



## طس افاسی - ۱۴۰۳/۹/۲۷

- تفاوت سه پروتکل HTTP و DNS و DHCP چیست؟
- در مرورگر خود یک سایت را باز و ترافیک را با استفاده از Wireshark کپچر کنید. طی یک گزارش تک صفحه ای ترافیک کپچر شده را تحلیل نمایید. (امکان استفاده از سایر پروتکل های مطرح مثل ICMP و DHCP هم وجود دارد).

۱- پروتکل DNS به ما اجازه می دهد به جای IP، آدرس و دامنه داشته باشیم.

DHCP برای توزیع و تقسیم IP مورد استفاده قرار می لیرد و به ما اجازه می دهد به صورت اتوماتیک IP ها را به دستگاه های مختلف داخل شبکه والذار کنیم. و HTTP می از باید ای ترین پروتکل های موجود در وب به حساب می آید که برای برخواری ارتباط مورد استفاده قرار می لیرد و به مرورگرهای اجازه می دهد داده ها را بفرستند و جواب را بخیزند و به ما نهایی دهند.

۲- ترافیک wifi را خواهیم بررسی کنیم. در این مثال ما سایت github را باز کردیم و برای پروتکل ها حاضر محمد دلیلی نهاده استیم تمام پروتکل ها را در نظر اصلی به مانسان می دهد.

در سرمهور packet NO ترتیب به مانمانش می دهد در سرمهور Time، از زمان یک که ما در خواست را فرستادیم تا زمان حال را به مانسان ای دهد که packet های مانکن به آنها رسیده اند.

در Source به مانسان می دهد که از جهی IP، داده ها ارسال شده است به طر

مثال در پکیت اول که درخواست است از ۱۹۲.۱۶۸.۱.۱۰۱ IP ما است زیرا.

در پکیت، به مانند این دھرده پکیت که ارسال کرد و این پکیت را کجا زنده نمایم - Destination کدام IP سیستم ما آمده است.

در قسمت protocol، چون ما محدودیت قرار ندادیم، پروتکل های متناسب دیگر سود ماید DNS، HTTP، TCP و ...

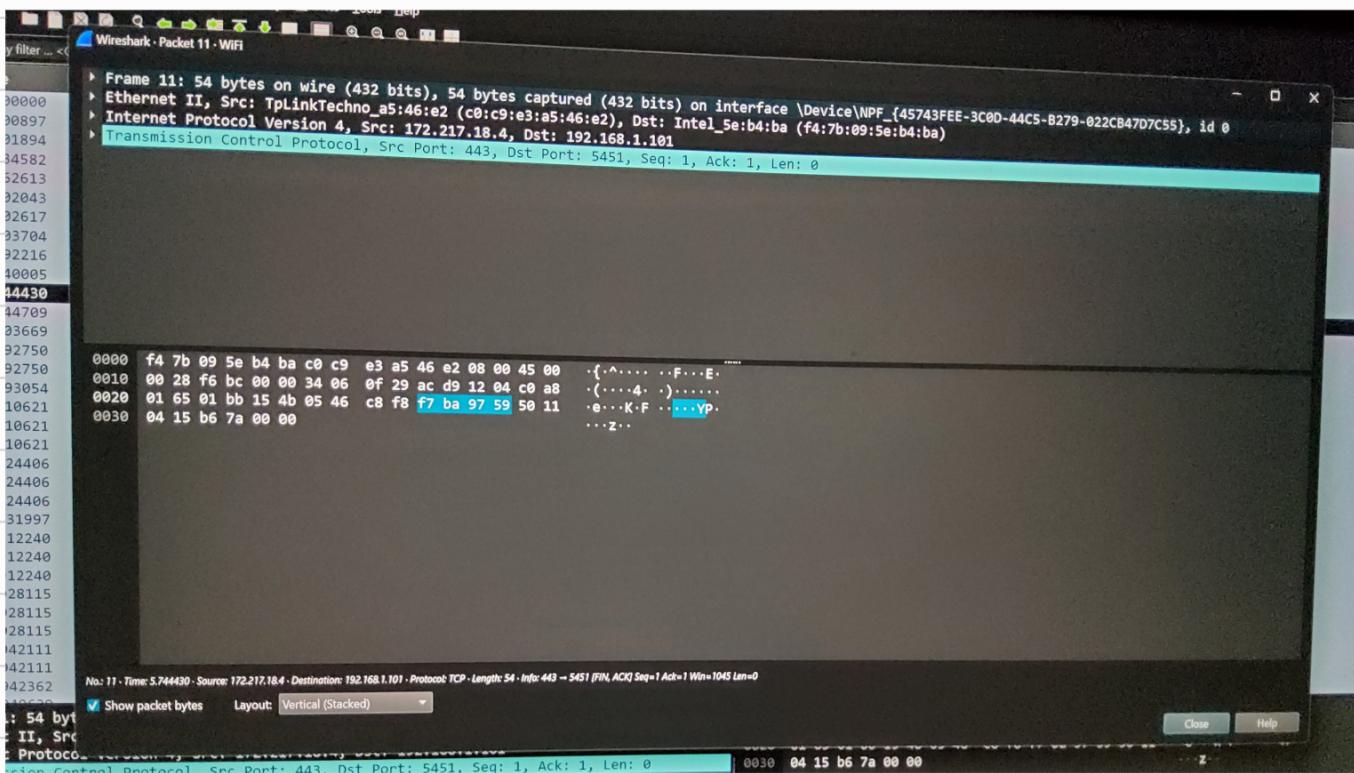
و در طول پروتکل های بروزرسانی شود مثلاً پروتکل length است.

و در مرستون آنچه Info را داریم که اطلاعات و دیتای اطلاعاتی اضافه در مورد پکیت در آن قرار داده شد. مثلاً نوعش چیز، Id آن پکیت و ...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	230.0.0.1	UDP	92	59420 → 6666 Len=50
2	1.000897	192.168.1.101	230.0.0.1	UDP	92	59420 → 6666 Len=50
3	2.001894	192.168.1.101	230.0.0.1	UDP	92	59420 → 6666 Len=50
4	2.834582	192.168.1.101	185.25.183.36	TLSv...	113	Application Data
5	2.962613	185.25.183.36	192.168.1.101	TCP	54	27025 → 1360 [ACK] Seq=1 Ack=60 Win=16387 Len=0
6	3.002043	192.168.1.101	230.0.0.1	UDP	92	59420 → 6666 Len=50
7	4.002617	192.168.1.101	230.0.0.1	UDP	92	59420 → 6666 Len=50
8	5.003704	192.168.1.101	230.0.0.1	UDP	92	59420 → 6666 Len=50
9	5.392216	192.168.1.101	78.157.42.101	DNS	94	Standard query 0x56ee A p2p-dxb1.discovery.steamserver.net
10	5.448005	78.157.42.101	192.168.1.101	DNS	194	Standard query response 0x56ee A p2p-dxb1.discovery.steamserver.net A 185.25.183.36 A 185.25.183.52
11	5.744430	172.217.18.4	192.168.1.101	TCP	54	443 → 5451 [FIN, ACK] Seq=1 Ack=1 Win=1045 Len=0
12	5.744709	192.168.1.101	172.217.18.4	TCP	54	5451 → 443 [ACK] Seq=1 Ack=2 Win=515 Len=0
13	6.003669	192.168.1.101	230.0.0.1	UDP	92	59420 → 6666 Len=50
14	6.792750	192.168.1.1	239.255.255.250	SSDP	459	NOTIFY * HTTP/1.1
15	6.792750	192.168.1.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
16	6.793054	192.168.1.1	239.255.255.250	SSDP	531	NOTIFY * HTTP/1.1
17	6.810621	192.168.1.1	239.255.255.250	SSDP	523	NOTIFY * HTTP/1.1
18	6.810621	192.168.1.1	239.255.255.250	SSDP	466	NOTIFY * HTTP/1.1
19	6.810621	192.168.1.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1
20	6.824406	192.168.1.1	239.255.255.250	SSDP	539	NOTIFY * HTTP/1.1
21	6.824406	192.168.1.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
22	6.824406	192.168.1.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
23	6.831997	192.168.1.1	239.255.255.250	SSDP	521	NOTIFY * HTTP/1.1
24	6.912240	192.168.1.1	239.255.255.250	SSDP	459	NOTIFY * HTTP/1.1
25	6.912240	192.168.1.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
26	6.912240	192.168.1.1	239.255.255.250	SSDP	531	NOTIFY * HTTP/1.1
27	6.928115	192.168.1.1	239.255.255.250	SSDP	523	NOTIFY * HTTP/1.1
28	6.928115	192.168.1.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
29	6.928115	192.168.1.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1
30	6.942111	192.168.1.1	239.255.255.250	SSDP	539	NOTIFY * HTTP/1.1
31	6.942111	192.168.1.1	239.255.255.250	SSDP	466	NOTIFY * HTTP/1.1
32	6.942362	192.168.1.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
33	6.942362	192.168.1.1	239.255.255.250	SSDP	443	NOTIFY * HTTP/1.1
Frame 11: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{...}						
Ethernet II, Src: TpLinkTechno_a5:46:e2 (c0:9:e5:a5:46:e2), Dst: Intel_Et:bb:ba (f4:7b:09:5e:b4:ba)						
Internet Protocol Version 4, Src: 172.217.18.4, Dst: 192.168.1.101						
Transmission Control Protocol, Src Port: 443, Dst Port: 5451, Seq: 1, Ack: 1, Len: 0						
0000 f4 7b 09 5e b4 ba c0 c9 e3 a5 46 e2 08 00 45 00 { .. F-E .. }						
0010 00 28 f6 bc 00 34 06 0f 29 ac d9 12 04 c8 a8 { .. 4 .. }						
0020 01 65 01 bb 15 4b 05 46 c8 f8 f7 ba 97 59 50 11 e-4-YP .. Z ..						
0030 04 15 b6 7a 00 00						
Packets: 12232						

ب مکانی روی پکیت معاوی کو از آن را بینیم.

برای مثال الگوریتم ۱۱ مکانی کنم، صفحه بازسده می کوئیم بنظر های پایین صفحه را به طور دقیق تر بینیم. (بنظر ناسین که در ویندوز)



در نیزه دستگاهی کوآنتم اطلاعات Ethernet II، IPv4، TCP را باز کرده که تفکر کنید که محتوا که مختلف سلسله هستند که صورت آن که صدر جدای روی درخواست و ارسال بیکند.

با باز کردن صورت ادام از ۳ لایه تفکر کوآنتم جزئیات بینتری را بررسی کنید  
بارگذاری از لایه TCP بسته لایه های پهنی سه ایما، Ethernet II بسته ایما افزاری فرمی شود.

در قسمت Source میتوانیم چیزی که سورس بررسی می کنیم، آدرس Destination را مشاهده کنیم.

در لایه Ethernet II میتوانیم آدرس در انتشار ماقراری لیدر و را Type مشاهده کنیم.

که بعده میتوانیم Frame میتوانیم افزاری است.