

گزارش کار دوم آزمایشگاه شبکه

سوال اول)

سایت های جست و جو شده: Gmail، GitHub، Twitter، Reddit، YouTube

لیست پروتکل های مشاهده شده:

TCP, TLSv1.2, TLSv1.3, HTTP, TLS, HTTPS, DNS

35554	95.293383	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35555	95.293412	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263816] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17094881 SLE=17074481 SRE=17074481
35556	95.298094	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35557	95.298107	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263817] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17096241 SLE=17074481 SRE=17074481
35558	95.304235	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35559	95.304274	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263818] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17097601 SLE=17074481 SRE=17074481
35560	95.309602	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35561	95.309639	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263819] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17098961 SLE=17074481 SRE=17074481
35562	95.315166	142.132.225.80	192.168.1.8	TLSv1.3	1414 Continuation Data
35563	95.320420	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35564	95.320477	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263820] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17100321 SLE=17074481 SRE=17074481
35565	95.326064	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35566	95.326903	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263821] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17101681 SLE=17074481 SRE=17074481
35567	95.331594	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35568	95.331633	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263822] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17103041 SLE=17074481 SRE=17074481
35569	95.336619	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35570	95.336619	84.17.47.126	192.168.1.8	TCP	54 9002 → 65175 [ACK] Seq=681771 Ack=38432 Win=64128 Len=0
35571	95.336674	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263823] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17104401 SLE=17074481 SRE=17074481
35572	95.343086	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35573	95.343153	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263824] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17105761 SLE=17074481 SRE=17074481
35574	95.349124	84.17.47.126	192.168.1.8	TLSv1.2	1414 Ignored Unknown Record
35575	95.349165	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263825] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17107121 SLE=17074481 SRE=17074481
> Frame 35565: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-91056B1A8FBD}, id 0					
> Ethernet II, Src: ProwareT_80:20:3c (6c:fd:b9:80:20:3c), Dst: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85)					
> Internet Protocol Version 4, Src: 84.17.47.126, Dst: 192.168.1.8					
> Transmission Control Protocol, Src Port: 9002, Dst Port: 64970, Seq: 3393, Ack: 1700321, Len: 1360					
> Transport Layer Security					
0000	e6 0a bd cf d5 85 6c fd b9 80 20 3c 08 00 45	1E		
0010	05 78 6e 40 40 00 36 06 8c 00 54 11 2f 7e c0 a8	2T		
0020	01 08 23 2a fd ca 08 a7 14 52 4a 13 a7 58 50 18	3XP		
0030	01 f5 5e 00 00 00 46 5f ac bb 91 94 3d 10 73 9c	4S		
0040	8a 01 29 5e 78 c4 68 b8 24 e4 a9 60 e3 fd ac d1	5h		
0050	0a 11 14 74 fa 91 28 f4 be ad 39 28 53 24 b3 cd	69S		
0060	73 67 82 3f 01 68 70 64 e6 a7 cf 1b f3 37 41 96	77A		
0070	fa d1 95 fb 1b a5 c8 0b 85 ed 60 2a d9 cd 98 e9	8		
0080	1f fa 14 30 ee 77 17 59 7b ea b6 67 a8 ec ec 10	9g		
0090	56 fc 83 f8 5a b3 a3 e5 c7 bb 0b 55 c7 48 60 75	10U		

سوال دوم)

در package انتخابی، دو پروتکل استفاده شده: Transmission Control Protocol و Internet Protocol Version 4. لایه Transmission Control Protocol بعد از Internet Protocol Version 4 و آن هم بعد از Ethernet II و آن هم بعد از Frame آمده است. به عبارتی ترتیب قرارگیری به خارجی ترین است.

اندازه Frame لایه دو این بسته برابر ۹۰ بایت است. جزئیات این package را مشاهده میکنید:

35561	95.309639	192.168.1.8	84.17.47.126	TCP	90 [TCP Dup ACK 35263819] 64970 → 9002 [ACK] Seq=3393 Ack=17048641 Win=2082 Len=0 SLE=17082641 SRE=17098961 SLE=17074481 SRE=17074481
35562	95.315166	142.132.225.80	192.168.1.8	TLSv1.3	1414 Continuation Data
> Frame 35561: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-91056B1A8FBD}, id 0					
> Ethernet II, Src: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85), Dst: ProwareT_80:20:3c (6c:fd:b9:80:20:3c)					
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 84.17.47.126					
> Transmission Control Protocol, Src Port: 64970, Dst Port: 9002, Seq: 3393, Ack: 17048641, Len: 0					
0000	6c fd b9 80 20 3c e6 0a bd cf d5 85 00 00 45 00	1E		
0010	00 4c 0e 21 40 00 00 06 27 4b c0 a8 01 00 54 11	2T		
0020	2f 7e fd ca 23 2a 4a 13 a7 58 08 a6 4a 72 e0 10	3X		
0030	08 22 7b ec 00 00 01 01 05 22 08 a6 cf 42 08 a7	4B		
0040	0f 02 08 a6 af 62 08 a6 ba 02 08 a6 8f 82 08 a6	5		
0050	94 d2 08 a6 9a 22 08 a6 9f 72	6r		

گزارش کار دوم آزمایشگاه شبکه

سوال سوم)

بله. همانطور که در عکس پایین مشاهده میشود Package های ARP دارای لایه های Network، Application و Transport نیستند. پروتکل استفاده شده در این package ها برای Data Link هستند:

No.	Time	Source	Destination	Protocol	Length	Info
14430	40.497072	Arcadyan_43:bc:5b	e6:0a:bd:cf:d5:85	ARP	42	Who has 192.168.1.8? Tell 192.168.1.2
14431	40.497086	e6:0a:bd:cf:d5:85	Arcadyan_43:bc:5b	ARP	42	192.168.1.8 is at e6:0a:bd:cf:d5:85
6395	17.286333	192.168.1.8	192.168.1.1	DNS	75	Standard query 0x53fd A armmf.adobe.com
6498	17.606182	192.168.1.8	192.168.1.1	DNS	75	Standard query 0x53fd A armmf.adobe.com
6531	17.695533	192.168.1.1	192.168.1.8	DNS	203	Standard query response 0x53fd A armmf.adobe.com CNAME ssl.adobe.com.edgeke

> Frame 14430: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-91056B1A8FBD}, id 0
> Ethernet II, Src: Arcadyan_43:bc:5b (1c:c6:3c:43:bc:5b), Dst: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85)
> Address Resolution Protocol (request)

سوال چهارم)

در برنامه Wireshark یک package انتخاب شده و سپس مشخصات لایه 4 Internet Protocol Version باز شد. همانطور که مشاهده میشود Header Checksum برابر 0x5f28 است. در شکل زیر درستی این حرف اثبات میشود:

> Frame 122: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-91056B1A8FBD}, id 0
> Ethernet II, Src: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85), Dst: ProwareT_80:20:3c (6c:fd:b9:80:20:3c)
v Internet Protocol Version 4, Src: 192.168.1.8, Dst: 84.17.47.126
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x565c (22108)
 > Flags: 0x40, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: TCP (6)
 Header Checksum: 0x5f28 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.8
 Destination Address: 84.17.47.126
 > Transmission Control Protocol, Src Port: 64970, Dst Port: 9002, Seq: 65, Ack: 80671, Len: 0

سوال پنجم)

پورت ها برای انتقال دیتا حیاتی هستند. دو پورت Source برابر 64970 و Destination برابر 9002 است. بین این پورت ها میتوان دیتا فرستاد یا دریافت کرد. Checksum پروتکل TCP برابر 0xfebe و پروتکل UDP برابر 0x35c5 است.

128	0.350548	192.168.1.8	84.17.47.126	TCP	54	64970 → 9002 [ACK] Seq=65 Ack=86111 Win=2082 Len=0
129	0.350551	84.17.47.126	192.168.1.8	TCP	60	9002 → 64970 [ACK] Seq=80671 Ack=65 Win=2082 Len=0

v Transmission Control Protocol, Src Port: 64970, Dst Port: 9002, Seq: 65, Ack: 77951, Len: 0
 Source Port: 64970
 Destination Port: 9002
 [Stream index: 0]
 [Conversation completeness: Incomplete (12)]
 [TCP Segment Len: 0]
 Sequence Number: 65 (relative sequence number)
 Sequence Number (raw): 1242798680
 [Next Sequence Number: 65 (relative sequence number)]
 Acknowledgment Number: 77951 (relative ack number)
 Acknowledgment number (raw): 128145072
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
 Window: 2082
 [Calculated window size: 2082]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0xfebe [unverified]
 [Checksum Status: Unverified]

گزارش کار دوم آزمایشگاه شبکه

سوال ششم)

پروتکل لایه Transport برابر UDP بوده و پورت مقصد برابر 192.168.1.8 است. لایه دوم Ethernet II است که آدرس مبدا c:fd:b9:80:20:3c و آدرس مقصد e6:0a:bd:cf:d5:85 است.

22	83.327956	192.168.1.1	192.168.1.8	DNS	318	Standard query response 0xef81 A is3-ssl.mzstatic.com CNAME is-ssl.mzstatic.com.itunes-apple.com.akadns.net CNAME mzstatic.com.ed...
23	83.362850	192.168.1.1	192.168.1.8	DNS	297	Standard query response 0x2ba2 A is2-ssl.mzstatic.com CNAME is-ssl.mzstatic.com.itunes-apple.com.akadns.net CNAME mzstatic.com.ed...
24	83.415507	192.168.1.1	192.168.1.8	DNS	297	Standard query response 0xb6cd A is1-ssl.mzstatic.com CNAME is-ssl.mzstatic.com.itunes-apple.com.akadns.net CNAME mzstatic.com.ed...
25	108.741939	192.168.1.1	192.168.1.8	DNS	79	Standard query 0xda72 A play.googleapis.com
26	108.826924	192.168.1.1	192.168.1.8	DNS	95	Standard query response 0xda72 A play.googleapis.com A 172.217.18.138
27	142.757007	192.168.1.1	192.168.1.1	DNS	89	Standard query 0x99d4 A v10.events.data.microsoft.com
28	142.886514	192.168.1.1	192.168.1.1	DNS	89	Standard query 0x99d4 A v10.events.data.microsoft.com
29	143.900236	192.168.1.1	192.168.1.1	DNS	89	Standard query 0x99d4 A v10.events.data.microsoft.com
30	144.020036	192.168.1.1	192.168.1.8	DNS	291	Standard query response 0x99d4 A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedscolp...
31	181.183482	192.168.1.1	192.168.1.1	DNS	77	Standard query 0x852d A k-ring.msedge.net
32	181.270351	192.168.1.1	192.168.1.8	DNS	170	Standard query response 0x852d A k-ring.msedge.net CNAME k-ring.k-9999.k-msedge.net CNAME k-9999.k-msedge.net A 13.107.18.254
33	184.285444	192.168.1.1	192.168.1.1	DNS	87	Standard query 0xd32e A roaming.officeapps.live.com
34	184.371847	192.168.1.1	192.168.1.8	DNS	205	Standard query response 0xd32e A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net CNAME eur.roaming1.live.com...

```
> Frame 2: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{008FD591-4480-43CE-81BA-91056B1A8FBD}, id 0
  Ethernet II, Src: ProwareT_80:20:3c (6c:fd:b9:80:20:3c), Dst: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85)
    Destination: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85)
    Source: ProwareT_80:20:3c (6c:fd:b9:80:20:3c)
    Type: IPv4 (0x0000)
  Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.8
    User Datagram Protocol, Src Port: 53, Dst Port: 64047
      Source Port: 53
      Destination Port: 64047
      Length: 131
      Checksum: 0xe855 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
      [Timestamps]
      UDP payload (123 bytes)
    > Domain Name System (response)
```

```
Microsoft Windows [Version 10.0.22000.556]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Keivan>ping google.com

Pinging google.com [142.250.180.46] with 32 bytes of data:
Reply from 142.250.180.46: bytes=32 time=122ms TTL=111
Reply from 142.250.180.46: bytes=32 time=118ms TTL=111
Reply from 142.250.180.46: bytes=32 time=117ms TTL=111
Reply from 142.250.180.46: bytes=32 time=118ms TTL=111

Ping statistics for 142.250.180.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 117ms, Maximum = 122ms, Average = 118ms

C:\Users\Keivan>nslookup 1.1.1.1
Server:      Unknown
Address:     192.168.1.1

Name:       one.one.one.one
Address:    1.1.1.1
```

سوال هفتم)

از آن جایی که interface انتخابی WIFI بوده، آدرس آن را در ipconfig/all مشاهده میکنیم.

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : domain.name
Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
Physical Address. . . . . : E6-0A-BD-CF-D5-85
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::641c:74d1:67d:33c9%2(Preferred)
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, April 11, 2022 11:20:15 PM
Lease Expires . . . . . : Wednesday, April 13, 2022 7:26:02 AM
Default Gateway . . . . . : fe80::6efd:b9ff:fe80:203c%2
```

همانطور که مشاهده میشود Physical Address چاپ شده با سوال ششم همخوانی دارد.

گزارش کار دوم آزمایشگاه شبکه

سوال هشتم)

در لایه Query و بخش Query تایپ PTR انتخاب شده. این تایپ برای تبدیل یک IP Address به Host Name استفاده میشود. (برعکس این تایپ یعنی تایپ A، عکس این عملیات را انجام میدهد.)

11	17.041925	192.168.1.8	192.168.1.1	DNS	80 Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
12	17.127939	192.168.1.1	192.168.1.8	DNS	109 Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one
13	17.471509	192.168.1.1	192.168.1.1	DNS	87 Standard query 0x3187 A roaming.officeapps.live.com
14	17.555109	192.168.1.1	192.168.1.8	DNS	205 Standard query response 0x3187 A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net CNAME eur.roaming1.live.com...
15	17.214460	192.168.1.8	192.168.1.1	DNS	94 Standard query 0xb12c A tile-service.weather.microsoft.com
16	17.302508	192.168.1.1	192.168.1.8	DNS	273 Standard query response 0xb12c A tile-service.weather.microsoft.com CNAME wildcard.weather.microsoft.com.edgekey.net CNAME e15275...
17	17.205585	192.168.1.8	192.168.1.1	DNS	87 Standard query 0xc172 A safebrowsing.googleapis.com
18	17.309638	192.168.1.1	192.168.1.8	DNS	103 Standard query response 0xc172 A safebrowsing.googleapis.com A 172.217.18.138

> Frame 11: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-9105681A8FBD}, id 0
> Ethernet II, Src: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85), Dst: ProwareT_80:20:3c (6c:fd:b9:80:20:3c)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 54186, Dst Port: 53
v Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
> 1.1.1.1.in-addr.arpa: type PTR, class IN
[Response In: 12]

در عکس، سطر تایپ انتخاب شده.

سوال نهم)

برای دستور nslookup تایپ A استفاده شده است. این تایپ برای تبدیل یک Host Name به IP Address استفاده میشود. (برعکس سوال قبل، PTR)

18	17.309638	192.168.1.1	192.168.1.8	DNS	103 Standard query response 0xc172 A safebrowsing.googleapis.com A 172.217.18.138
----	-----------	-------------	-------------	-----	---

> Frame 18: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-9105681A8FBD}, id 0
> Ethernet II, Src: ProwareT_80:20:3c (6c:fd:b9:80:20:3c), Dst: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.8
> User Datagram Protocol, Src Port: 53, Dst Port: 49938
v Domain Name System (response)
Transaction ID: 0xc172
> Flags: 0x8100 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
v Queries
> safebrowsing.googleapis.com: type A, class IN
> Answers
[Request In: 17]
[Time: 0.104053000 seconds]

سوال دهم)

سه نوع کوثری دیگر:

- کوثری تایپ MD مربوط به Mail Destination
- کوثری تایپ TXT مربوط به Text Strings
- کوثری تایپ HINFO مربوط به Host Information

سوال یازدهم)

در صورت انتخاب این فیلتر فقط package هایی که IP مقصد یا مبدا آنها برابر IP که دادیم بود نمایش داده میشوند. از طرفی تمام پروتکل های مشاهده شده برابر ICMP میشود. همانطور که در شکل مشاهده میشود فیلتر اعمال شده:

گزارش کار دوم آزمایشگاه شبکه

No.	Time	Source	Destination	Protocol	Length	Info
5640	74.011352	192.168.1.8	192.168.1.8	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
5641	74.013583	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=6 (no response found!)
5644	74.098122	10.22.26.114	192.168.1.8	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
5645	74.099909	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=6 (no response found!)
5646	74.102511	10.22.26.114	192.168.1.8	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
5760	79.730564	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=7 (no response found!)
5763	79.821948	10.202.1.5	192.168.1.8	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
5764	79.823875	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=7 (no response found!)
5765	79.907009	10.202.1.5	192.168.1.8	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
5766	79.908959	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=7 (no response found!)
5767	79.921252	10.202.1.5	192.168.1.8	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
5876	85.714905	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=8 (no response found!)
6045	89.330582	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=8 (no response found!)
6160	93.338731	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=8 (no response found!)
6243	97.342121	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=9 (reply in 6244)
6244	97.425827	5.144.130.115	192.168.1.8	ICMP	106	Echo (ping) reply id=0x0001, seq=35/8960, ttl=9 (request in 6243)
6245	97.427812	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=9 (reply in 6246)
6246	97.510892	5.144.130.115	192.168.1.8	ICMP	106	Echo (ping) reply id=0x0001, seq=36/9216, ttl=9 (request in 6245)
6247	97.513849	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=9 (reply in 6248)
6248	97.597445	5.144.130.115	192.168.1.8	ICMP	106	Echo (ping) reply id=0x0001, seq=37/9472, ttl=9 (request in 6247)

از آنجایی که IP Address سایت p30download.com برابر ۵.۱۴۴.۱۳۰.۱۱۵ است، فیلتر اعمال شده:

ip.addr == 5.144.130.115

سوال دوازدهم)

در قسمت Internet Control Message Protocol، تایپ برابر Echo (ping) Request است. از طرفی TTL یا Time To

Live برابر ۹ بوده است. در شکل مشاهده میشود:

> Frame 6243: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{000FD591-4480-43CE-81BA-91056B1A8FB0}, id 0
> Ethernet II, Src: e5:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85), Dst: ProwareT_80:20:3c (6c:fd:b9:80:20:3c)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 5.144.130.115
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0xf463 (62563)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 9
Protocol: ICMP (1)
Header Checksum: 0x738a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.8
Destination Address: 5.144.130.115
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7db [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 35 (0x0023)
Sequence Number (LE): 8960 (0x2300)
[Response frame: 6244]
> Data (64 bytes)

سوال سیزدهم)

بله، مقادیر در حال تغییر هستند زیرا در صورت بروز هر خطایی در دریافت/ارسال بسته ها TTL یا Time To Live از گیر کردن در حلقه بینهایت جلوگیری میکند.

سوال چهاردهم)

این فیلتر را تایید میکند. [Wikipedia](#) سایت این مشاهده را تایید میکند.