

پروژه دوم شبکه

مریم خدایاری

۴۰۱۱۳۰۲۹۳

پاسخ سوال یک:

HTTP : پروتکل انتقال داده‌ها در وب است (برای درخواست صفحات وب).

DNS : برای تبدیل نام دامنه‌ها به آدرس‌های IP استفاده می‌شود.

DHCP : آدرس‌های IP را به طور خودکار به دستگاه‌های شبکه اختصاص می‌دهد.

پاسخ سوال دو:

The image shows a Wireshark network traffic capture. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by 'Apply a display filter: <Ctrl-F>'. The list shows various DNS queries and responses, as well as HTTP application data. The packet details pane on the right shows the structure of the selected packet (No. 1), which is a DNS Standard query. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.186.80	185.51.200.2	DNS	84	Standard query 0x85ab A www.google-analytics.com
2	0.001526	192.168.186.80	178.22.122.100	DNS	84	Standard query 0x5bbe HTTPS www.google-analytics.com
3	0.073465	192.168.186.80	204.12.192.219	TLSv1.2	194	Application Data
4	0.348103	204.12.192.219	192.168.186.80	TCP	54	443 → 65204 [ACK] Seq=1 Ack=141 Win=245 Len=0
5	0.348103	204.12.192.219	192.168.186.80	TLSv1.2	304	Application Data, Application Data, Application Data, Application Data
6	0.349170	192.168.186.80	204.12.192.219	TLSv1.2	93	Application Data
7	0.659195	204.12.192.219	192.168.186.80	TCP	54	443 → 65204 [ACK] Seq=251 Ack=180 Win=245 Len=0
8	1.027415	192.168.186.80	185.51.200.2	DNS	84	Standard query 0xc38 HTTPS www.google-analytics.com
9	1.990520	178.22.122.100	192.168.186.80	DNS	84	Standard query response 0x5bbe HTTPS www.google-analytics.com
10	2.987918	192.168.186.80	204.12.192.221	TCP	55	65167 → 5228 [ACK] Seq=1 Ack=1 Win=254 Len=1
11	3.216294	204.12.192.221	192.168.186.80	TCP	66	5228 → 65167 [ACK] Seq=1 Ack=2 Win=245 Len=0 SLE=1 SRE=2
12	3.833066	185.51.200.2	192.168.186.80	DNS	100	Standard query response 0x85ab A www.google-analytics.com A 50.7.87.86
13	3.835761	192.168.186.80	50.7.87.86	TCP	66	65220 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
14	4.037595	50.7.87.86	192.168.186.80	TCP	66	443 → 65220 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1400 SACK_PERM WS=128
15	4.037805	192.168.186.80	50.7.87.86	TCP	54	65220 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
16	4.042104	192.168.186.80	50.7.87.86	TLSv1.3	1788	Client Hello (SHA=www.google-analytics.com)
17	4.042109	192.168.186.80	50.7.87.86	TCP	54	65221 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
18	4.240265	185.51.200.2	192.168.186.80	DNS	84	Standard query response 0xc38 HTTPS www.google-analytics.com
19	4.240265	50.7.87.86	192.168.186.80	TCP	54	443 → 65220 [ACK] Seq=1 Ack=1401 Win=31360 Len=0
20	4.240265	50.7.87.86	192.168.186.80	TCP	54	443 → 65220 [ACK] Seq=1 Ack=1735 Win=31360 Len=0
21	4.240265	50.7.87.86	192.168.186.80	TCP	66	443 → 65221 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1400 SACK_PERM WS=128
22	4.240265	50.7.87.86	192.168.186.80	TLSv1.3	5654	Server Hello, Change Cipher Spec
23	4.240265	50.7.87.86	192.168.186.80	TLSv1.3	427	Application Data
24	4.241154	192.168.186.80	50.7.87.86	TCP	54	65221 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
25	4.241294	192.168.186.80	50.7.87.86	TCP	54	65220 → 443 [ACK] Seq=1735 Ack=5974 Win=65792 Len=0
26	4.254587	192.168.186.80	50.7.87.86	TLSv1.3	335	Client Hello (SHA=www.google-analytics.com)
27	4.445910	50.7.87.86	192.168.186.80	TCP	54	443 → 65221 [ACK] Seq=1 Ack=282 Win=31872 Len=0
28	4.445910	50.7.87.86	192.168.186.80	TLSv1.3	4254	Server Hello, Change Cipher Spec
29	4.445910	50.7.87.86	192.168.186.80	TLSv1.3	567	Application Data
30	4.445637	192.168.186.80	50.7.87.86	TCP	54	65221 → 443 [ACK] Seq=282 Ack=4714 Win=65792 Len=0

Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{D0BCA14D-65-4A-40-80-00} over Ethernet II, Src: Intel_d1:57:18 (a8:7e:ea:d1:57:18), Dst: 76:ea:7e:03:87:a0 (76:ea:7e:03:87:a0)

> Internet Protocol Version 4, Src: 192.168.186.80, Dst: 185.51.200.2

> User Datagram Protocol, Src Port: 65175, Dst Port: 53

> Domain Name System (query)

0000 76 ea 7e 03 87 a0 a8 7e ea d1 57 18 08 00 45 00 www.google-analytics.com

0010 00 46 ea d8 00 00 00 11 00 00 c0 a8 ba 50 b9 33 www.google-analytics.com

0020 c8 02 fe 97 00 35 00 32 fc 72 85 ab 01 00 00 01 www.google-analytics.com

0030 00 00 00 00 00 00 03 77 77 77 10 67 6f 6f 6c www.google-analytics.com

0040 65 2d 61 6e 61 6c 79 74 69 63 73 03 63 6f 6d 00 www.google-analytics.com

0050 00 01 00 01

گزارش تحلیل ترافیک شبکه با استفاده از Wireshark

در این گزارش، ترافیک کپچر شده هنگام باز کردن سایت www.w3schools.com با استفاده از نرم افزار Wireshark تحلیل شده است. هدف از این تحلیل، بررسی ارتباط بین مرورگر و سرورهای مورد نیاز برای دسترسی به این سایت و همچنین شناسایی پروتکل های استفاده شده در این فرآیند است.

"تحلیل ترافیک"

۱. پروتکل: DNS

- در ابتدا، مرورگر برای تبدیل نام دامنه www.w3schools.com به آدرس IP، از پروتکل DNS استفاده کرده است.
- در بسته های شماره ۱ و ۴، درخواست های DNS (Query) به سرور DNS ارسال شده اند. درخواست شامل نام دامنه و نوع رکورد مورد نظر بوده است.
- پاسخ های DNS (Response) در بسته های شماره ۳ و ۶ دریافت شده اند که حاوی آدرس IP سرورهای مقصد است.

۲. پروتکل: TCP

- پس از دریافت آدرس IP، ارتباط بین کلاینت و سرور آغاز شده است. در بسته های شماره ۱۰ و ۱۱، ارتباط TCP با استفاده از فرآیند **Three-Way Handshake** برقرار شده است:

- **SYN:** کلاینت درخواست اتصال به سرور را ارسال می کند.
- **SYN-ACK:** سرور این درخواست را تأیید می کند.
- **ACK:** کلاینت پاسخ تأیید سرور را ارسال می کند.

۳. پروتکل: TLS

- از آنجا که سایت از HTTPS استفاده می کند، ارتباط ایمن از طریق پروتکل TLS برقرار شده است.

- در بسته‌های شماره ۱۴ و ۱۵، پیام‌های **Client Hello** و **Server Hello** مشاهده می‌شوند که برای شروع فرآیند رمزنگاری استفاده شده‌اند.
- مراحل دیگر TLS، شامل **Change Cipher Spec** و **Application Data**، نشان می‌دهند که ارتباط رمزگذاری شده است.

۴. تحلیل ترافیک: HTTP

- پس از برقراری ارتباط TLS، مرورگر شروع به ارسال درخواست‌های HTTP در قالب (HTTPS) می‌کند. این درخواست‌ها احتمالاً شامل GET یا POST برای دریافت منابع سایت هستند. به دلیل رمزگذاری، جزئیات این درخواست‌ها در کیچر مشاهده نمی‌شود.

در نگاه کلی...

- این ترافیک نشان‌دهنده فرآیند معمول باز کردن یک وبسایت است:
- ابتدا از **DNS** برای تبدیل نام دامنه به آدرس IP استفاده شده است.
 - سپس اتصال TCP برقرار شده و از طریق **TLS** ارتباط رمزگذاری شده‌ای برای ارسال و دریافت داده‌ها ایجاد شده است.
 - استفاده از پروتکل‌های استاندارد مانند DNS، TCP و TLS امنیت و کارایی ارتباط را تضمین می‌کند.
- این تحلیل نشان می‌دهد که هر یک از پروتکل‌ها نقش مهمی در برقراری ارتباط و انتقال داده‌ها در شبکه ایفا می‌کنند.