

شبکه های کامپیوتری

امتحان وایر شارک

مصطفی فضلی - ۹۸۲۲۸۰۳

سوال 1

The image displays a Wireshark packet capture and a Windows command prompt window. The Wireshark window shows a packet capture on the 'Wi-Fi' interface, with a packet list and packet details pane. The packet details pane shows the structure of an ICMP Echo (ping) request from 192.168.243.162 to 152.89.13.54. The packet list shows a series of ICMP Echo requests and responses, with some requests timed out. The Windows command prompt window shows the execution of the command 'tracert sharif.ir', which traces the route to sharif.ir [152.89.13.54] over a maximum of 30 hops. The output shows the route taken by the ping requests, including the source IP, destination IP, and the time taken for each hop.

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
77	318612	192.168.243.162	172.26.0.5	NBNS	92	Name query NBSTAT *<00><00><00>
78	816355	192.168.243.162	172.26.0.5	NBNS	92	Name query NBSTAT *<00><00><00>
80	317615	192.168.243.162	172.26.0.5	NBNS	92	Name query NBSTAT *<00><00><00>
81	246043	192.168.243.141	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
82	269269	192.168.243.141	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
82	759974	192.168.243.162	152.89.13.54	ICMP	106	Echo (ping) request id=0x0001
82	901806	172.26.0.9	192.168.243.162	ICMP	134	Time-to-live exceeded (Time to
82	903867	192.168.243.162	152.89.13.54	ICMP	106	Echo (ping) request id=0x0001
83	054304	172.26.0.9	192.168.243.162	ICMP	134	Time-to-live exceeded (Time to
83	057209	192.168.243.162	152.89.13.54	ICMP	106	Echo (ping) request id=0x0001
83	124270	172.26.0.9	192.168.243.162	ICMP	134	Time-to-live exceeded (Time to
83	125656	192.168.243.162	192.168.243.245	DNS	83	Standard query 0x8a0f PTR 9.0.2
83	221476	192.168.243.245	192.168.243.162	DNS	83	Standard query response 0x8a0f
83	221675	192.168.243.162	172.26.0.9	NBNS	92	Name query NBSTAT *<00><00><00>
83	295610	192.168.243.141	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
84	318198	192.168.243.141	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
84	712925	192.168.243.162	172.26.0.9	NBNS	92	Name query NBSTAT *<00><00><00>
86	215474	192.168.243.162	172.26.0.9	NBNS	92	Name query NBSTAT *<00><00><00>
87	449377	192.168.243.162	18.66.192.125	TCP	55	[TCP Keep-Alive] 51169 > 443 [A
87	540420	18.66.192.125	192.168.243.162	TCP	66	[TCP Keep-Alive ACK] 443 > 5116
87	957632	b2:33:ed:90:ac:a5	192.168.243.162	ARP	42	Who has 192.168.243.162? Tell 1
87	957644	IntelCor_61:8f:b9	b2:33:ed:90:ac:a5	ARP	42	192.168.243.162 is at 34:cf:f6:
88	656131	192.168.243.162	152.89.13.54	ICMP	106	Echo (ping) request id=0x0001
88	725114	172.26.0.33	192.168.243.162	ICMP	70	Time-to-live exceeded (Time to
88	726354	192.168.243.162	152.89.13.54	ICMP	106	Echo (ping) request id=0x0001

Windows Command Prompt:

```
C:\Windows\system32>tracert sharif.ir

Tracing route to sharif.ir [152.89.13.54]
over a maximum of 30 hops:

 0  26 ms  1 ms  2 ms  192.168.243.245
 1  *      *      *      Request timed out.
 2  47 ms  40 ms  49 ms  10.196.23.193
 3  55 ms  53 ms  66 ms  10.196.89.146
 4  *      *      *      Request timed out.
 5  394 ms  51 ms  51 ms  10.196.89.65
 6  *      *      *      Request timed out.
 7  54 ms  52 ms  55 ms  10.136.131.30
 8  68 ms  58 ms  55 ms  10.196.119.5
 9  64 ms  50 ms  59 ms  10.201.217.34
10  66 ms  58 ms  75 ms  172.26.0.5
11  141 ms  151 ms  67 ms  172.26.0.9
12  69 ms  57 ms  58 ms  172.26.0.33
13  150 ms  59 ms  81 ms  172.26.0.50
14  73 ms  59 ms  65 ms  152.89.13.54

Trace complete.
```

Wireshark Packet Details:

Frame 266: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF{5F40C480-567E-4EBC-B7B1-D232EB1111} Ethernet II, Src: IntelCor_61:8f:b9 (34:cf:f6:61:8f:b9), Dst: b2:33:ed:90:ac:a5 (b2:33:ed:90:ac:a5)

Internet Protocol Version 4, Src: 192.168.243.162, Dst: 152.89.13.54

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 92

Identification: 0xd617 (54807)

Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 12

Protocol: ICMP (1)

Header Checksum: 0x7eaf [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.243.162

Destination Address: 152.89.13.54

دستور traceroute در cmd ویندوز فعال نیست، به همین دلیل از دستور tracert استفاده می کنیم که همانند این دستور است. اسکرین شات این بخش در نیمه سمت راست صفحه نمایش آمده است.

بخش اول

همزمان با این دستور فرآیند رهگیری پکت ها و ایر شارک را فعال می کنیم، در این هنگام می توانیم طول هدر را مشاهده می کنیم که برابر ۲۰ بایت است.

طول payload برابر طول کل پکت منهای طول هدر فایل است که طول کل پکت برابر ۹۲ بایت است و اگر ۲۰ بایت را از آن کم کنیم برابر ۷۲ بایت است.

$$92-20=72$$

بخش دوم

اگر بخش fragment offset برابر صفر باشد، بدین معناست که این پکت دارای تکه بعدی نمی باشد.

Wireshark packet capture showing an ICMP Echo (ping) request. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP) fields. The ICMP Echo (ping) request field is highlighted in green, showing the Echo (ping) request with ID 0x0001, sequence 6717152, and TTL 12. The packet bytes pane shows the raw data of the packet.

Packet Details:

- Ethernet II, Src: IntelCor_61:8f:b9 (34:c:f6:61:8f:b9), Dst: b2:33:ed:90:ac:a5 (b2:33:ed:90:ac:a5)
- Internet Protocol Version 4, Src: 192.168.243.162, Dst: 152.89.13.54
- Internet Control Message Protocol

Packet Bytes:

```
0000  b2 33 ed 90 ac a5 34 cf f6 61 8f b9 00 00 45 00  -3--4- -E-
0010  00 5c a6 17 00 00 00 00 00 00 00 00 00 00 00  -\.- -D---Y
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  -6- -D---
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  -.....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  -.....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  -.....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  -.....
```

بخش سوم

فیلدهایی که ثابت میمانند:

ورژن (بخاطر این است که همه پکت ها از یک ورژن آیپی استفاده می کنند)

طول هدر (همه پکت ها از نوع ICMP هستند)

آیپی مبدا (اطلاعات از یک مبدا ارسال می شوند)

آیپی مقصد (اطلاعات به یک مقصد ارسال می شوند)

لایه بالایی پروتکل (هنگامی که همه پکت ها از نوع ICMP هستند)

خدمات مختلف

فیلدهایی که باید ثابت بمانند:

ورژن (بخاطر این است که همه پکت ها از یک ورژن آیپی استفاده می کنند)

طول هدر (همه پکت ها از نوع ICMP هستند)

آیپی مبدا (اطلاعات از یک مبدا ارسال می شوند)

آیپی مقصد (اطلاعات به یک مقصد ارسال می شوند)

لایه بالایی پروتکل (هنگامی که همه پکت ها از نوع ICMP هستند)

خدمات های مختلف

فیلدهایی که باید تغییر کنند:

شناسایی (آیدی های پکت های مختلف باید متفاوت باشند)

Time To Live (TTL) با دستور traceroute هر پکت زیرشاخه افزایش می یابد)

Checksum هدر: این بخش با تغییر هدر تغییر میکند)

بخش چهارم

با توجه به طول پکت های ارسال شده مشاهده می شود که از یک تکه (fragment) تشکیل شده است.

در قسمت توضیحات اسلاید می توان متوجه شد که اگر با استفاده از نرم افزار PingPlotter طول پکت های ارسالی را افزایش دهیم، این بخش دارای تکه ها(fragment)های بیشتری می شود.

۲. TCP/UDP

بخش اول

فیلد طول UDP طول فیلدهای هدر و داده های بخش UDP است.

در بایت اندازه گیری می شود). بسته نمایش داده شده دارای طول فیلد ۵۸ بایت است. ما می دانیم که ۸ بایت هدر وجود دارد. اگر به قسمت محتوای بسته نگاه کنیم، همچنین ۵۰ بایت داده هگزادسیمال یا کدگذاری شده با ASCII را پیدا می کنیم که مربوط به بار این بخش UDP است.

The image shows a Wireshark packet capture of a UDP packet. The packet list shows a packet from 192.168.1.102 to 192.168.1.104, protocol UDP, length 108. The packet details pane shows the following structure:

- Ethernet II, Src: Realtek (08:00:27:00:00:00), Dst: Realtek (08:00:27:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
- User Datagram Protocol, Src Port: 4344, Dst Port: 161
 - Source Port: 4344
 - Destination Port: 161
 - Length: 108
 - Checksum: 0x5f1f [unverified]
 - Checksum Status: Unverified
 - Stream Index: 161
 - [Timestamps]
 - UDP payload (98 bytes)
 - Simple Network Management Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII part shows the text "108" followed by a series of null bytes.

بخش دوم

پورت آن برابر ۱۷ است و عدد هگزادسیمال آن از بخش پائین نمایش داده می شود که برابر ۱۱ در بمنای ۱۶ است.

The image shows a Wireshark packet capture analysis. The top pane displays a list of network packets. The selected packet is a GET request for a protected page, which resulted in a 404 Not Found response. The bottom pane shows the detailed view of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol (HTTP) section.

No.	Time	Source	Destination	Protocol	Length	Info
93	12.330382	192.168.1.102	192.168.1.100	SYN	60	93 Tree Disconnect Response
94	12.330770	192.168.1.100	192.168.1.102	TCP	60	3819 → 139 [FIN, ACK] Seq=1770 Ack=1338 Win=42962 Len=0
95	12.330796	192.168.1.100	192.168.1.102	TCP	60	139 → 3819 [FIN, ACK] Seq=1339 Ack=1771 Win=8958 Len=0
96	12.331815	192.168.1.100	192.168.1.102	TCP	60	3819 → 139 [ACK] Seq=1771 Ack=1340 Win=42962 Len=0
97	12.542618	128.119.245.12	192.168.1.102	TCP	60	80 → 4335 [FIN, ACK] Seq=1685 Ack=518 Win=6432 Len=0
98	12.542644	192.168.1.102	128.119.245.12	TCP	60	4335 → 80 [ACK] Seq=518 Ack=1686 Win=64240 Len=0
99	15.884828	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
100	15.882314	192.168.1.104	192.168.1.102	SNMP	92	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
101	17.856218	192.168.1.102	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1>
102	18.182656	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
103	18.119969	192.168.1.104	192.168.1.102	SNMP	92	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
104	18.495188	192.168.1.102	128.119.245.12	TCP	62	4342 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
105	18.496682	192.168.1.102	128.119.245.12	TCP	54	4335 → 80 [FIN, ACK] Seq=518 Ack=1686 Win=64240 Len=0
106	18.516388	128.119.245.12	192.168.1.102	TCP	62	80 → 4342 [SYN, ACK] Seq=0 Ack=1 Win=6400 Len=0 MSS=1460 SACK_PERM=1
107	18.516415	192.168.1.102	128.119.245.12	TCP	54	4342 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
108	18.516793	192.168.1.102	128.119.245.12	HTTP	622	GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1
109	18.516869	128.119.245.12	192.168.1.102	TCP	60	80 → 4335 [ACK] Seq=1686 Ack=519 Win=6832 Len=0
110	18.538277	128.119.245.12	192.168.1.102	TCP	60	80 → 4342 [ACK] Seq=1 Ack=569 Win=6816 Len=0
111	18.541671	128.119.245.12	192.168.1.102	HTTP	499	HTTP/1.1 200 OK (text/html)
112	18.489453	192.168.1.102	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1>
113	18.453296	192.168.1.102	128.119.245.12	TCP	54	4342 → 80 [ACK] Seq=569 Ack=446 Win=63795 Len=0
114	19.355486	192.168.1.102	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1>
115	21.120381	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
116	21.137866	192.168.1.104	192.168.1.102	SNMP	92	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

Frame 57: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0, Src: Realtek (08:00:27:00:00:00), Dst: Dell (af:36:23) (08:00:74:4f:36:23)

Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102

0800 = Version: 4

.... 0801 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 79

Identification: 0x6da7 (68839)

Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 60

Protocol: UDP (17)

Header Checksum: 0x0cdd [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.104

Destination Address: 192.168.1.102

User Datagram Protocol, Src Port: 161, Dst Port: 4140

0800 00 00 74 4f 36 23 00 30 c1 61 eb ed 00 00 45 00 ...TOS: 0 ...E

0010 00 4f ed a7 00 00 30 00 0c 00 c0 ad 01 68 c0 a0 ...O ...h

0020 01 66 00 a1 10 f4 00 30 4e ec 30 31 02 01 00 04 ...f ...N 01

0030 00 70 75 62 ec 69 63 a2 24 02 02 19 00 02 01 00 ...public: 00

0040 02 01 00 30 18 30 14 00 11 20 00 01 01 00 02 ...0 0 0 0 0 2

0050 03 09 04 02 01 02 02 02 01 00 04 01 10 ...0 0 0 1 0

بخش سوم

این مقدار برابر ترتیب پکت های ارسالی می باشد. و در اینجا برابر ۰ می باشد.

The image shows a Wireshark packet capture analysis. The main packet list displays a series of SYN packets from source 192.168.1.102 to destination 192.168.1.100. The selected packet (No. 213) is a SYN packet with sequence number 0 and window size 16384. The packet details show the TCP header with flags SYN and the IP header with source address 192.168.1.102 and destination address 192.168.1.100.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
5.125919	128.119.245.12	192.168.1.102	192.168.1.100	TCP	60	60 80 → 1161 [ACK] Seq=154117 Win=62780 Len=0
5.197286	128.119.245.12	192.168.1.102	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.197588	192.168.1.102	128.119.245.12	192.168.1.100	TCP	1514	1161 → 80 [ACK] Seq=156469 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
5.198188	192.168.1.102	128.119.245.12	192.168.1.100	TCP	1514	1161 → 80 [ACK] Seq=157929 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
5.199275	192.168.1.102	128.119.245.12	192.168.1.100	TCP	1514	1161 → 80 [ACK] Seq=158109 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
5.200252	192.168.1.102	128.119.245.12	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.201158	192.168.1.102	128.119.245.12	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.202024	192.168.1.102	128.119.245.12	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.297257	128.119.245.12	192.168.1.100	192.168.1.102	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.297341	192.168.1.102	128.119.245.12	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.389471	128.119.245.12	192.168.1.100	192.168.1.102	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.447887	128.119.245.12	192.168.1.100	192.168.1.102	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.455838	128.119.245.12	192.168.1.100	192.168.1.102	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.461175	128.119.245.12	192.168.1.100	192.168.1.102	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.500090	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.509082	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
5.651240	192.168.1.102	128.119.245.12	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
6.181044	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
6.182009	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
6.600152	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
6.640180	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
7.182852	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
7.183788	192.168.1.100	192.168.1.100	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0
7.193537	192.168.1.102	128.119.245.12	192.168.1.100	TCP	60	80 80 → 1161 [ACK] Seq=156469 Win=62780 Len=0

Packet Details:

Ethernet II, Src: Actione_Ba781a (08:20:e0:8a:78:1a), Dst: 08:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.100

TCP, Seq=0, Win=16384, Len=0

Flags: 0x002 (SYN)

Window: 16384

Checksum: 0x9c2 (unverified)

Urgent Pointer: 0

Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted

Timestamps

Raw packet data:

```
0000 00 06 25 da af 73 00 20 e0 8a 78 1a 00 00 45 00 5: s
0010 00 38 1e 4e 40 00 00 1d 4c c8 a8 01 66 c7 82 0: 8
0020 35 ce 04 8a 82 77 04 f3 82 b9 00 00 00 70 82 5: w
0030 40 00 ec 92 00 00 02 04 05 b4 01 01 04 02 0: p
```

بخش چهارم

پورت و آییی با توجه به شکل ها

آییی مبدا ۱۹۲.۱۶۸.۱.۱۰۲

پورت مبدا ۱۱۶۲ یا ۱۱۶۱

پورت مقصد ۸۰

Wireshark packet capture showing a SYN flood attack. The packet list shows multiple SYN packets from 192.168.1.100 to 192.168.1.102. The packet details show the TCP header with Seq=23293803 and the IP header with Src=192.168.1.100. The packet bytes show the raw data of the SYN packet.

Wireshark packet capture showing a SYN flood attack. The packet list shows multiple SYN packets from 192.168.1.100 to 192.168.1.102. The packet details show the TCP header with Seq=23293803 and the IP header with Src=192.168.1.100. The packet bytes show the raw data of the SYN packet.

۳. DHCP

بخش اول

آدرس آپی آن برابر 192.168.1.1 می باشد

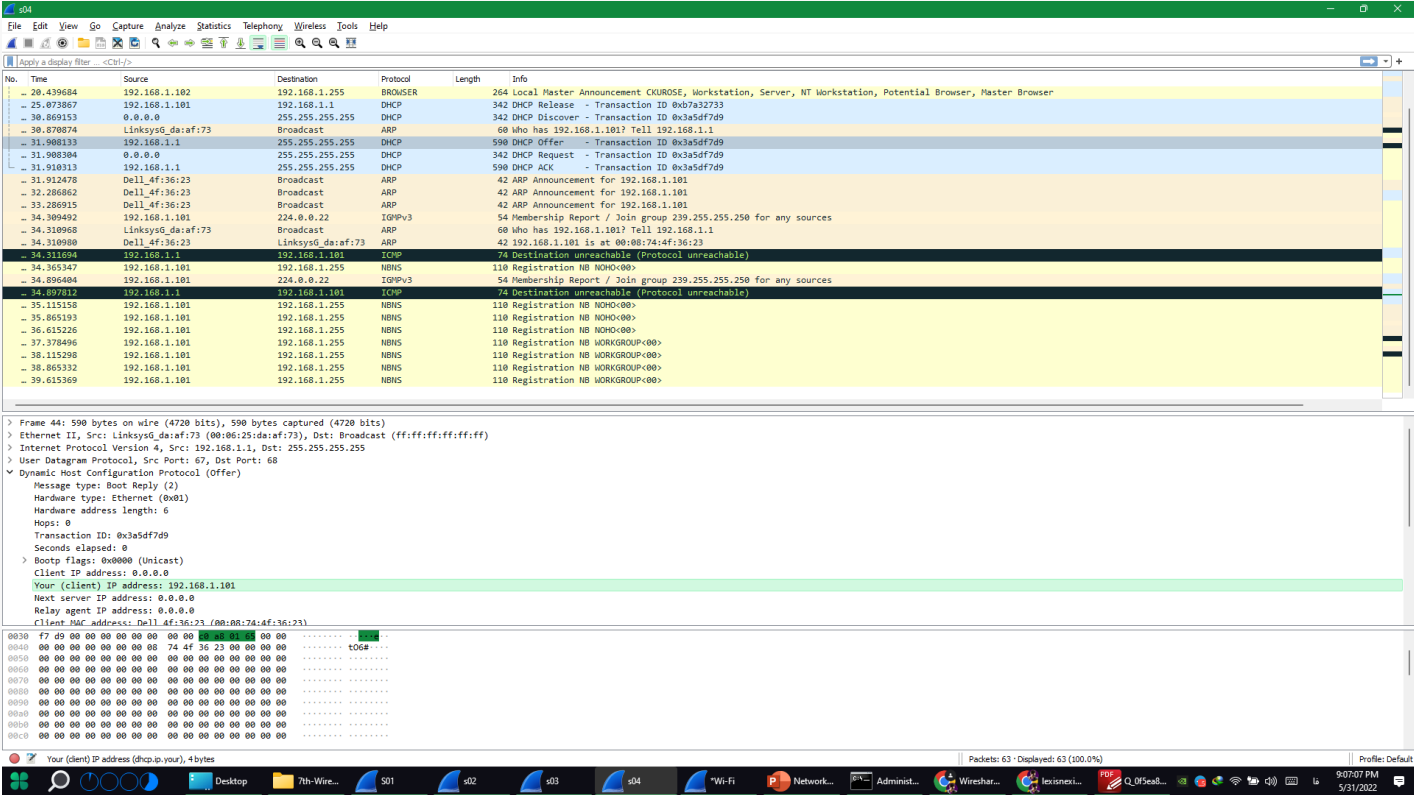
Wireshark packet capture showing DHCP traffic. The packet list shows a DHCP Offer (342) and a DHCP Request (342) from 192.168.1.1 to 192.168.1.1. The packet details show the DHCP Offer message with fields like Transaction ID, Offered IP Address, and Lease Time. The packet bytes show the raw data of the DHCP message.

Packet 342: DHCP Offer (Transaction ID: 0x3a5df7d9) from 192.168.1.1 to 192.168.1.1. The packet details show the DHCP Offer message with fields like Transaction ID, Offered IP Address, and Lease Time.

Packet 342: DHCP Request (Transaction ID: 0x3a5df7d9) from 192.168.1.1 to 192.168.1.1. The packet details show the DHCP Request message with fields like Transaction ID, Requested IP Address, and Lease Time.

بخش دوم

آدرس آپی پیشنهادی آن برابر ۱۹۲.۱۶۸.۱.۱۰۱ است.



بخش سوم

خط روتر نشان دهنده Default Getway است و خط ماسک زیر شبکه را به کلاینت اطلاع رسانی می کند.

این مدت زمانی که که سرور DHCP یک آیپی را به یک کلاینت اختصاص می دهد، در طول این مدت زمان سرور نباید این آیپی را به کس دیگری اختصاص دهد مگر آنکه زمان اجاره آن منقضی شده باشد.
(در این قسمت این مقدار برابر یک روز می باشد)

[illegible]

۴. بخش اول DNS

```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>nslookup Amazon.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 192.168.243.245

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name: Amazon.com
Addresses: 205.251.242.103
          54.239.28.85
          176.32.103.205

C:\Windows\system32>
```

بخش دوم

با استفاده از پروتکل های DNS و مشاهده بخش User Datagram Protocol (UDP) می توان این نتیجه را گرفت که بر پایه UDP است.

The image displays a Wireshark packet capture and a Windows command prompt. The Wireshark interface shows a list of network packets, with the selected packet (No. 11) being a User Datagram Protocol (UDP) packet. The packet details pane shows the following information:

- Frame 11: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface \Device\NPF_{5F40C480-567E-4EBC-87B1-D232E8111C}
- Ethernet II, Src: b2:33:ed:90:ac:a5 (b2:33:ed:90:ac:a5), Dst: IntelCor_61:8f:b9 (34:cf:f6:61:8f:b9)
- Internet Protocol Version 4, Src: 192.168.243.245, Dst: 192.168.243.162
- User Datagram Protocol, Src Port: 53, Dst Port: 65289
 - Source Port: 53
 - Destination Port: 65289
 - Length: 103
 - Checksum: 0x0b93 [unverified]
 - Checksum Status: Unverified
 - [Stream index: 0]
 - [Timestamps]
 - UDP payload (95 bytes)
 - Domain Name System (response)

The packet bytes pane shows the raw data of the UDP payload, which is a DNS response. The Windows command prompt shows the execution of the command `C:\Windows\system32>nslookup Amazon.com`, which returns the following output:

```
C:\Windows\system32>nslookup Amazon.com
DNS request timed out.
    timeout was 2 seconds.
Server: Unknown
Address: 192.168.243.245

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:   Amazon.com
Addresses: 205.251.242.103
          54.239.28.85
          176.32.103.205

C:\Windows\system32>nslookup Amazon.com
Server: Unknown
Address: 192.168.243.245

Non-authoritative answer:
Name:   amazon.com
Addresses: 205.251.242.103
          176.32.103.205
          54.239.28.85

C:\Windows\system32>
```


بخش سوم

برخی پکت های ارسال شده خیر این بخش هیچ پاسخی ندارد(اسکرین شات سمت چپ) و برخی چندین پاسخ دارند (اسکرین شات سمت راست).

(طبق پاسخ حل المسائل)

The screenshot shows a Wireshark packet capture of a DNS transaction. The packet list on the left shows a query (No. 1) and a response (No. 2). The packet details pane for packet 2 shows the following structure:

- Frame 2: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0\{DeviceNPF...}
- Ethernet II, Src: 62-77-40-00-00-00, Dst: 02-00-00-00-00-00
- Internet Protocol Version 4, Src: 192.168.243.100, Dst: 192.168.243.102
- User Datagram Protocol, Src Port: 53, Dst Port: 5353
- Domain Name System (query response)
- Transaction ID: 0x0000
- Flags: 0x0000 Standard query response, no error
- Answer: 1
 - Question: 1
 - Answer: 1
 - Authority: 0x00
 - Additional: 0x00
- Queries
- Authoritative answers only
- Response: 1 (0.000000 seconds)

The packet bytes pane shows the raw data of the response packet.

The screenshot shows a Wireshark packet capture of a DNS transaction. The packet list on the left shows a query (No. 1) and a response (No. 2). The packet details pane for packet 2 shows the following structure:

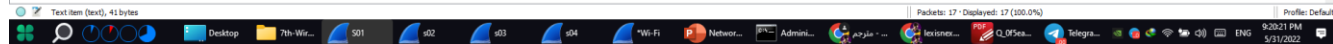
- Frame 2: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0\{DeviceNPF...}
- Ethernet II, Src: 62-77-40-00-00-00, Dst: 02-00-00-00-00-00
- Internet Protocol Version 4, Src: 192.168.243.100, Dst: 192.168.243.102
- User Datagram Protocol, Src Port: 53, Dst Port: 5353
- Domain Name System (query response)
- Transaction ID: 0x0000
- Flags: 0x0000 Standard query response, no error
- Question: 1
- Answer: 0
- Authority: 0x00
- Additional: 0x00
- Queries
- Authoritative answers only
- Response: 1 (0.000000 seconds)

The packet bytes pane shows the raw data of the response packet.

بخش چهارم

خیر اگر سایتی شامل چند عکس باشد هربار در هنگام لود سایت پیش از دریافت عکس ها dns query انجام نمی شود.

ورژن HTTP برابر ۱.۱ است.



بخش دوم

پروتکل معلوم بررسی میکند که آیا از تاریخی که شئی ذخیره شده در سرور تغییری کرده است یا خیر، اگر این فایل تغییری کرده باشد، سرور شئی را دوباره ارسال میکند، در غیر اینصورت پیغام ۳۰۴ not modified را ارسال میکند تا سرور کش از فایل درون دیتابیس خود استفاده کند.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and filtering.

The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. Packet 439 is selected, which is an HTTP GET request to /1.200 OK.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol (HTTP) request. The status line is 'HTTP/1.1 200 OK'. Headers include 'Server: Apache/2.0.40 (Red Hat Linux)', 'Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT', 'ETag: "libfed-49-79d5bf00"', 'Accept-Ranges: bytes', 'Content-Length: 73', 'Keep-Alive: timeout=10, max=100', and 'Connection: Keep-Alive'. The body content is 'libfed-49-79d5bf00'.
- Packet Bytes:** Displays the raw data of the packet in hexadecimal and ASCII. The ASCII column shows the text representation of the data, including the status line and headers.

The status bar at the bottom indicates that the last packet is selected, and the display filter is 'HTTP Last Modified (http.last_modified), 46 bytes'.

بخش سوم

با شمارش بخش ها، دارای دو درخواست **Get** است و آدرس آبیی سرور مقصد آن ۱۲۸.۱۱۹.۲۴۵.۱۲ می باشد.

Wireshark packet capture showing network traffic. The selected packet is an HTTP GET request for /favicon.ico.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	0.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	0.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A galia.cs.umass.edu
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x044d A galia.cs.umass.edu A 128.119.245.12 NS unix1.cs.umass.edu NS nic.umass.edu NS ns1.umass.edu NS ns4.cw.net NS kira.ecc.umass.edu A 128.119.40.12
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724532	192.168.1.102	128.119.245.12	HTTP	54	GET /favicon.ico HTTP/1.1
14	4.760366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.834987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.852471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

بخش چهارم

بخش OK داده شده پروتکل HTTP دارای طول ۷۳ بایت است

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP		92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP		93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	0.017086	192.168.1.102	192.168.1.104	SNMP		92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	0.034572	192.168.1.104	192.168.1.102	SNMP		93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS		77 Standard query 0x044d A gaia.cs.umass.edu
6	4.663785	63.240.76.19	192.168.1.102	DNS		293 Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 HS unix1.cs.umass.edu HS nic.umass.edu HS nsl.umass.edu HS ns4.cw.net HS kira.ecc.umass.edu A 128.119.40.12
7	4.675312	192.168.1.102	128.119.245.12	TCP		62 4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP		62 80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	4.694458	192.168.1.102	128.119.245.12	TCP		54 4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
+	4.694598	192.168.1.102	128.119.245.12	HTTP		555 GET /etherlab-labs/lab2-1.html HTTP/1.1
+	4.717389	128.119.245.12	192.168.1.102	TCP		60 80 → 4127 [ACK] Seq=1 Ack=592 Win=6432 Len=0
+	4.718993	128.119.245.12	192.168.1.102	HTTP		439 HTTP/1.1 200 OK (text/html)
+	4.724332	192.168.1.102	128.119.245.12	HTTP		541 GET /favicon.ico HTTP/1.1
+	4.750366	128.119.245.12	192.168.1.102	HTTP		1395 HTTP/1.1 404 Not Found (text/html)
+	4.859777	192.168.1.102	128.119.245.12	TCP		54 4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
6	0.034572	192.168.1.102	192.168.1.104	SNMP		92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
+	0.052471	192.168.1.104	192.168.1.102	SNMP		93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

```

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
Etag: "1bfed-49-79d5bf00"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 73\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.024143000 seconds]
[Request in frame: 10]
[Next request in frame: 13]
[Next response in frame: 14]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 73 bytes
> Line-based text data: text/html (3 lines)

0120 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 65 63 74 69 6f x=100--C connectio
0130 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 n: Keep-Alive--C
0140 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 content-Type: tex
0150 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d t/html; charset=
0160 49 53 4f 2d 38 38 35 39 3d 2d 31 0d 0a 0d 0a ISO-8859-1...
0170 69 6c 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 101-100 gratulatio
0180 6f 6e 73 6e 20 55 6f 75 27 76 65 20 64 6f 6fow. You've de
0190 77 6e uc of 61 04 05 04 20 74 68 65 20 66 69 86 unloaded the fil
01a0 65 20 uc 61 62 32 2d 68 20 68 68 66 6c 21 0d 0a 101-100.html)
01b0 6f 6e 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d t/html;

```