محمد رضائی 401130363

HTTP (Hypertext Transfer Protocol)

پروتکل **HTTP** برای ارتباط بین مرورگرهای وب و سرورها به کار می‌رود. وقتی شما یک وب‌سایت را باز می‌کنید، مرورگر از طریق HTTP درخواست ارسال می‌کند و سرور، صفحه وب یا فایل مورد نظر را برمی‌گرداند. این پروتکل در لایه کاربرد مدل OSI قرار دارد و اساساً برای انتقال صفحات وب و داده‌های دیگر در اینترنت استفاده می‌شود.

DNS (Domain Name System)

DNS به تبدیل نام‌های دامنه به آدرس‌های IP کمک می‌کند. وقتی شما آدرس یک وب‌سایت مثل "example.com" را وارد می‌کنید، DNSاین نام را به آدرس IP متناظر تبدیل می‌کند تا مرورگر بتواند سرور درست را پیدا کرده و به آن متصل شود. این پروتکل هم در لایه کاربرد قرار دارد و نقش کلیدی در هدایت درخواست‌های وب دارد.

DHCP (Dynamic Host Configuration Protocol)

اما **DHCP** یک پروتکل است که به طور خودکار به دستگاه‌ها در شبکه آدرس‌های IP اختصاص می‌دهد. به جای این‌که کاربر به صورت دستی IP تنظیم کند، DHCP به دستگاه‌هایی که به شبکه متصل می‌شوند، یک آدرس IP و سایر تنظیمات شبکه را به صورت خودکار می‌دهد. DHCP کارکردی متفاوت دارد و برای ساده‌سازی مدیریت شبکه‌ها بسیار کاربردی است.

در نتیجه، HTTP برای انتقال داده‌ها در وب، DNS برای پیدا کردن سرورها از طریق نام دامنه و DHCP برای مدیریت آدرس‌دهی IP در شبکه استفاده می‌شود.

Capture traffic

udp.stream eq 4

No.	Time	Source	Destination	Protocol	Length	Info
6	1.134935485	192.168.131.133	192.168.131.2	DNS	68	Standard query 0x2070 HTTPS snapp.ir
25	6.137884742	192.168.131.133	192.168.131.2	DNS	68	Standard query 0x2070 HTTPS snapp.ir
26	6.642897210	192.168.131.2	192.168.131.133	DNS	149	Standard query response 0x2070 HTTPS snapp.ir SOA vip7.alidns.com
108	8.187233682	192.168.131.2	192.168.131.133	DNS	149	Standard query response 0x2070 HTTPS snapp.ir SOA vip7.alidns.com
109	8.187424252	192.168.131.133	192.168.131.2	ICMP	177	Destination unreachable (Port unreachable)
119	8.325848884	192.168.131.133	192.168.131.2	DNS	76	Standard query 0x1d38 A web-cdn.snapp.ir
172	8.487438399	192.168.131.2	192.168.131.133	DNS	108	Standard query response 0x1d38 A web-cdn.snapp.ir A 185.143.234.120

ip.addr == 185.143.234.120

No.	Time	Source	Destination	Protocol	Length	Info
56	7.500308204	192.168.131.133	185.143.234.120	TCP	74	35912 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=89822360 TS
63	7.616950992	185.143.234.120	192.168.131.133	TCP	60	443 → 35912 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
64	7.616985926	192.168.131.133	185.143.234.120	TCP	54	35912 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
65	7.617823944	192.168.131.133	185.143.234.120	TLSv1.3	1153	Client Hello
66	7.618100088	185.143.234.120	192.168.131.133	TCP	60	443 → 35912 [ACK] Seq=1 Ack=1100 Win=64240 Len=0
71	7.698065908	192.168.131.133	185.143.234.120	TCP	74	35914 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=89822558 TS
74	7.701438832	185.143.234.120	192.168.131.133	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
75	7.701483082	192.168.131.133	185.143.234.120	TCP	54	35912 → 443 [ACK] Seq=1100 Ack=213 Win=64028 Len=0
76	7.701949705	192.168.131.133	185.143.234.120	TLSv1.3	118	Change Cipher Spec, Application Data
77	7.702228605	185.143.234.120	192.168.131.133	TCP	60	443 → 35912 [ACK] Seq=213 Ack=1164 Win=64240 Len=0
78	7.702377363	192.168.131.133	185.143.234.120	TLSv1.3	224	Application Data
79	7.702454092	192.168.131.133	185.143.234.120	TLSv1.3	580	Application Data
80	7.702604439	185.143.234.120	192.168.131.133	TCP	60	443 → 35912 [ACK] Seq=213 Ack=1334 Win=64240 Len=0
81	7.702604529	185.143.234.120	192.168.131.133	TCP	60	443 → 35912 [ACK] Seq=213 Ack=1860 Win=64240 Len=0
82	7.761697040	185.143.234.120	192.168.131.133	TCP	60	443 → 35914 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
83	7.761758804	192.168.131.133	185.143.234.120	TCP	54	35914 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
84	7.762695616	192.168.131.133	185.143.234.120	TLSv1.3	1171	Client Hello
85	7.763218225	185.143.234.120	192.168.131.133	TCP	60	443 → 35914 [ACK] Seq=1 Ack=1118 Win=64240 Len=0
86	7.767329673	185.143.234.120	192.168.131.133	TLSv1.3	534	Application Data, Application Data
87	7.769249417	192.168.131.133	185.143.234.120	TLSv1.3	85	Application Data
88	7.769552782	185.143.234.120	192.168.131.133	TCP	60	443 → 35912 [ACK] Seq=693 Ack=1891 Win=64240 Len=0
89	7.837677862	185.143.234.120	192.168.131.133	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
90	7.837745735	192.168.131.133	185.143.234.120	TCP	54	35914 → 443 [ACK] Seq=1118 Ack=213 Win=64028 Len=0

۱ .تحلیل ترافیکDNS

در این ترافیک، pc با آدرس IP 192.168.131.133 چندین درخواست DNS به سرور DNS با آدرس 192.168.131.2 ارسال می‌کند. این درخواست‌ها مربوط به دامنه‌های **snapp.ir**و **web-cdn.snapp.ir**هستند.

- **کوئری DNS برای snapp.ir**: دستگاه درخواست‌هایی را برای رکوردهای SOA و A دامنه snapp.irارسال می‌کند و پاسخ‌های دریافتی شامل اطلاعات موردنظر هستند.
- **کوئری DNS برای web-cdn.snapp.ir**: درخواست برای رکورد A دامنه web-cdn.snapp.ir CDN پاسخ داده می‌شود و آدرس IP **185.143.234.120** برای این دامنه بازگردانده می‌شود. این آدرس در مراحل بعدی برای اتصال TCP و TLS استفاده می‌شود.

۲ .تحلیل ترافیکTCP

بعد از اینکه DNS آدرس IP را پیدا کرد، دستگاه شروع به برقراری اتصال TCP به آدرس IP **185.143.234.120** آدرس دامنه (web-cdn.snapp.ir) می‌کند. این اتصال شامل چندین بسته SYN، ACKو FIN است.

- **هندشیک:TCP**

- **هندشیک سه‌طرفه :**در ابتدا یک بسته SYN از طرف client (192.168.131.133) به پورت 443 پروتکل HTTPS در سرور ارسال می‌شود. سپس سرور با یک SYN-ACK پاسخ می‌دهد و دستگاه ما نیز یک ACK برای تکمیل هندشیک ارسال می‌کند.

- **انتقال داده:**

  - پس از هندشیک، داده‌های شروع به تبادل می‌شوند. این داده‌ها شامل بسته‌های رمزنگاری‌شده هستند که در طول‌های مختلف TCP قابل‌مشاهده است و نشان‌دهنده انتقال معمول داده‌های HTTPS است.

۳ .تحلیل ترافیکTLS/SSL

پس از برقراری اتصالTCP، دستگاه یک Session TLS را آغاز می‌کند که به عنوان Client Hello در ترافیک دیده می‌شود.

- **هندشیک TLS**:

  - Client برای شروع ارتباط امن، یک پیام Client Helloارسال می‌کند. این پیام شامل اطلاعات رمزنگاری مانند مجموعه رمزها و نسخه‌های پشتیبانی‌شده است.
  - سپس سرور با ارسال Server Hello پاسخ می‌دهد که شامل مجموعه رمز انتخاب‌شده و سایر تنظیمات امنیتی برای برقراری ارتباط رمزنگاری‌شده است.

- **داده‌های TLS**:

  - بعد از اتمام هندشیکTLS، تبادل داده‌های رمزنگاری‌شده بین client و سرور آغاز می‌شود. این بسته‌های داده تحت عنوان Application Data در ترافیک دیده می‌شوند. به دلیل رمزنگاری، محتوای این داده‌ها `