

پروژه دوم شبکه آیلین امیدی 401130163

1.

HTTP یکی از پایه ای ترین پروتکل های وب به حساب میاد که برای برقراری ارتباط استفاده میشه. به مرورگر اجازه میده دیتاهایی مثل فیلم، عکس و... رو بفرسته و جواب رو بگیره و به ما نمایش بده.

DNS مثل دفترچه تلفن میمونه که به ما اجازه میده به جای **ip** آدرس و دامنه داشته باشیم. مثلاً وقتی سرچ میکنیم **google.com** به **DNS** ای داریم که **Google.com** رو داره و **ip** رو هم داره و **request** رو میفرسته سمت **ip**.

DHSP یکی از پروتکل های مهم است که برای توزیع و تقسیم **ip** مورد استفاده قرار میگیره. به ما اجازه میده **ip** ها را به صورت اتوماتیک به دستگاه های داخل شبکه **assign** کنیم.

*Wi-Fi (icmp)						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.212.157	138.68.89.78	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
2	0.000004	192.168.212.157	162.243.166.128	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
3	0.000108	192.168.212.157	213.183.53.174	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
4	0.000432	192.168.212.157	5.188.181.4	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
5	0.001778	192.168.212.157	138.68.89.78	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
6	0.002177	192.168.212.157	162.243.166.128	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
7	0.002421	192.168.212.157	213.183.53.174	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
8	0.002514	192.168.212.157	5.188.181.4	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
9	0.003623	192.168.212.157	138.68.89.78	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
10	0.003948	192.168.212.157	162.243.166.128	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
11	0.004134	192.168.212.157	213.183.53.174	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
12	0.004467	192.168.212.157	5.188.181.4	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
13	0.005650	192.168.212.157	138.68.89.78	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
14	0.006019	192.168.212.157	162.243.166.128	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
15	0.006341	192.168.212.157	213.183.53.174	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
16	0.006633	192.168.212.157	5.188.181.4	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
17	0.008553	192.168.212.157	138.68.89.78	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
18	0.009384	192.168.212.157	162.243.166.128	ICMP	82	Echo (ping) request id=0x3a94, seq=0/0, ttl=64 (no response found!)
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{78C6C968-44-40-00-00-00-00-00-00} (0.000000)				0000 86 49 99 92 e2 45 2c 3b 70 b0 49 cd 08 00 45 00 .I...E;; p-I...E.		
Ethernet II, Src: AzureWaveTec_b0:49:cd (2c:3b:70:b0:49:cd), Dst: 86:49:99:92:e2:45 (86:49:99:92:e2:45)				0010 00 44 94 b0 40 00 40 01 2d 23 c0 a8 d4 9d 8a 44 D...@...-#.....D		
Internet Protocol Version 4, Src: 192.168.212.157, Dst: 138.68.89.78				0020 59 4e 08 00 d3 7a 3a 94 00 00 fa 33 f7 b8 04 00 YN...z...-...3....		
Internet Control Message Protocol				0030 00 00 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d --012345 6789;=<		
				0040 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d >>@ABCDE FGHIJKLM		
				0050 4e 4f NO		

تعداد زیادی packet داریم از طریق سرچ کردن یک سایت که ستون No. تعداد آن و عدد هر packet را مشخص می کند. با توجه به ترافیک کپچر شده با پروتکل ICMP، می توانیم در ستون time زمان ارسال پیام ها و زمان دریافت جواب ها را مشاهده کنیم. در ستون source و destination می توانیم به ترتیب آدرس گیرنده و فرستنده پیام را مشاهده کنیم. ستون پروتکل هم به ما نشان می دهد که از چه پروتکلی برای ارتباط بین دو سرور استفاده شده است که در اینجا به خاطر محدود کردن پروتکل ها، فقط پروتکل ICMP را داریم. اما در کل پروتکل ها رنگ های متفاوتی دارند. در ستون length طول packet را مشاهده می کنیم که طول پروتکل ICMP، 82 بایت است. ستون info اطلاعاتی راجع به packet به ما می دهد. برای مثال ping آن، request یا reply بودن آن، طول بازه زمانی reply شده و... را نشان می دهد که در اینجا response یا reply موجود نیست.

قسمت پایین سمت راست ماشین کد است که برای ما کامل قابل فهم نیست.

قسمت پایین سمت چپ دیتا هایی راجع به هر packet در اختیار ما می گذارد که برای هر کدوم از packet ها می تواند متفاوت باشد. که داخل آن اطلاعاتی مانند اطلاعاتی که در بخش info داشتیم دریافت می کنیم اما با جزییات بیشتر.

Frame 1 : دیتای مربوط به سخت افزار به صورت خلاصه در اینجا قرار دارد.

Ethernet 2 : حالت سخت افزاری دارد. Type آی پی را نیز نشان می دهد.

Ip : اینکه Ip چقدر در دسترس هست و source adress و destination adress آن چیست.

ICMP : مهم ترین چیزی که از این بخش متوجه می شویم این هست که جواب آن packet کجا آمده است.