حسین باقریان

401130193

سوال 1)

HTTP یک پروتکل برای انتقال صفحات وب و داده های مرتبط بین کلاینت و سرور است. وقتی URL سایتی را وارد میکنیم درخواست HTTP برای دریافت صفحه وب به سرور ارسال می‌شود.

DNS پروتکلی است که که مانند یک دفترچه تلفن، نام های دامنه را به آدرس های IP متانظر تبدیل می‌کند. وقتی ما دامنه ای مثل example.com را وارد میکنیم DNS این دامنه را به IP متناظر با این دامنه مثل 192.168.1 تبدیل می‌کند.

DHCP وظیفه تخصیص خودکار آدرس‌های IP و اطلاعات پیکربندی شبکه به دستگاه‌های کلاینت (مانند کامپیوترها و گوشی‌های هوشمند) را دارد. هر زمان که دستگاهی به شبکه ای مثل Wi-Fi متصل می‌شود DHCP به صورت خودکار یک آدرس IP موقتی به همراه اطلاعات دیگری به آن اختصاص می‌دهد تا دستگاه بتواند به شبکه و اینترنت متصل شود.

سوال 2)

سایت کپچر شده: hut.ac.ir

DNS:

157	21.664485	192.168.43.121	178.22.122.100	DNS	73 Standard query 0x2bd0 HTTPS www.hut.ac.ir
158	21.753567	178.22.122.100	192.168.43.121	DNS	123 Standard query response 0x2bd0 HTTPS www.hut.ac.ir SOA ns1.hut.ac.ir
377	23.309856	192.168.43.121	178.22.122.100	DNS	69 Standard query 0x5c1b HTTPS hut.ac.ir
381	23.468375	192.168.43.121	185.51.200.2	DNS	69 Standard query 0x5c1b HTTPS hut.ac.ir
408	24.474883	192.168.43.121	178.22.122.100	DNS	69 Standard query 0x5c1b HTTPS hut.ac.ir
535	24.728715	185.51.200.2	192.168.43.121	DNS	119 Standard query response 0x5c1b HTTPS hut.ac.ir SOA ns1.hut.ac.ir
543	24.730441	178.22.122.100	192.168.43.121	DNS	119 Standard query response 0x5c1b HTTPS hut.ac.ir SOA ns1.hut.ac.ir
550	24.734646	178.22.122.100	192.168.43.121	DNS	119 Standard query response 0x5c1b HTTPS hut.ac.ir SOA ns1.hut.ac.ir
888	25.223256	192.168.43.121	178.22.122.100	DNS	79 Standard query 0x672d HTTPS trustseal.enamad.ir
889	25.223259	192.168.43.121	178.22.122.100	DNS	68 Standard query 0x0bb3 HTTPS balad.ir
890	25.227930	192.168.43.121	178.22.122.100	DNS	79 Standard query 0xb747 A trustseal.enamad.ir
891	25.228225	192.168.43.121	178.22.122.100	DNS	68 Standard query 0xf835 A balad.ir
987	25.285991	178.22.122.100	192.168.43.121	DNS	151 Standard query response 0x672d HTTPS trustseal.enamad.ir SOA g.ns.arvancdn.ir
1000	25.289476	178.22.122.100	192.168.43.121	DNS	100 Standard query response 0xf835 A balad.ir A 185.166.104.3 A 185.166.104.4
1001	25.290287	178.22.122.100	192.168.43.121	DNS	95 Standard query response 0xb747 A trustseal.enamad.ir A 212.16.67.4
1060	25.380978	192.168.43.121	185.51.200.2	DNS	68 Standard query 0x0bb3 HTTPS balad.ir
1131	25.490997	192.168.43.121	178.22.122.100	DNS	72 Standard query 0x2e85 HTTPS cdn.balad.ir
1132	25.497936	192.168.43.121	178.22.122.100	DNS	84 Standard query 0x21d8 HTTPS www.googletagmanager.com

1- عملیات DNS Query و Response:

در تصویر مشاهده می کنید که چندین Standard Query به سمت سرور DNS ارسال شده است تا آدرس IP متناظر با دامنه های مختلفی مثل balad.ir و trustseal.enamad.ir و hut.ac.ir به دست بیاید.

2- DNS Response:

بعد از ارسال کوئری، DNS Server به درخواست مرورگر پاسخ می‌دهد. پاسخ‌ها معمولاً شامل آدرس IP هستند که مرورگر از آن برای ایجاد ارتباط با سرور استفاده می‌کند.

برای مثال یک استاندارد کوئری برای hut.ac.ir (خط اول) که با پاسخ 178.22.122.100 (خط دوم) تکمیل شده است.

TCP:

369	23.294277	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=223222 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
370	23.294277	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=224622 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
371	23.294326	192.168.43.121	78.39.212.44	TCP	54 65362 → 443 [ACK] Seq=1379 Ack=226022 Win=131584 Len=0
372	23.304689	192.168.43.121	78.39.212.44	TCP	66 65366 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
373	23.304864	192.168.43.121	78.39.212.44	TCP	66 65367 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
374	23.309214	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=226022 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
375	23.309214	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=227422 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
376	23.309250	192.168.43.121	78.39.212.44	TCP	54 65362 → 443 [ACK] Seq=1379 Ack=228822 Win=131584 Len=0
378	23.320807	192.168.43.121	78.39.212.44	TCP	66 65368 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
379	23.338835	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=228822 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
380	23.388656	192.168.43.121	78.39.212.44	TCP	54 65362 → 443 [ACK] Seq=1379 Ack=230222 Win=131584 Len=0
382	23.500044	192.168.43.121	78.39.212.44	TCP	715 [TCP Retransmission] 65365 → 443 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=661
383	23.580759	192.168.43.121	78.39.212.44	TCP	66 65369 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
384	23.799560	192.168.43.121	78.39.212.44	TCP	715 [TCP Retransmission] 65365 → 443 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=661
385	23.928510	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=230222 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
386	23.941996	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=231622 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
387	23.942056	192.168.43.121	78.39.212.44	TCP	54 65362 → 443 [ACK] Seq=1379 Ack=233022 Win=131584 Len=0
388	23.942484	78.39.212.44	192.168.43.121	TCP	1454 443 → 65362 [ACK] Seq=233022 Ack=1379 Win=31872 Len=1400 [TCP PDU reassembled in 391]
389	23.987971	192.168.43.121	78.39.212.44	TCP	54 65362 → 443 [ACK] Seq=1379 Ack=234422 Win=131584 Len=0

تصویر مربوط به ترافیک پروتکلTCP است که شامل تبادل پکت ها بین IP های مختلف است.

پروتکل TCP برای برقراری ارتباط قابل اعتماد بین دو دستگاه استفاده می‌شود. هر اتصال TCP شامل سه مرحله اصلی است:

- SYN برای شروع ارتباط
- ACK برای تایید دریافت پکت ها
- FIN یا RST برای پایان دادن به ارتباط

در ترافیک کپچر شده پکت های TCP بین آدرس IP خصوصی 192.168.43.121 که مربوط به سیستم خودم است و آدرس IP عمومی 78.39.212.44 که برای سرور است مبادله شده اند.

پکت های SYN: بسته هایی که حاوی SYN هستند معمولا برای شروع یک ارتباط TCP استفاده می‌شوند. (در شکل خط های چهارم و ششم ریکوئست هایی با SYN از سیستم من به سرور ارسال شده است).

پکت های ACK: نشان دهنده تایید دریافت داده ها هستند. مثلا در خطوط اول، دوم و سوم مثال هایی از تایید دریافت اطلاعات بین دستگاه من و سرور است.

پکت هایی که با رنگ تیره نمایش داده شده اند، در ارسال اولیه، پاسخی از دست رفته و سرور مجبور به ارسال مجدد شده است.