

سوال 1:

1. HTTP

- پروتکل انتقال داده‌های وب بین کلاینت و سرور.
- کلاینت درخواست ارسال می‌کند (مانند باز کردن یک صفحه وب) و سرور پاسخ می‌دهد.
- نسخه امن آن، HTTPS****، از ** TLS** برای رمزنگاری داده‌ها استفاده می‌کند.

2. DNS

- مسئول تبدیل نام دامنه‌مثل ('www.google.com') به آدرس IP
- کلاینت درخواست DNS می‌فرستد تا آدرس IP مرتبط با دامنه دریافت کند.
- به صورت پیش‌فرض بدون رمزنگاری است، ولی نسخه‌های امن مانند DoH و DoT وجود دارند.

3. DHCP

- تخصیص خودکار آدرس‌های IP به دستگاه‌ها در شبکه.
- وقتی دستگاهی به شبکه متصل می‌شود، از DHCP درخواست IP می‌کند و سرور DHCP به آن یک آدرس موقت اختصاص می‌دهد.

پروتکل	وظیفه	نوع ارتباط	پورت پیش‌فرض	رمزنگاری
HTTP	انتقال داده‌های وب (صفحات وب و منابع مرتبط)	درخواست-پاسخ	80 (HTTP)، 443 (HTTPS)	فقط در HTTPS رمزنگاری دارد
DNS	ترجمه نام دامنه به آدرس IP	درخواست-پاسخ	53	به طور پیش‌فرض ندارد، ولی DoH و DoT رمزنگاری می‌کنند
DHCP	تخصیص پویا آدرس IP به دستگاه‌ها	ارسال خودکار و پویا	67 (سرور)، 68 (کلاینت)	ندارد

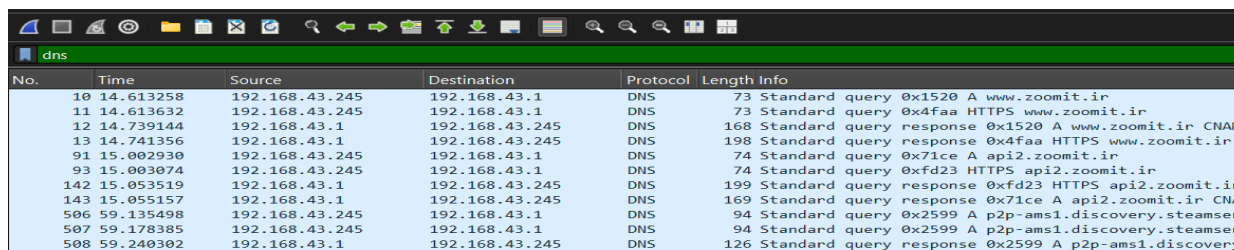
سوال 2:

ارتباطی مبتنی بر TCP و بر روی پورت 443 (پورت https) است. ارتباط از طریق TLSv1.3 ، (SSL/TLS) است.

مبدا (192.168.43.245): دستگاهی در شبکه محلی

مقصد (185.166.104.4): سرور خارجی

DNS



No.	Time	Source	Destination	Protocol	Length	Info
10	14.613258	192.168.43.245	192.168.43.1	DNS	73	Standard query 0x1520 A www.zoomit.ir
11	14.613632	192.168.43.245	192.168.43.1	DNS	73	Standard query 0x4faa HTTPS www.zoomit.ir
12	14.739144	192.168.43.1	192.168.43.245	DNS	168	Standard query response 0x1520 A www.zoomit.ir CNAME
13	14.741356	192.168.43.1	192.168.43.245	DNS	198	Standard query response 0x4faa HTTPS www.zoomit.ir CNAME
91	15.002930	192.168.43.245	192.168.43.1	DNS	74	Standard query 0x71ce A api2.zoomit.ir
93	15.003074	192.168.43.245	192.168.43.1	DNS	74	Standard query 0xfd23 HTTPS api2.zoomit.ir
142	15.053519	192.168.43.1	192.168.43.245	DNS	199	Standard query response 0xfd23 HTTPS api2.zoomit.ir CNAME
143	15.055157	192.168.43.1	192.168.43.245	DNS	169	Standard query response 0x71ce A api2.zoomit.ir CNAME
506	59.135498	192.168.43.245	192.168.43.1	DNS	94	Standard query 0x2599 A p2p-ams1.discovery.steamserver
507	59.178385	192.168.43.245	192.168.43.1	DNS	94	Standard query 0x2599 A p2p-ams1.discovery.steamserver
508	59.240302	192.168.43.1	192.168.43.245	DNS	126	Standard query response 0x2599 A p2p-ams1.discovery

پکت 10: کلاینت درخواست DNS A Record برای گرفتن IP دامنه www.zoomit.ir به سرور (192.168.43.1) DNS ارسال کرده.

پکت 11: کلاینت درخواست HTTPS Record برای دامنه www.zoomit.ir ارسال کرده.

پکت 12: سرور (192.168.43.1) DNS به درخواست A Record پاسخ داده و IP دامنه www.zoomit.ir (185.166.104.4) و 185.166.104.3 دامنه برگردانده.

پکت 13: به درخواست HTTPS Record پاسخ داده.

(Handshake)

TCP (TCP Three-Way Handshake)

پکت 14: کلاینت با ارسال پکت SYN ، درخواست برقراری ارتباط را آغاز کرده

پکت 15: سرور پاسخ با SYN, ACK داده و درخواست را تأیید کرده

پکت 16: کلاینت نیز پکت ACK را ارسال کرده تا تأیید کند که ارتباط TCP برقرار شده

TLS Handshake

پس از برقراری ارتباط TCP ، کلاینت شروع به انجام Handshake پروتکل TLS می کند:

پکت 18: پکت Client Hello ارسال کرده که بخشی از TLSv1.3 Handshake است. در این پکت، کلاینت اطلاعات الگوریتم های رمزنگاری را به سرور ارسال کرده. در این پکت، SNI به zoomit.ir اشاره می کند که یعنی با سرور آن است.

- پس از Handshake

پکت 21: سرور با ارسال پکت Server Hello و داده های اپلیکیشن شروع به ارسال داده های رمز شده کرده.

پکت های 22 تا 200: پکت های Application Data هستند که نشان می دهد داده های رمز شده بین کلاینت و سرور می شوند.

- در پکته 525 کلاینت با ارسال پکت FIN, ACK درخواست پایان ارتباط می دهد و سرور درخواست را با ارسال پکت FIN, ACK در پکت 526 تأیید می کند.

پکت های 14 تا 527 در فایل packets.txt