

## HTTP:

یکی از پایه ای ترین پروتکل های وب که برای ارتباط استفاده میشود و به مرورگر ها اجازه انتقال داده ، تصویر ، ویدیو و.... را میدهد

## DNS:

مثل یک دفترچه تلفن است که بجای ip ادرس و دامنه میدهد

## DHSP:

یکی از مهم ترین پروتکل های وب برای توزیع و تقسیم ip استفاده میشود و اجازه میدهد ip را به صورت خودکار به دستگاه های شبکه assign کنیم

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.180	149.154.167.92	TCP	78	64854 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=2722991383 TSecr=0 SACK_PERM
2	0.379665	192.168.1.180	173.194.182.74	TCP	78	64863 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2233395991 TSecr=0 SACK_PERM
3	0.406111	192.168.1.180	172.217.19.206	TCP	66	64845 → 443 [FIN, ACK] Seq=1 Ack=1 Win=2048 Len=0 TSval=3946818412 TSecr=2967465142
4	0.444678	172.217.19.206	192.168.1.180	TCP	66	443 → 64845 [FIN, ACK] Seq=1 Ack=2 Win=1033 Len=0 TSval=2967468665 TSecr=3946818412
5	0.444921	192.168.1.180	172.217.19.206	TCP	66	64845 → 443 [ACK] Seq=2 Ack=2 Win=2048 Len=0 TSval=3946818450 TSecr=2967468665
6	0.471738	173.194.182.74	192.168.1.180	TCP	74	443 → 64863 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 SACK_PERM TSval=3226238078 TSecr=2233396085
7	0.471965	192.168.1.180	173.194.182.74	TCP	66	64863 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=2233396083 TSecr=3226238078
8	0.472985	192.168.1.180	173.194.182.74	TCP	1462	64863 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=1396 TSval=2233396085 TSecr=3226238078 [TCP PDU reassembled]
9	0.473023	192.168.1.180	173.194.182.74	TLSv1..	416	Client Hello [SNI=rr5---sn-4g5e6ns7.c.drive.google.com]
10	0.563397	173.194.182.74	192.168.1.180	TCP	66	443 → 64863 [ACK] Seq=1 Ack=1397 Win=68352 Len=0 TSval=3226238170 TSecr=2233396085
11	0.563397	173.194.182.74	192.168.1.180	TCP	66	443 → 64863 [ACK] Seq=1 Ack=1747 Win=71168 Len=0 TSval=3226238171 TSecr=2233396085
12	0.563397	173.194.182.74	192.168.1.180	TLSv1..	1462	Server Hello, Change Cipher Spec
13	0.563517	192.168.1.180	173.194.182.74	TCP	66	64863 → 443 [ACK] Seq=1747 Ack=1397 Win=129792 Len=0 TSval=2233396175 TSecr=3226238171
14	0.565016	173.194.182.74	192.168.1.180	TCP	1462	443 → 64863 [ACK] Seq=1397 Ack=1747 Win=71168 Len=1396 TSval=3226238171 TSecr=2233396085 [TCP PD...
15	0.565017	173.194.182.74	192.168.1.180	TCP	1462	443 → 64863 [ACK] Seq=2793 Ack=1747 Win=71168 Len=1396 TSval=3226238171 TSecr=2233396085 [TCP PD...
16	0.565018	173.194.182.74	192.168.1.180	TLSv1..	504	Application Data
17	0.565104	192.168.1.180	173.194.182.74	TCP	66	64863 → 443 [ACK] Seq=1747 Ack=4627 Win=127808 Len=0 TSval=2233396177 TSecr=3226238171
18	0.565198	192.168.1.180	173.194.182.74	TCP	66	[TCP Window Update] 64863 → 443 [ACK] Seq=1747 Ack=4627 Win=131072 Len=0 TSval=2233396177 TSecr=...
19	0.566027	192.168.1.180	173.194.182.74	TLSv1..	130	Change Cipher Spec, Application Data
20	0.566315	192.168.1.180	173.194.182.74	TCP	1462	64863 → 443 [ACK] Seq=1811 Ack=4627 Win=131072 Len=1396 TSval=2233396178 TSecr=3226238171 [TCP P...
21	0.566333	192.168.1.180	173.194.182.74	TLSv1..	1308	Application Data

در این تصویر تعدادی از ارتباطات را میبینیم که از دستگاهی که ip ان در بخش source نوشته شده به سمت مقصد ip ای که در destination نوشته شده ارسال شده

در بخش protocol نوع پروتکل استفاده شده را میبینیم که در این بخش از ترافیک بیشتر نوع tcp است

در بخش length اندازه هر بسته داده‌ای است که در شبکه انتقال یافته است. این اندازه بر حسب بایت است

این تصویر یک تحلیل شبکه توسط ابزار Wireshark است و بسته‌های TCP را نشان می‌دهد. در اینجا یک سری ارتباطات بین یک آدرس IP لوکال (192.168.1.180) و چند سرور خارجی مانند 149.154.167.92، 172.217.19.206 و 173.194.182.74 مشاهده می‌شود.. از این تصویر، می‌توان نتیجه گرفت که دستگاهی با IP 192.168.1.180 در حال برقراری یک ارتباط رمزنگاری شده با سرورهایی در اینترنت است که به احتمال زیاد به سرویس‌های Google و یا دیگر سرویس‌های اینترنتی مرتبط می‌باشند.