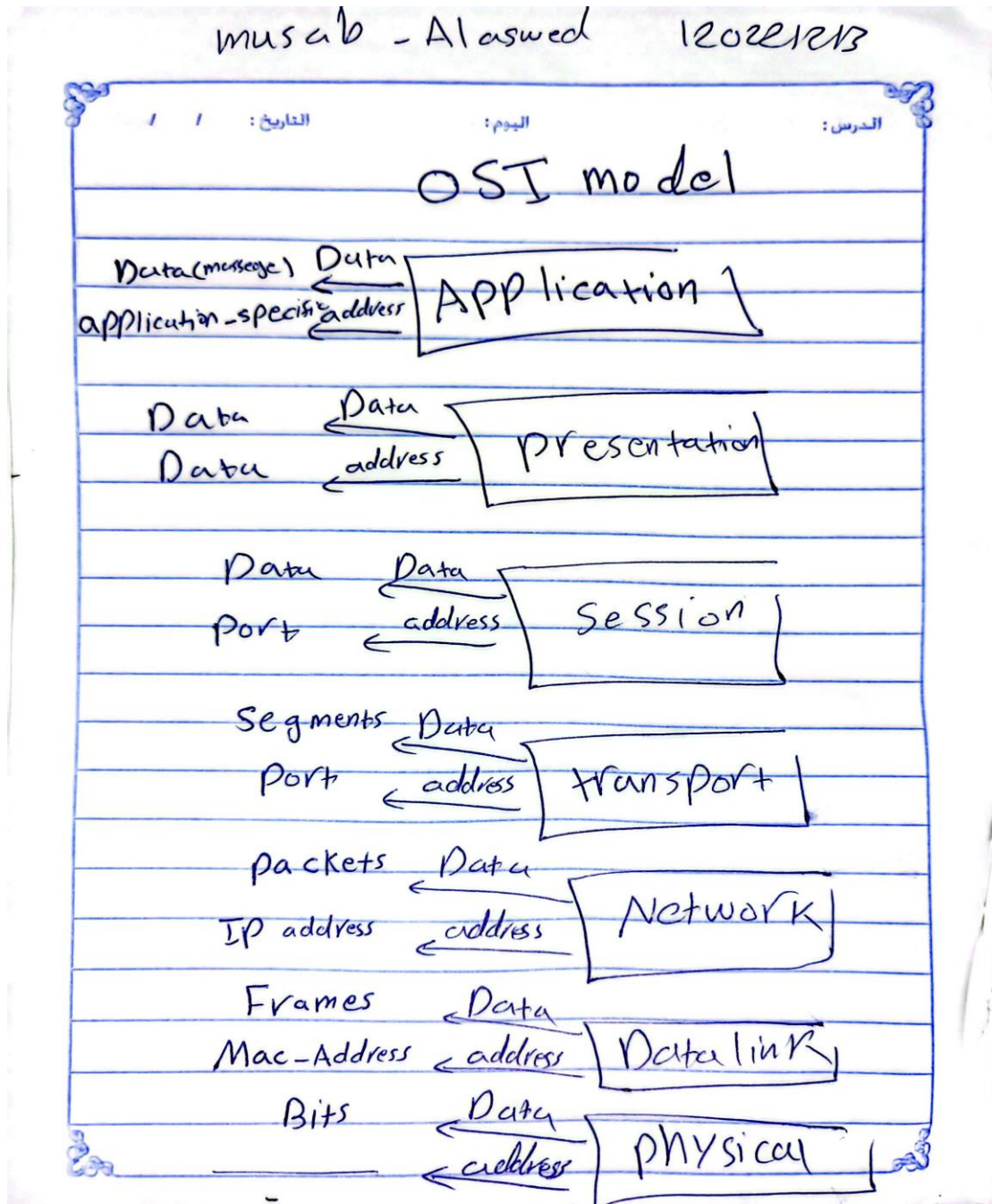
Form item: "email" = "dadad@gmail.com"

Form item: "password" = "dsafdsawer"

Frame (780 bytes) Reassembled TCP (2136 bytes)

Packets: 1097 - Displayed: 28 (2.6%) - Dropped: 0 (0.0%)

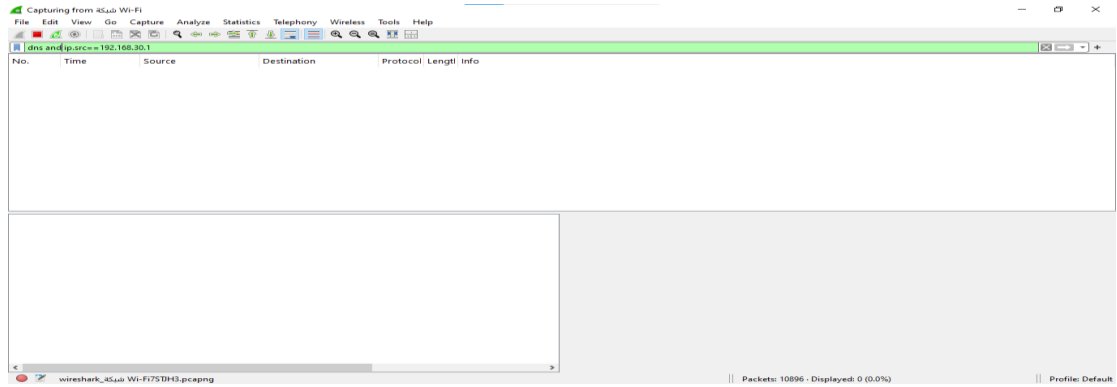
Q1: Draw the OSI model, then show the types of data and address types at each layer.



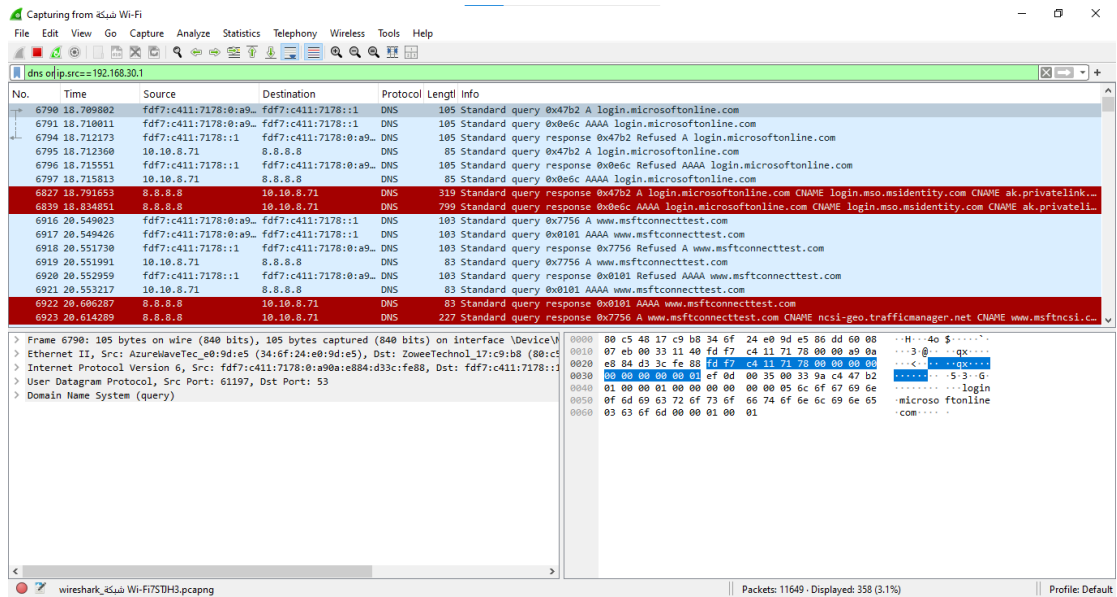
Q2: Create a command line to put it into the Filter window to get the following:

- DNS packets with source ip = 192.168.30.1

dns and ip.src==192.168.30.1 (تحقق الاثنين معا)



dns or ip.src==192.168.30.1 (تحقق احد الحالتين)



- All packets except the packets with ip = 192.168.30.1

The screenshot shows the Wireshark interface with the filter `!(ip.src==192.168.30.1 and ip.dst==192.168.30.1)` applied. The packet list displays 16 packets, including MDNS, DHCP, ICMPv6, and TLSv1.2. The packet details pane shows the selected packet (No. 16) as a Domain Name System (query) packet. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.9.254	224.0.0.251	MDNS	127	Standard query 0x0000 ANY Android-100.local, "QM" question ANY Android-100.local, "QM" question A 10.10.9...
2	0.001787	fe80::ef8f:7848:91d...	ff02::fb	MDNS	147	Standard query 0x0000 ANY Android-100.local, "QM" question ANY Android-100.local, "QM" question A 10.10.9...
3	0.005006	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xee736ae7
4	0.006333	fe80::ef8f:7848:91d...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
5	0.008255	213.244.74.83	10.10.8.71	UDP	1274	443 → 51245 Len=1232
6	0.011295	57.144.244.145	10.10.8.71	TLSv1.2	86	Application Data
7	0.011328	10.10.8.71	57.144.244.145	TCP	54	[TCP ACKed unseen segment] 52544 → 443 [ACK] Seq=1 Ack=151 Win=259 Len=0
8	0.011473	10.10.8.71	213.244.74.83	UDP	79	51245 → 443 Len=37
9	0.011913	213.244.74.83	10.10.8.71	UDP	1274	443 → 51245 Len=1232
10	0.011913	213.244.74.83	10.10.8.71	UDP	1274	443 → 51245 Len=1232
11	0.011904	10.10.8.71	57.144.244.145	TLSv1.2	90	Application Data
12	0.013841	10.10.8.71	57.144.244.145	TLSv1.2	90	Application Data
13	0.013558	213.244.74.83	10.10.8.71	UDP	1274	443 → 51245 Len=1232
14	0.016776	213.244.74.83	10.10.8.71	UDP	1274	443 → 51245 Len=1232
15	0.016935	10.10.8.71	213.244.74.83	UDP	76	51245 → 443 Len=34
16	0.023945	213.244.74.83	10.10.8.71	UDP	1274	443 → 51245 Len=1232

- Display http packet or DNS packet with source ip = 192.168.30.2 and destination ip = 192.168.30.4



(http or dns) and (ip.src==192.168.30.2 && ip.dst==192.168.30.4)

The screenshot shows the Wireshark interface with the filter `(http or dns) and (ip.src==192.168.30.2 && ip.dst==192.168.30.4)` applied. The packet list is currently empty, indicating that no packets matching the filter were found in the capture.

Q3: Capture packets in wireshark, and show me the details of layers. Please put your screenshot.

5 layer → DNS

Wireshark interface showing a capture of DNS traffic. The packet list displays several DNS queries and responses. The packet details pane shows the structure of a DNS query packet, including the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query) layers.

Handwritten text "Slaxer" is visible in the bottom right corner of the screenshot.

Wireshark interface showing a capture of HTTP traffic. The packet list displays several HTTP GET requests and responses. The packet details pane shows the structure of an HTTP GET request packet, including the Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers.

Wireshark interface showing a capture of ARP traffic. The packet list displays several ARP requests and responses. The packet details pane shows the structure of an ARP request packet, including the Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol layers.

Wireshark packet capture analysis showing UDP traffic. The packet list displays various DNS queries and responses. The packet details pane shows the structure of a DNS response, including the header, question, and answer sections. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6902	20.353504	10.10.8.71	20.190.177.84	TCP	54	52572 → 443 [ACK] Seq=2516 Ack=7897 Win=261888 Len=0
6903	20.353504	10.10.8.71	20.190.177.84	TCP	54	52572 → 443 [RST, ACK] Seq=2516 Ack=7897 Win=0 Len=0
6904	19.723406	10.10.8.71	57.144.244.145	TLSv1.2	83	Application Data
6905	19.883701	57.144.244.145	10.10.8.71	TCP	60	443 → 52541 [ACK] Seq=26 Ack=59 Win=498 Len=0
6906	19.978765	57.144.244.145	10.10.8.71	TLSv1.2	79	Application Data
6907	19.981242	10.10.8.71	57.144.244.145	TLSv1.2	123	Application Data
6908	20.028596	10.10.8.71	57.144.244.145	TCP	54	52541 → 443 [ACK] Seq=59 Ack=51 Win=258 Len=0
6909	20.172893	57.144.244.145	10.10.8.71	TLSv1.2	125	Application Data
6910	20.219250	10.10.8.71	57.144.244.145	TCP	54	52554 → 443 [ACK] Seq=70 Ack=72 Win=1039 Len=0
6911	20.616192	10.10.8.71	213.244.74.210	TCP	66	52573 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
6912	20.626429	10.10.8.71	213.244.74.210	TCP	66	80 → 52573 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
6913	20.626753	10.10.8.71	213.244.74.210	HTTP	165	GET /connecttest.txt HTTP/1.1
6914	20.637219	213.244.74.210	10.10.8.71	TCP	60	80 → 52573 [ACK] Seq=1 Ack=112 Win=64256 Len=0
6915	20.638894	213.244.74.210	10.10.8.71	HTTP	241	HTTP/1.1 200 OK (text/plain)
6916	20.638894	213.244.74.210	10.10.8.71	TCP	60	80 → 52573 [FIN, ACK] Seq=108 Ack=112 Win=64256 Len=0

Wireshark packet capture analysis showing TCP traffic. The packet list displays various TCP connections and data transfers. The packet details pane shows the structure of a TCP segment, including the header and data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6902	19.353504	10.10.8.71	20.190.177.84	TCP	54	52572 → 443 [ACK] Seq=2516 Ack=7897 Win=261888 Len=0
6903	19.421852	10.10.8.71	20.190.177.84	TCP	54	52572 → 443 [RST, ACK] Seq=2516 Ack=7897 Win=0 Len=0
6904	19.723406	10.10.8.71	57.144.244.145	TLSv1.2	83	Application Data
6905	19.883701	57.144.244.145	10.10.8.71	TCP	60	443 → 52541 [ACK] Seq=26 Ack=59 Win=498 Len=0
6906	19.978765	57.144.244.145	10.10.8.71	TLSv1.2	79	Application Data
6907	19.981242	10.10.8.71	57.144.244.145	TLSv1.2	123	Application Data
6908	20.028596	10.10.8.71	57.144.244.145	TCP	54	52541 → 443 [ACK] Seq=59 Ack=51 Win=258 Len=0
6909	20.172893	57.144.244.145	10.10.8.71	TLSv1.2	125	Application Data
6910	20.219250	10.10.8.71	57.144.244.145	TCP	54	52554 → 443 [ACK] Seq=70 Ack=72 Win=1039 Len=0
6911	20.616192	10.10.8.71	213.244.74.210	TCP	66	52573 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
6912	20.626429	10.10.8.71	213.244.74.210	TCP	66	80 → 52573 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
6913	20.626753	10.10.8.71	213.244.74.210	HTTP	165	GET /connecttest.txt HTTP/1.1
6914	20.637219	213.244.74.210	10.10.8.71	TCP	60	80 → 52573 [ACK] Seq=1 Ack=112 Win=64256 Len=0
6915	20.638894	213.244.74.210	10.10.8.71	HTTP	241	HTTP/1.1 200 OK (text/plain)
6916	20.638894	213.244.74.210	10.10.8.71	TCP	60	80 → 52573 [FIN, ACK] Seq=108 Ack=112 Win=64256 Len=0