

لایه بندی پروتکل ها

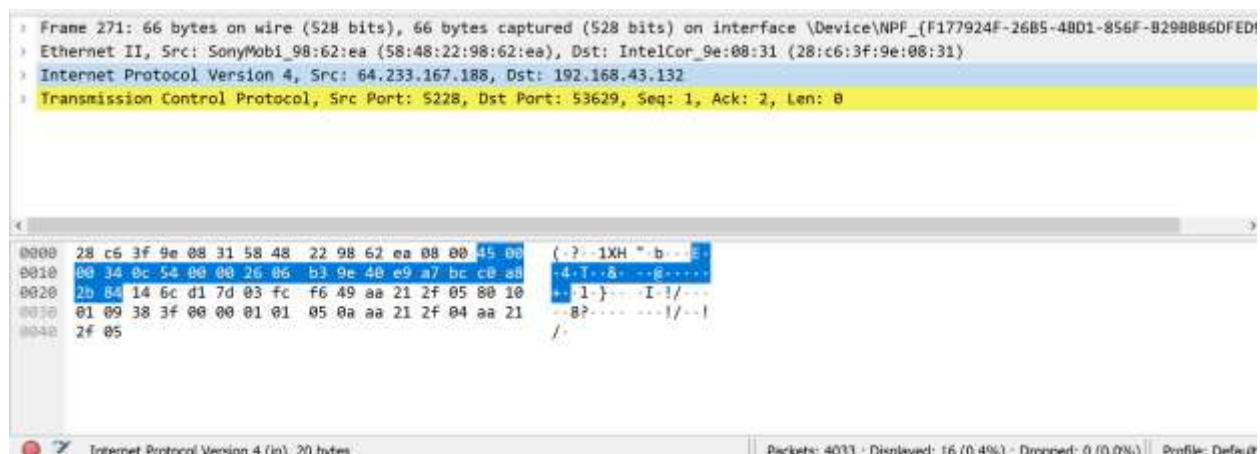
۱. به یک بخش دلخواه از بسته های شنود شده مراجعه کنید. چه پروتکل هایی را مشاهده می کنید؟ لیست آنها را یادداشت کنید.

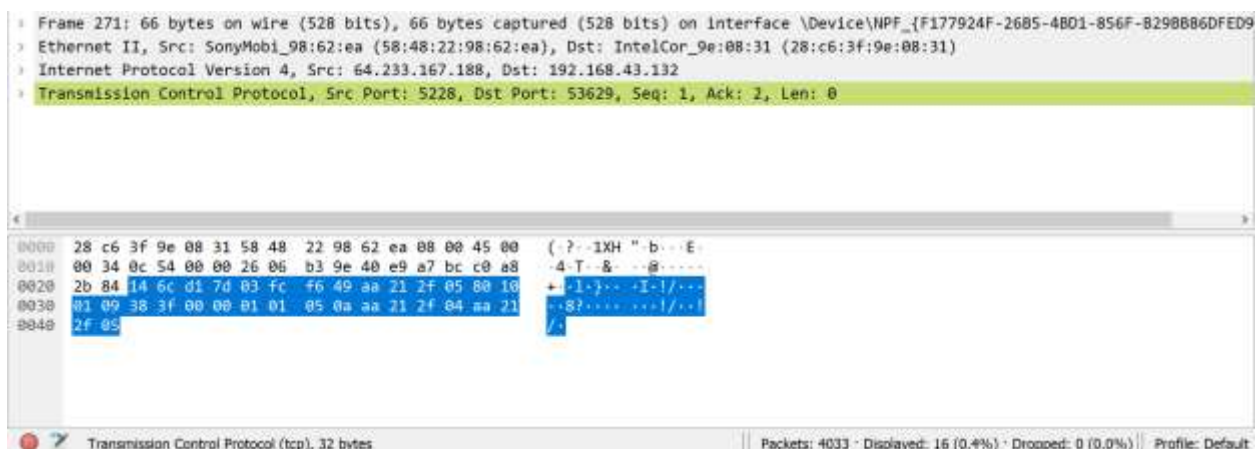
پروتکل هایی همانند TCP, TLSv1, TLSv1.2, TLSv1.3, SSL, QUIC, ARP, DNS

۲. یک بسته را به دلخواه انتخاب کنید. مشخص کنید که چه پروتکل هایی در لایه های مختلف آن استفاده شده است. ترتیب قرارگیری بیت های داخل بسته چه ارتباطی با لایه های مختلف دارد؟ اندازه ی فریم لایه ی دو این بسته چقدر است؟ اندازه بسته لایه سه چقدر است؟

یک بسته ی با پروتکل TCP انتخاب می شود.

بسته ی انتخاب شده دارای سه لایه ی Data link Layer, Network Layer و Transport Layer است. بیت های بسته به ترتیب گفته شده در بالا از زیری ترین لایه به بالا اطلاعات مربوط به هر لایه را مشخص می کند (به ترتیب : اول لایه ی لینک، دوم لایه ی نتورک و در نهایت لایه ی Transport). لایه ی دوم همان لایه ی Network است. اندازه ی این لایه طبق پیام ارسال شده، برابر با 20 بایت است (از بایت 14 تا 33). اندازه ی بسته ی لایه ی سوم برابر با 32 بایت است (از بایت 34 تا 65).





۳. آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Application, Transport, Network باشند؟ این بسته‌ها از چه پروتوکلی استفاده کرده‌اند؟

بسته‌ی مربوط به پروتکل ARP فاقد لایه‌های Network, Transport و Application است. این پروتکل برای یافتن آدرس لایه‌ی لینک (همانند Mac address) استفاده می‌شود.

No.	Time	Source	Destination	Protocol	Length	Info
3988	115.798881	192.46.236.154	192.168.43.132	UDP	155	22 → 64689 Len=113
3989	115.798881	192.46.236.154	192.168.43.132	UDP	251	22 → 64689 Len=209
3990	115.798881	192.46.236.154	192.168.43.132	UDP	74	22 → 64689 Len=32
3991	115.798881	192.46.236.154	192.168.43.132	UDP	187	22 → 64689 Len=65
3992	115.798881	SonyMobi_98:62:ea	IntelCor_9e:08:31	ARP	42	Who has 192.168.43.132? Tell 192.168.43.1
3993	115.798881	64.233.167.188	192.168.43.132	TCP	66	[TCP Keep-Alive ACK] 5228 → 53629 [ACK] Seq=27 Ac
3994	115.798881	192.46.236.154	192.168.43.132	UDP	74	22 → 64689 Len=32

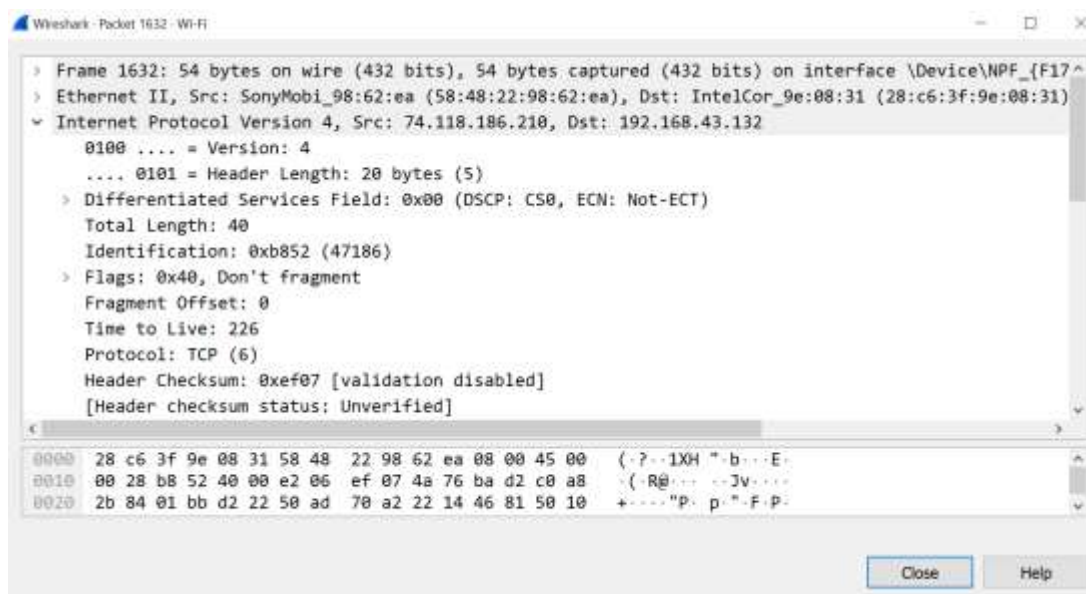
Frame 3992: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F177924F-26B5-4B01-856F-8298B86DFED9}

Ethernet II, Src: SonyMobi_98:62:ea (58:48:22:98:62:ea), Dst: IntelCor_9e:08:31 (28:c6:3f:9e:08:31)

Address Resolution Protocol (request)

۴. از یکی از بسته‌ها، بخش مربوط به پروتوکول (IP) Internet Protocol را پیدا کنید. Checksum پروتکل IP را پیدا کنید و آن را یادداشت کنید.

مقدار Checksum هدر پروتکل IP یکی از بسته‌ها برابر با 0xef07 است.



۵. از یکی از بسته‌ها بخش مربوط به پروتکل TCP یا UDP را پیدا کنید. عدد مربوط به پورت مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص می‌کند؟ Checksum مربوط به پروتکل‌های TCP و UDP را مشخص کنید.

پروتکل بسته‌ی مورد بحث UDP است. عدد پورت مبدا 64689 و عدد پورت مقصد 22 است. مقدار پورت در شبکه‌های کامپیوتری، نوع سرویس را نشان می‌دهند. برای مثال پورت 53 و پورت 80 به ترتیب برای سرویس‌های مربوط به DNS و HTTP مورد استفاده قرار می‌گیرند. مقدار Checksum مربوط به یکی از بسته‌های دارای پروتکل UDP برابر با 0xcbc5 و یکی از بسته‌های دارای پروتکل TCP برابر با 0xc53e است.

کار با فیلترکننده بسته

۶. یکی از بسته‌ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه‌ی Transport چیست؟ آدرس IP مقصد چیست؟ سرآیند لایه‌ی دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

پروتکل استفاده‌شده در لایه‌ی Transport، User Datagram Protocol (UDP) است. آدرس مقصد برابر با 192.168.43.1 است. (از هات‌اسپات برای اتصال به شبکه استفاده شده است.)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.132	192.168.43.1	DNS	74	Standard query 0xe939 A dns.google.com
2	0.003316	192.168.43.1	192.168.43.132	DNS	106	Standard query response 0xe939 A dns.google.com A
3	0.798404	192.168.43.132	192.168.43.1	DNS	73	Standard query 0xa02e A www.google.ru
4	0.802840	192.168.43.1	192.168.43.132	DNS	89	Standard query response 0xa02e A www.google.ru A
5	4.416392	192.168.43.132	192.168.43.1	DNS	86	Standard query 0xbf8d A mozilla.cloudflare-dns.co

Internet Protocol Version 4, Src: 192.168.43.132, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 62072, Dst Port: 53
Source Port: 62072
Destination Port: 53
Length: 39
Checksum: 0x6243 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Time Range: 1]

۷. کدام یک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستور `ipconfig /all` مشاهده کنید.

هر دوی مبدا و مقصد را می‌توان در خروجی مشاهده کرد.

آدرس مقصد به عنوان DNS Servers و آدرس مبدا به عنوان IPv4 Address آمده‌اند.

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
Physical Address. . . . . : 28-C6-3F-9E-08-31
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::940b:b4b5:d373:94f8%17(Preferred)
IPv4 Address. . . . . : 192.168.43.132(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, April 5, 2021 1:15:01 AM
Lease Expires . . . . . : Monday, April 5, 2021 3:12:48 AM
Default Gateway . . . . . : 192.168.43.1
DHCP Server . . . . . : 192.168.43.1
DHCPv6 IAID . . . . . : 103335487
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-14-6F-FF-28-C6-3F-9E-08-31
DNS Servers . . . . . : 192.168.43.1
NetBIOS over Tcpip. . . . . : Enabled

```

۸. یک بسته مربوط به دستور **ping** را انتخاب کنید و به بخش مربوط به پروتکل **DNS** در آن بروید. به بخش **Queries** بروید. چه **type** ای انتخاب شده است؟ به نظر شما این درخواست **DNS** برای چه کاری استفاده شده است؟

تایپ **A** انتخاب شده است. از این تایپ برای پیدا کردن آدرس **IP** یک **URL** استفاده می‌شود.
(طبق پروتکل **DNS**)

۹. یک بسته مربوط به دستور **nslookup** را انتخاب کنید و به بخش مربوط به پروتکل **DNS** در آن بروید. به بخش **Queries** بروید. چه **type** ای انتخاب شده است؟ به نظر شما این درخواست **DNS** برای چه کاری استفاده شده است؟

تایپ **PTR** انتخاب شده است. این تایپ دقیقاً برعکس تایپ **A** عمل می‌کند و برای پیدا کردن **Domain Name** یک آدرس **IP** بکار برده می‌شود.

۱۰. به نظر شما چه **type** های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

طبق RFC 1035 تایپ‌هایی همانند NS, MD, MF, CNAME, SOA, MB, MG, MR, NULL, WKS, HINFO, MINFO, MX و TXT بغیر از دو مورد ذکر شده وجود دارند.

۱۱. بعد از کلیک کردن بر روی OK چه اتفاقی می‌افتد؟ در بسته‌هایی که مشخص شده‌اند، چه پروتکل‌هایی را مشاهده می‌کنید؟

با کلیک کردن، تنها بسته‌هایی که مبدا یا مقصد آنها برابر با آدرس p30download.com هستند، نشان داده می‌شوند. (آدرس p30download.com توسط tracert برابر با 5.144.130.115 بدست آمد.) پروتکل بسته‌ها ICMP است.

۱۲. اولین بسته را انتخاب کنید. به بخش پروتکل ICMP بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

مقدار type برابر با (echo (ping) request) 8 است. مقدار TTL در اولین بسته برابر با 1 است.

۱۳. به نظر شما هدف از تغییر مقدار TTL چیست؟ می‌توانید با مراجعه به هدف tracert آن را شرح دهید.

بدلیل اینکه از تجهیزات Packet Switch برای ارسال بسته‌ها استفاده می‌شود و مسیر هر بسته تا مقصد با بسته‌های دیگر متفاوت است، مقدار TTL متغیر است.

۱۴. فیلتر 6 == ip.proto چه کاری انجام می‌دهد؟

با استفاده از این فیلتر، تمامی بسته‌هایی که IP protocol آنها TCP است نمایش داده می‌شود.