Sakai：CS 305 01 fall2022：练习与测验

lab2_practice_Wireshark

- 返回测验列表

大项 1 of 1 - 8.0/ 10.0 得分

题目 1 of 10

1.0/ 1.0 得分

Which expression(s) may work if we want to capture packages satisfying particular conditions?

- A. net 360.9.0.0
- B. src net 192.168.0.0/48
- C. port 39928000
- D. net 192.168.0.0 mask 255.255.255.0

题目 2 of 10

1.0/ 1.0 得分

According to the nslookup executing results, if we want to capture all the data between local PC and Baidu server by Wireshark, which expression(s) will be suitable?

A. ip.addr == 183.232.231.172 and 183.232.231.174

B. ip.addr == 183.232.231.172 or 183.232.231.174

C. host 183.232.231.172 and 183.232.231.174

D. ip.addr == 183.232.231.172 and ip.addr == 183.232.231.174

E. host 183.232.231.172 or 183.232.231.174

F. host 183.232.231.172 and host 183.232.231.174

G. host 183.232.231.172 or host 183.232.231.174

H. ip.addr == 183.232.231.172 or ip.addr == 183.232.231.174

题目 3 of 10

1.0/ 1.0 得分

According to the nslookup executing results, if we want to display all the data between local PC and Baidu server in details by Wireshark, which expression(s) will be suitable?

A. host 183.232.231.172 or 183.232.231.174

B. ip.addr == 183.232.231.172 and ip.addr == 183.232.231.174

C. host 183.232.231.172 or host 183.232.231.174

D. ip.addr == 183.232.231.172 or ip.addr == 183.232.231.174

E. host 183.232.231.172 and 183.232.231.174

F. host 183.232.231.172 and host 183.232.231.174

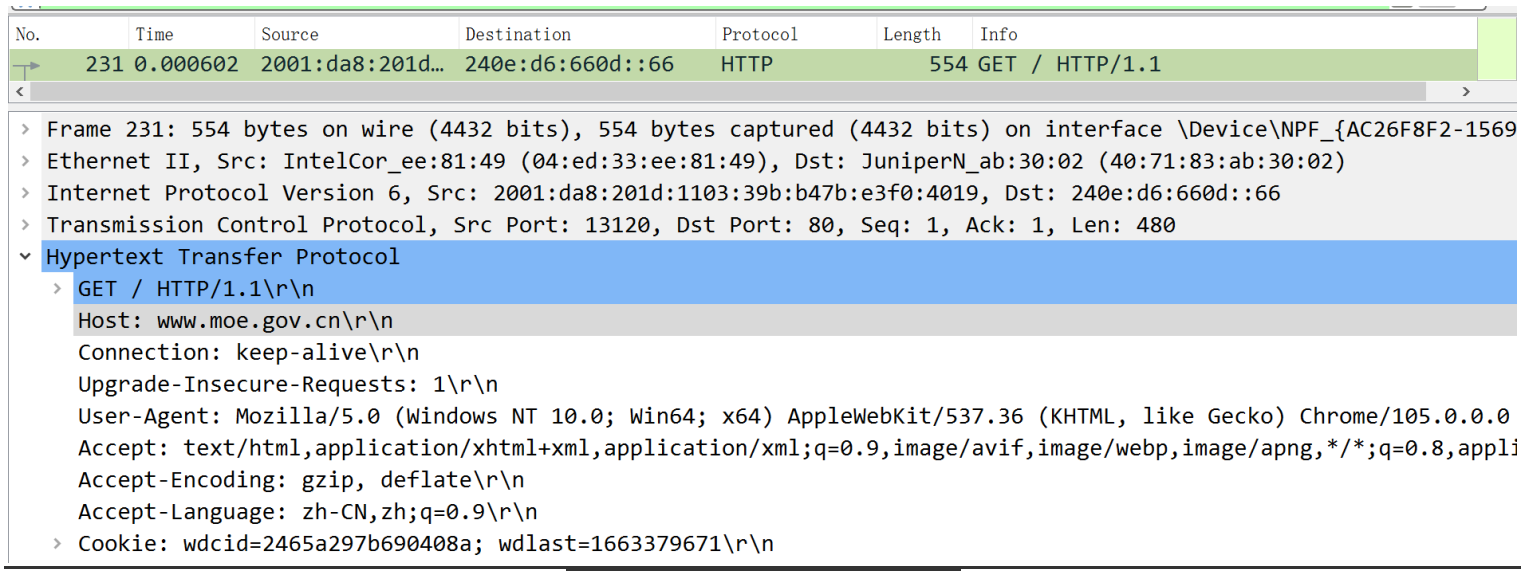
G. ip.addr == 183.232.231.172 or 183.232.231.174

H. ip.addr == 183.232.231.172 and 183.232.231.174

题目 4 of 10

1.0/ 1.0 得分

If we want to show the package in the figure, which expression(s) will not work?



A. http contains www.moe.gov.cn

B. http.request.method == GET

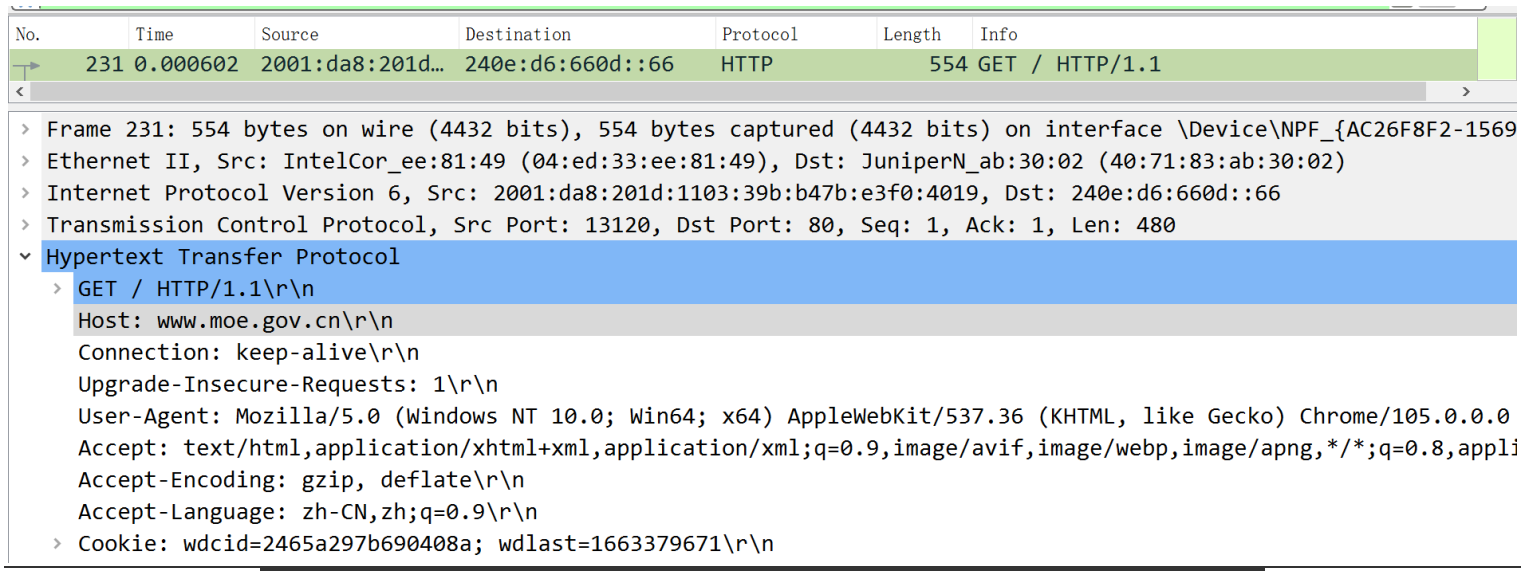
C. http.port == 13120

D. http.host == www.moe.gov.cn

题目 5 of 10

0.0/ 1.0 得分

If we want to show the package in the figure, which expression(s) may work?



No.	Time	Source	Destination	Protocol	Length	Info
231	0.000602	2001:da8:201d…	240e:d6:660d::66	HTTP	554	GET / HTTP/1.1

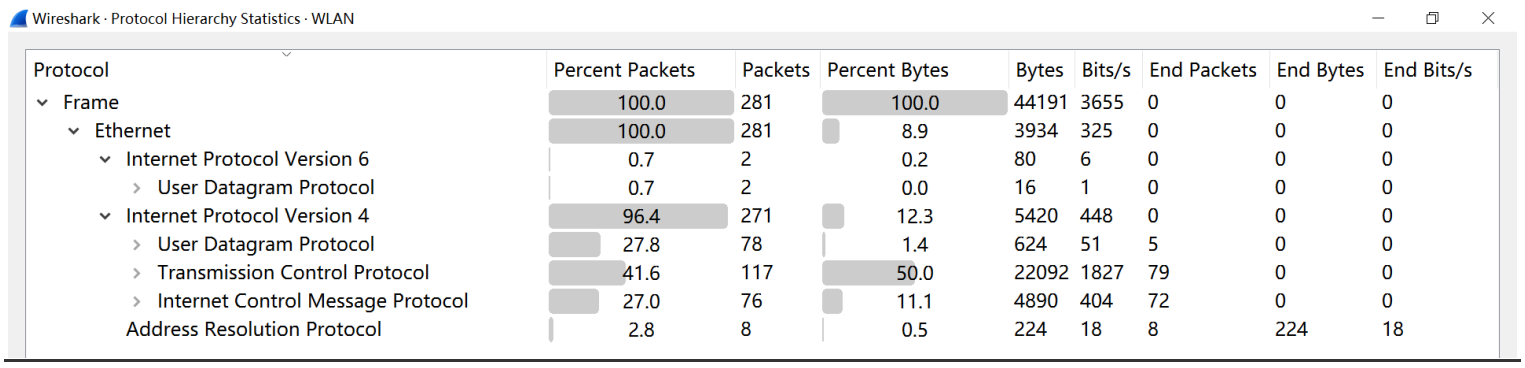
```
Frame 231: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{AC26F8F2-1569
Ethernet II, Src: IntelCor_ee:81:49 (04:ed:33:ee:81:49), Dst: JuniperN_ab:30:02 (40:71:83:ab:30:02)
Internet Protocol Version 6, Src: 2001:da8:201d:1103:39b:b47b:e3f0:4019, Dst: 240e:d6:660d::66
Transmission Control Protocol, Src Port: 13120, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: www.moe.gov.cn\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9\r\n
  Cookie: wdcid=2465a297b690408a; wdlast=1663379671\r\n
```

- [x] A. ipv6.src == 240e:d6:660d::66 && ipv6.dst == 2001:da8:201d:1103:39b:b47b:e3f0:4019
- [ ] B. eth.dst == 40:71:83:ab:30:02 && tcp.len == 554
- [ ] C. ipv6.addr == 240e:d6:660d::66
- [x] D. tcp.dstport == 80

题目 6 of 10

1.0/ 1.0 得分

We have a network data file named quiz2.pcapng, what conclusion can we infer from its protocol hierarchy statistics?



Wireshark · Protocol Hierarchy Statistics · WLAN

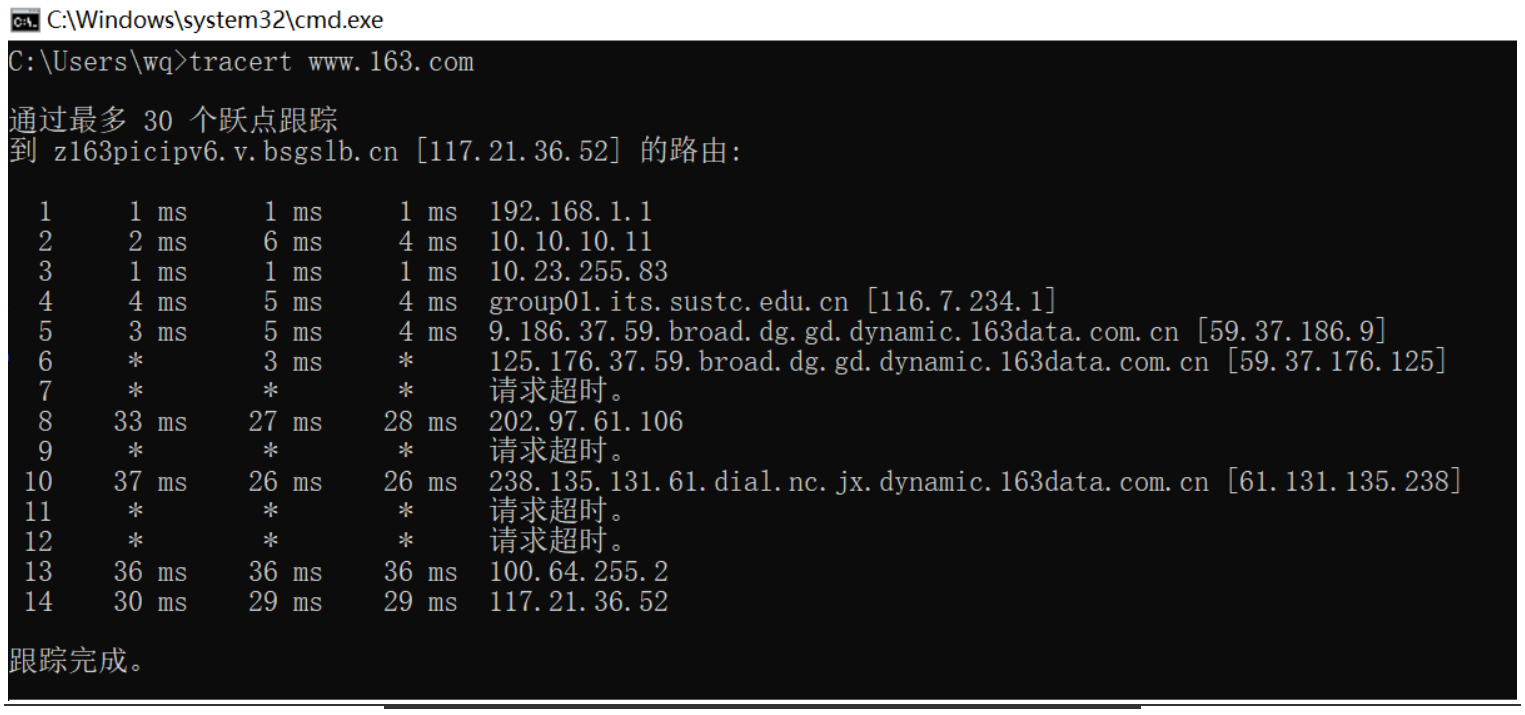
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	281	100.0	44191	3655	0	0	0
Ethernet	100.0	281	8.9	3934	325	0	0	0
Internet Protocol Version 6	0.7	2	0.2	80	6	0	0	0
User Datagram Protocol	0.7	2	0.0	16	1	0	0	0
Internet Protocol Version 4	96.4	271	12.3	5420	448	0	0	0
User Datagram Protocol	27.8	78	1.4	624	51	5	0	0
Transmission Control Protocol	41.6	117	50.0	22092	1827	79	0	0
Internet Control Message Protocol	27.0	76	11.1	4890	404	72	0	0
Address Resolution Protocol	2.8	8	0.5	224	18	8	224	18

- ( ) A. The user must have used “ping” command.
- ( ) B. The user must have used “arp -a” command.
- ( ) C. The user may have used “ipconfig” command.
- (•) D. The user may have used “tracert” command.

题目 7 of 10

0.0/ 1.0 得分

According to the executing result in the figure, which statement(s) is/are correct?

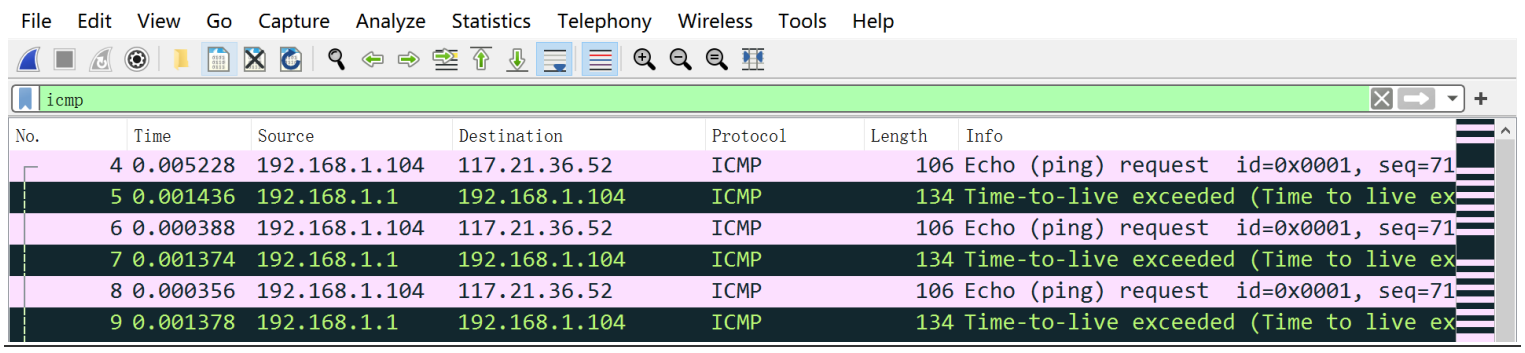


- [x] A. The source endpoint has sent 42 ICMP packages.
- [ ] B. The first “echo reply” message comes from 192.168.1.1.
- [x] C. The first “time-to-live exceed” message comes from 192.168.1.1.
- [ ] D. We can capture exactly 14 “time-to-live exceed” messages.

题目 8 of 10

1.0/ 1.0 得分

The figure shows 6 ICMP packages, what may be the correct TTL field values of the outermost IP layer for each package?

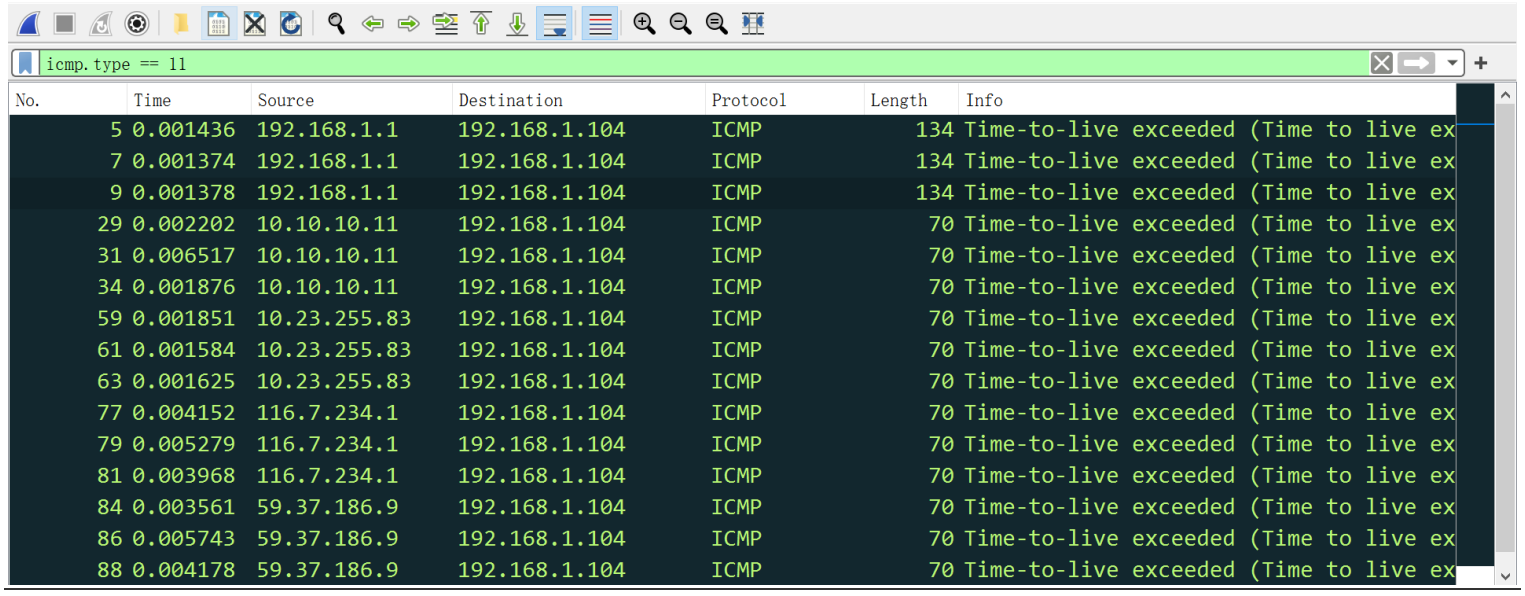


- ( ) A. 64 64 64 64 64 64
- ( ) B. 64 1 64 1 64 1
- (•) C. 1 64 1 64 1 64
- ( ) D. 1 1 1 1 1 1

题目 9 of 10

1.0/ 1.0 得分

The figure shows 15 ICMP packages, what may be the correct TTL field values of the outermost IP layer for each package?



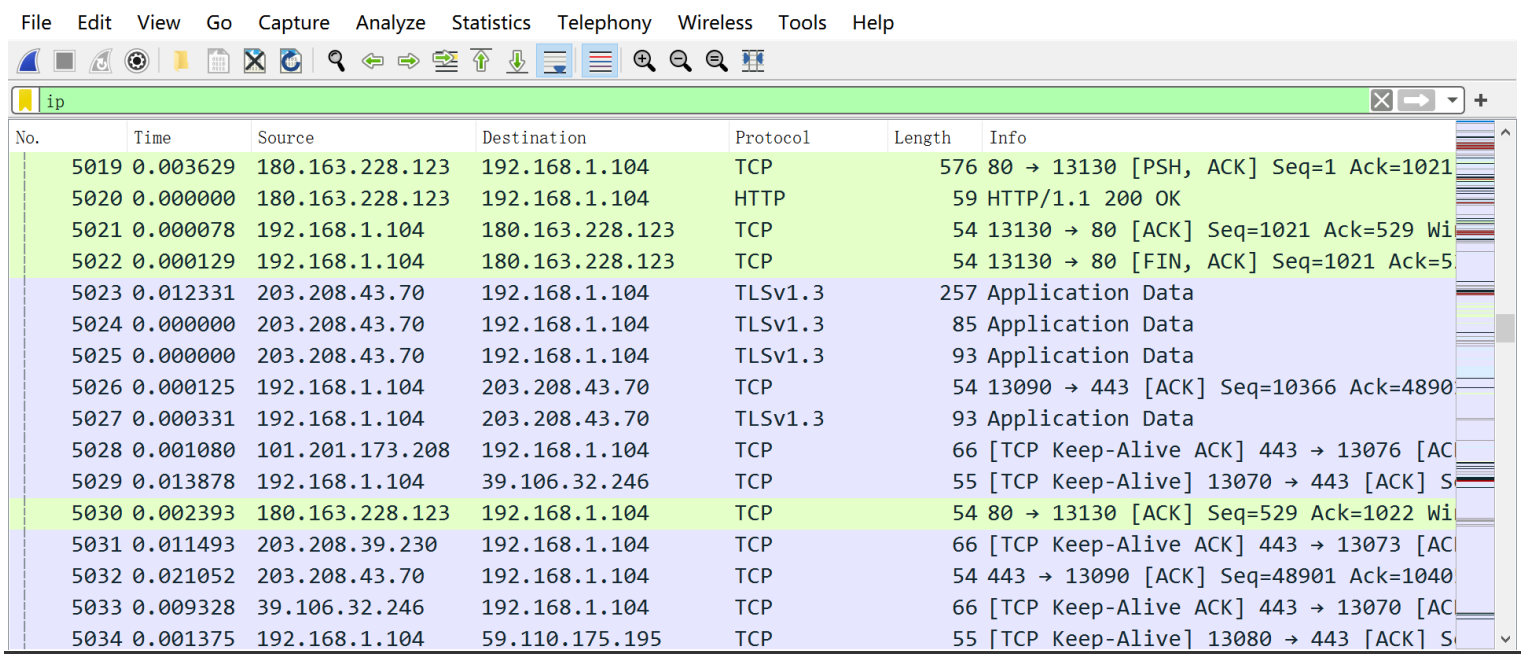
No.	Time	Source	Destination	Protocol	Length	Info
5	0.001436	192.168.1.1	192.168.1.104	ICMP	134	Time-to-live exceeded (Time to live ex
7	0.001374	192.168.1.1	192.168.1.104	ICMP	134	Time-to-live exceeded (Time to live ex
9	0.001378	192.168.1.1	192.168.1.104	ICMP	134	Time-to-live exceeded (Time to live ex
29	0.002202	10.10.10.11	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
31	0.006517	10.10.10.11	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
34	0.001876	10.10.10.11	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
59	0.001851	10.23.255.83	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
61	0.001584	10.23.255.83	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
63	0.001625	10.23.255.83	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
77	0.004152	116.7.234.1	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
79	0.005279	116.7.234.1	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
81	0.003968	116.7.234.1	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
84	0.003561	59.37.186.9	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
86	0.005743	59.37.186.9	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex
88	0.004178	59.37.186.9	192.168.1.104	ICMP	70	Time-to-live exceeded (Time to live ex

- A. 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
- B. 1 1 1 2 2 2 3 3 3 4 4 4 5 5 5
- C. 64 64 64 254 254 254 253 253 253 252 252 252 251 251 251
- D. 64 64 64 254 64 64 64 64 64 64 64 64 64 64 64

题目 10 of 10

1.0/ 1.0 得分

The figure shows some IP packages, which is a HTTPS package, please point its number.



No.	Time	Source	Destination	Protocol	Length	Info
5019	0.003629	180.163.228.123	192.168.1.104	TCP	576	80 → 13130 [PSH, ACK] Seq=1 Ack=1021
5020	0.000000	180.163.228.123	192.168.1.104	HTTP	59	HTTP/1.1 200 OK
5021	0.000078	192.168.1.104	180.163.228.123	TCP	54	13130 → 80 [ACK] Seq=1021 Ack=529 Wi
5022	0.000129	192.168.1.104	180.163.228.123	TCP	54	13130 → 80 [FIN, ACK] Seq=1021 Ack=5
5023	0.012331	203.208.43.70	192.168.1.104	TLSv1.3	257	Application Data
5024	0.000000	203.208.43.70	192.168.1.104	TLSv1.3	85	Application Data
5025	0.000000	203.208.43.70	192.168.1.104	TLSv1.3	93	Application Data
5026	0.000125	192.168.1.104	203.208.43.70	TCP	54	13090 → 443 [ACK] Seq=10366 Ack=4890
5027	0.000331	192.168.1.104	203.208.43.70	TLSv1.3	93	Application Data
5028	0.001080	101.201.173.208	192.168.1.104	TCP	66	[TCP Keep-Alive ACK] 443 → 13076 [AC
5029	0.013878	192.168.1.104	39.106.32.246	TCP	55	[TCP Keep-Alive] 13070 → 443 [ACK] S
5030	0.002393	180.163.228.123	192.168.1.104	TCP	54	80 → 13130 [ACK] Seq=529 Ack=1022 Wi
5031	0.011493	203.208.39.230	192.168.1.104	TCP	66	[TCP Keep-Alive ACK] 443 → 13073 [AC
5032	0.021052	203.208.43.70	192.168.1.104	TCP	54	443 → 13090 [ACK] Seq=48901 Ack=1040
5033	0.009328	39.106.32.246	192.168.1.104	TCP	66	[TCP Keep-Alive ACK] 443 → 13070 [AC
5034	0.001375	192.168.1.104	59.110.175.195	TCP	55	[TCP Keep-Alive] 13080 → 443 [ACK] S

- A. 5020
- B. 5023
- C. 5019
- D. 5021