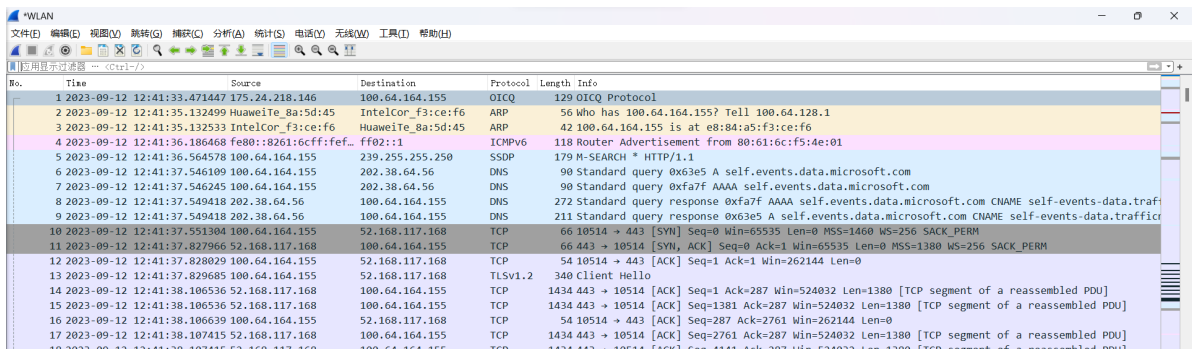


计网实验1

问答

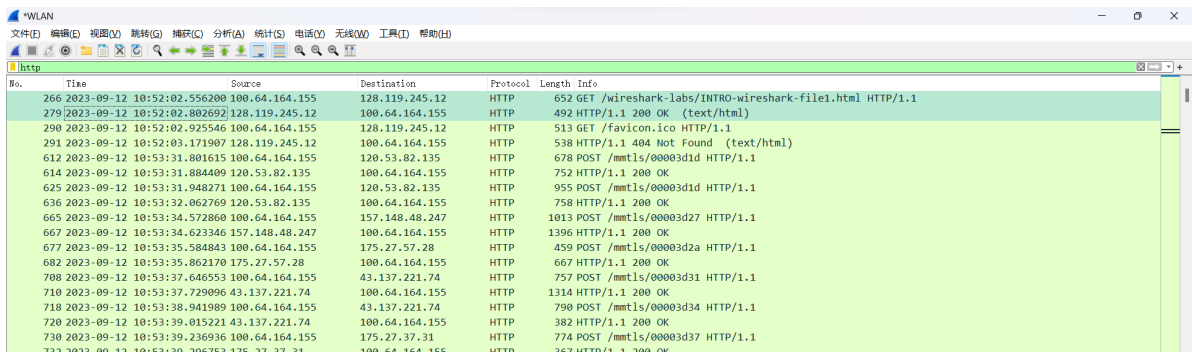
列出上述步骤7中出现在未过滤的分组列表窗口的协议列中的3种不同的协议



No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-12 12:41:33.471447	175.24.218.146	100.64.164.155	ICMP	129	ICMP Protocol
2	2023-09-12 12:41:35.132499	HuaweiTe_8a:5d:45	IntelCor_f3:ce:f6	ARP	56	who has 100.64.164.155? Tell 100.64.128.1
3	2023-09-12 12:41:35.132533	IntelCor_f3:ce:f6	HuaweiTe_8a:5d:45	ARP	42	100.64.164.155 is at e8:84:a5:f3:ce:f6
4	2023-09-12 12:41:36.186468	ff02::1	ff02::1	ICMPv6	118	Router Advertisement from 80:61:6c:f5:4e:01
5	2023-09-12 12:41:36.564578	100.64.164.155	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6	2023-09-12 12:41:37.546109	100.64.164.155	202.38.64.56	DNS	90	Standard query 0x63e5 A self.events.data.microsoft.com
7	2023-09-12 12:41:37.546245	100.64.164.155	202.38.64.56	DNS	90	Standard query 0xfa7f AAAA self.events.data.microsoft.com
8	2023-09-12 12:41:37.549418	202.38.64.56	100.64.164.155	DNS	272	Standard query response 0xfa7f AAAA self.events.data.microsoft.com CNAME self-events-data.traffic
9	2023-09-12 12:41:37.549418	202.38.64.56	100.64.164.155	DNS	211	Standard query response 0x63e5 A self.events.data.microsoft.com CNAME self-events-data.traffic
10	2023-09-12 12:41:37.551304	100.64.164.155	52.168.117.168	TCP	66	10514 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11	2023-09-12 12:41:37.827966	52.168.117.168	100.64.164.155	TCP	66	443 → 10514 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
12	2023-09-12 12:41:37.828029	100.64.164.155	52.168.117.168	TCP	54	10514 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
13	2023-09-12 12:41:37.829685	100.64.164.155	52.168.117.168	TLSv1.2	340	Client Hello
14	2023-09-12 12:41:38.106536	52.168.117.168	100.64.164.155	TCP	1434	443 → 10514 [ACK] Seq=1 Ack=287 Win=524032 Len=1380 [TCP segment of a reassembled PDU]
15	2023-09-12 12:41:38.106536	52.168.117.168	100.64.164.155	TCP	1434	443 → 10514 [ACK] Seq=1381 Ack=287 Win=524032 Len=1380 [TCP segment of a reassembled PDU]
16	2023-09-12 12:41:38.106639	100.64.164.155	52.168.117.168	TCP	54	10514 → 443 [ACK] Seq=287 Ack=2761 Win=262144 Len=0
17	2023-09-12 12:41:38.107415	52.168.117.168	100.64.164.155	TCP	1434	443 → 10514 [ACK] Seq=2761 Ack=287 Win=524032 Len=1380 [TCP segment of a reassembled PDU]
18	2023-09-12 12:41:38.107415	52.168.117.168	100.64.164.155	TCP	1434	443 → 10514 [ACK] Seq=4141 Ack=287 Win=524032 Len=1380 [TCP segment of a reassembled PDU]

从上图中可以看出，列举三种不同协议：ARP、TCP、DNS

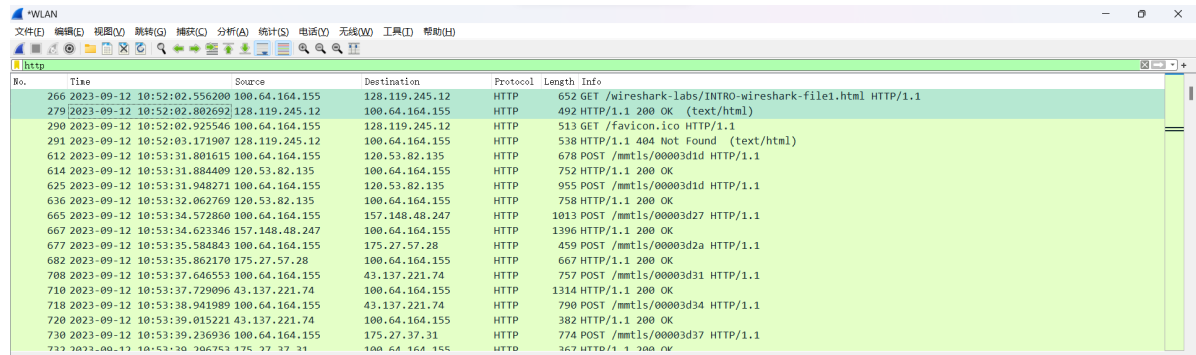
从HTTP GET报文发送到HTTP OK回复需要多长时间？



No.	Time	Source	Destination	Protocol	Length	Info
266	2023-09-12 10:52:02.556200	100.64.164.155	128.119.245.12	HTTP	652	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
279	2023-09-12 10:52:02.802692	128.119.245.12	100.64.164.155	HTTP	492	HTTP/1.1 200 OK (text/html)
290	2023-09-12 10:52:02.925546	100.64.164.155	128.119.245.12	HTTP	513	GET /favicon.ico HTTP/1.1
291	2023-09-12 10:52:03.171907	128.119.245.12	100.64.164.155	HTTP	538	HTTP/1.1 404 Not Found (text/html)
612	2023-09-12 10:53:31.801615	100.64.164.155	128.53.82.135	HTTP	678	POST /mmtls/00003did HTTP/1.1
614	2023-09-12 10:53:31.884409	128.53.82.135	100.64.164.155	HTTP	752	HTTP/1.1 200 OK
625	2023-09-12 10:53:31.948271	100.64.164.155	128.53.82.135	HTTP	955	POST /mmtls/00003did HTTP/1.1
636	2023-09-12 10:53:32.062769	128.53.82.135	100.64.164.155	HTTP	758	HTTP/1.1 200 OK
665	2023-09-12 10:53:34.572860	100.64.164.155	157.140.48.247	HTTP	1013	POST /mmtls/00003d27 HTTP/1.1
667	2023-09-12 10:53:34.623346	157.140.48.247	100.64.164.155	HTTP	1306	HTTP/1.1 200 OK
677	2023-09-12 10:53:35.584843	100.64.164.155	175.27.57.28	HTTP	459	POST /mmtls/00003d2a HTTP/1.1
682	2023-09-12 10:53:35.862170	175.27.57.28	100.64.164.155	HTTP	667	HTTP/1.1 200 OK
708	2023-09-12 10:53:37.646553	100.64.164.155	43.137.221.74	HTTP	757	POST /mmtls/00003d31 HTTP/1.1
710	2023-09-12 10:53:37.729096	43.137.221.74	100.64.164.155	HTTP	1314	HTTP/1.1 200 OK
718	2023-09-12 10:53:38.941989	100.64.164.155	43.137.221.74	HTTP	790	POST /mmtls/00003d34 HTTP/1.1
720	2023-09-12 10:53:39.015221	43.137.221.74	100.64.164.155	HTTP	382	HTTP/1.1 200 OK
730	2023-09-12 10:53:39.236936	100.64.164.155	175.27.37.31	HTTP	774	POST /mmtls/00003d37 HTTP/1.1
733	2023-09-12 10:53:39.306753	175.27.37.31	100.64.164.155	HTTP	367	HTTP/1.1 200 OK

选中两条时间差即为答案，约为0.25s

<http://gaia.cs.umass.edu> (也称为<http://wwwnet.cs.umass.edu>)的Internet地址是什么？您的计算机的Internet地址是什么？



The image shows a Wireshark packet capture window with the filter 'http'. The packet list shows several HTTP requests and responses. The first request (No. 266) is a GET request from 100.64.164.155 to 128.119.245.12. The response (No. 279) is a 200 OK response from 128.119.245.12 to 100.64.164.155. The time difference between these two packets is 0.25 seconds.

No.	Time	Source	Destination	Protocol	Length	Info
266	2023-09-12 10:52:02.556200	100.64.164.155	128.119.245.12	HTTP	652	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
279	2023-09-12 10:52:02.802692	128.119.245.12	100.64.164.155	HTTP	492	HTTP/1.1 200 OK (text/html)

从上图中可以看出，get的发送方是100.64.164.155，接收方是128.119.245.12，<http://gaia.cs.umass.edu>的ip地址是128.119.245.12，我的计算机ip地址是100.64.164.155

打印问题2提到的两个HTTP报文（GET和OK）

见另一份pdf