



# wireshark简介

Wireshark是最流行的网络嗅探器之一，图形界面非常友好，能在多种平台上抓取和分析网络包。在实验中，我们借助Wireshark直观地显示网络细节，在启动该软件后，在浏览器访问学校主页 [www.xjtu.edu.cn](http://www.xjtu.edu.cn)，并通过wireshark软件分析在访问过程中所用到的一些协议及协议细节。

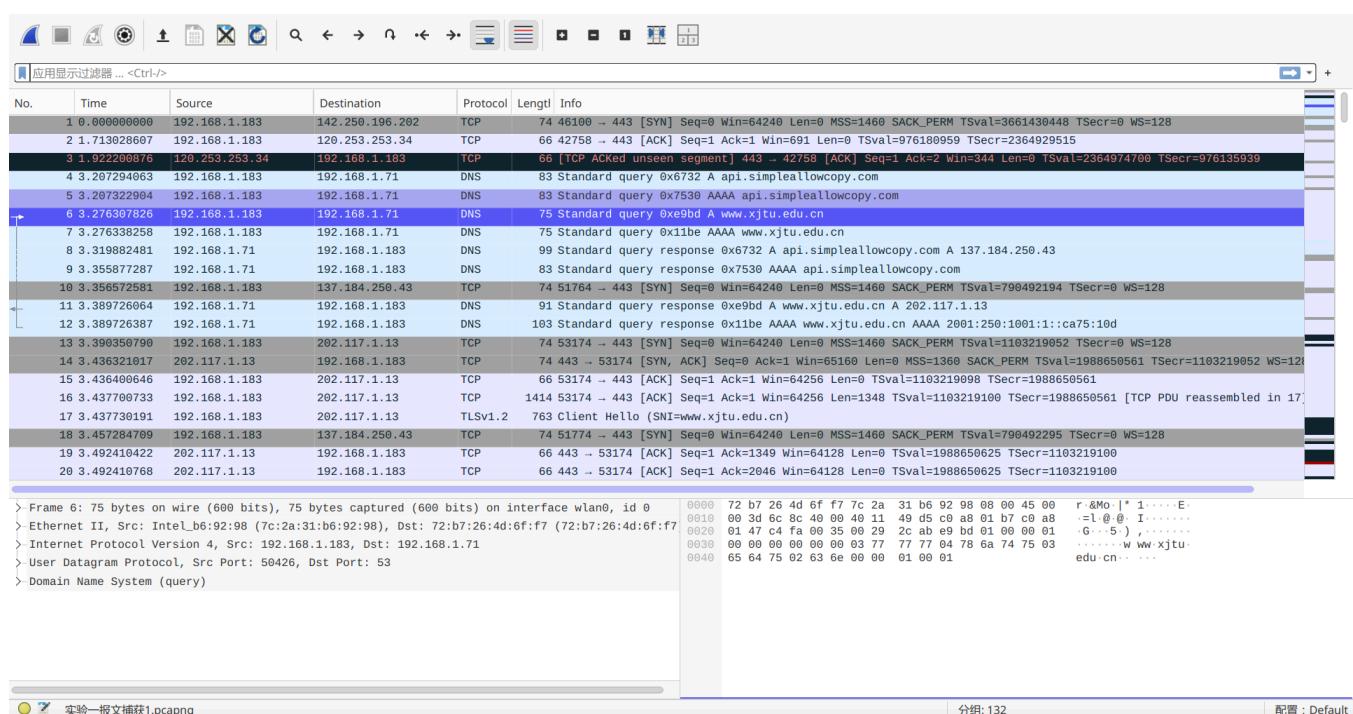
## 捕获报文分析

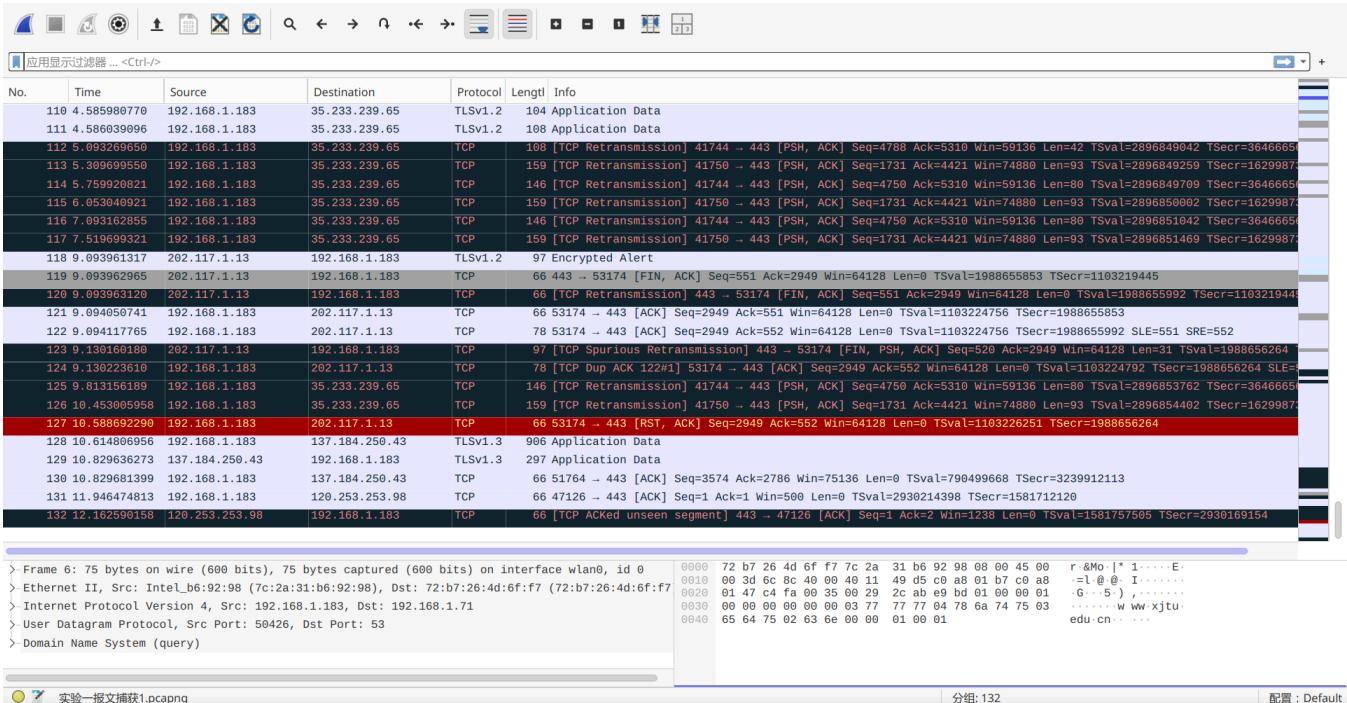
在通过域名 [www.xjtu.edu.cn](http://www.xjtu.edu.cn) 访问学校主页的过程中，网络应用层所使用的是HTTPS协议，而在wireshark软件中，我们无法直接查看到HTTPS的数据内容，而只能看到以TLS/SSL协议出现的加密后的流量，其中只包含TLS握手信息、证书交换、加密算法等，不利于捕获报文的分析。

因此，我选择进行两次报文捕获，第一次直接通过域名访问学校主页，通过访问过程中截获到的报文可以分析HTTPS访问中域名解析、TCP连接建立与释放等过程。在第二次报文捕获中，我通过第一次捕获到的DNS域名解析后的ip地址直接使用HTTP协议访问学校主页，成功捕获到访问过程中HTTP的请求与应答报文。

## HTTPS协议

第一次捕获到的报文结果如图：





由于捕获的报文数目较多，这里仅展示了捕获报文开头与结尾具有代表性的部分。其中，不同类型的报文条目用不同的颜色标识：

- 灰色：TCP报文中SYN连接建立请求报文
- 淡紫色：TCP ACK报文，TLS握手信息报文等
- 黑色：故障报文（超时重发、ACK报文丢失等）
- 青色：DNS域名解析报文
- 红色：RST重置连接报文，这里也表示网页的关闭、意外断开连接等。

考虑到捕获的报文数目过多，而且大部分与所要分析的学校主页访问报文无关，添加过滤器，只显示DNS报文以及与ip地址 202.117.1.13相关的报文信息。截图如下：

No.	Time	Source	Destination	Protocol	Length	Info
4	3.267294063	192.168.1.183	192.168.1.71	DNS	83	Standard query 0x6732 A api.simpleallowcopy.com
5	3.267322994	192.168.1.183	192.168.1.71	DNS	83	Standard query 0x7530 AAAA api.simpleallowcopy.com
6	3.276307826	192.168.1.183	192.168.1.71	DNS	75	Standard query 0xe9bd A www.xjtu.edu.cn
7	3.276338258	192.168.1.183	192.168.1.71	DNS	75	Standard query 0x11be AAAA www.xjtu.edu.cn
8	3.319882481	192.168.1.71	192.168.1.183	DNS	99	Standard query response 0x6732 A api.simpleallowcopy.com A 137.184.250.43
9	3.355877287	192.168.1.71	192.168.1.183	DNS	83	Standard query response 0x7530 AAAA api.simpleallowcopy.com
11	3.389726064	192.168.1.71	192.168.1.183	DNS	91	Standard query response 0xe9bd A www.xjtu.edu.cn A 202.117.1.13
12	3.389726387	192.168.1.71	192.168.1.183	DNS	103	Standard query response 0x11be AAAA www.xjtu.edu.cn AAAA 2001:250:1001:1::ca75:10d
13	3.390350799	192.168.1.183	202.117.1.13	TCP	74	53174 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1103219052 TSecr=0 WS=128
14	3.436321917	202.117.1.13	192.168.1.183	TCP	74	443 - 53174 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1360 SACK_PERM TStamp=1988650561 TSecr=1103219052 WS=128
15	3.436400646	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1103219098 TSecr=1988650561
16	3.437700733	192.168.1.183	202.117.1.13	TCP	1414	53174 - 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1103219100 TSecr=1988650561 [TCP PDU reassembled in 17]
17	3.437730191	192.168.1.183	202.117.1.13	TLSv1.2	763	Client Hello (SNI=www.xjtu.edu.cn)
19	3.492410422	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [ACK] Seq=1 Ack=1349 Win=64128 Len=0 TStamp=1988650625 TSecr=1103219100
20	3.492410768	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [ACK] Seq=1 Ack=2046 Win=64128 Len=0 TStamp=1988650625 TSecr=1103219100
21	3.492410863	202.117.1.13	192.168.1.183	TLSv1.2	222	Server Hello, Change Cipher Spec, Encrypted Handshake Message
22	3.492515781	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=2046 Ack=157 Win=64128 Len=0 TStamp=1103219154 TSecr=1988650626
23	3.493162578	192.168.1.183	202.117.1.13	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
24	3.493557811	192.168.1.183	202.117.1.13	TLSv1.2	918	Application Data
29	3.549074559	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [ACK] Seq=157 Ack=2949 Win=64128 Len=0 TStamp=1988650684 TSecr=1103219155
39	3.739815171	202.117.1.13	192.168.1.183	TLSv1.2	429	Application Data
52	3.743534887	192.168.1.183	192.168.1.71	DNS	80	Standard query 0xc62c A beacons.gcp.gvt2.com
53	3.743550164	192.168.1.183	192.168.1.71	DNS	80	Standard query 0xe12b AAAA beacons.gcp.gvt2.com
54	3.782944653	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=2949 Ack=520 Win=64128 Len=0 TStamp=1103219445 TSecr=1988650852
55	3.793436761	192.168.1.71	192.168.1.183	DNS	152	Standard query response 0xc62e A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com CNAME gce-beacons.gcp
56	3.806036693	192.168.1.71	192.168.1.183	DNS	136	Standard query response 0xc12b AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com CNAME gce-beacons
118	9.093961317	202.117.1.13	192.168.1.183	TLSv1.2	97	Encrypted Alert
119	9.093962965	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [FIN, ACK] Seq=551 Ack=2949 Win=64128 Len=0 TStamp=1988655853 TSecr=1103219445
120	9.093963120	202.117.1.13	192.168.1.183	TCP	66	[TCP Retransmission] 443 - 53174 [FIN, ACK] Seq=551 Ack=2949 Win=64128 Len=0 TStamp=1988655992 TSecr=1103219445
121	9.094058741	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=2949 Ack=551 Win=64128 Len=0 TStamp=1103224756 TSecr=1988655853
122	9.094411765	192.168.1.183	202.117.1.13	TCP	78	53174 - 443 [ACK] Seq=2949 Ack=552 Win=64128 Len=0 TStamp=1103224756 TSecr=1988655992 SLE=551 SRE=552
123	9.130160180	202.117.1.13	192.168.1.183	TCP	97	[TCP Spurious Retransmission] 443 - 53174 [FIN, PSH, ACK] Seq=520 Ack=2949 Win=64128 Len=31 TStamp=1988656264
124	9.130223610	192.168.1.183	202.117.1.13	TCP	78	[TCP Dup ACK 122#] 53174 - 443 [ACK] Seq=2949 Ack=552 Win=64128 Len=0 TStamp=1103224792 TSecr=1988656264 SLE=3
127	10.588692290	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [RST, ACK] Seq=2949 Ack=552 Win=64128 Len=0 TStamp=1103226251 TSecr=1988656264

No.	Time	Source	Destination	Protocol	Length	Info
9	3.355877287	192.168.1.71	192.168.1.183	DNS	83	Standard query response 0x7530 AAAA api.simpleallowcopy.com
11	3.389726064	192.168.1.71	192.168.1.183	DNS	91	Standard query response 0xe9bd A www.xjtu.edu.cn A 202.117.1.13
12	3.389726387	192.168.1.71	192.168.1.183	DNS	103	Standard query response 0x11be AAAA www.xjtu.edu.cn AAAA 2001:250:1001:1::ca75:10d
13	3.390350799	192.168.1.183	202.117.1.13	TCP	74	53174 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1103219052 TSecr=0 WS=128
14	3.436321917	202.117.1.13	192.168.1.183	TCP	74	443 - 53174 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1360 SACK_PERM TStamp=1988650561 TSecr=1103219052 WS=128
15	3.436400646	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1103219098 TSecr=1988650561
16	3.437700733	192.168.1.183	202.117.1.13	TCP	1414	53174 - 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1103219100 TSecr=1988650561 [TCP PDU reassembled in 17]
17	3.437730191	192.168.1.183	202.117.1.13	TLSv1.2	763	Client Hello (SNI=www.xjtu.edu.cn)
19	3.492410422	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [ACK] Seq=1 Ack=1349 Win=64128 Len=0 TStamp=1988650625 TSecr=1103219100
20	3.492410768	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [ACK] Seq=1 Ack=2046 Win=64128 Len=0 TStamp=1988650625 TSecr=1103219100
21	3.492410863	202.117.1.13	192.168.1.183	TLSv1.2	222	Server Hello, Change Cipher Spec, Encrypted Handshake Message
22	3.492515781	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=2046 Ack=157 Win=64128 Len=0 TStamp=1103219154 TSecr=1988650626
23	3.493162578	192.168.1.183	202.117.1.13	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
24	3.493557811	192.168.1.183	202.117.1.13	TLSv1.2	918	Application Data
29	3.549074559	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [ACK] Seq=157 Ack=2949 Win=64128 Len=0 TStamp=1988650684 TSecr=1103219155
39	3.739815171	202.117.1.13	192.168.1.183	TLSv1.2	429	Application Data
52	3.743534887	192.168.1.183	192.168.1.71	DNS	80	Standard query 0xc62c A beacons.gcp.gvt2.com
53	3.743550164	192.168.1.183	192.168.1.71	DNS	80	Standard query 0xe12b AAAA beacons.gcp.gvt2.com
54	3.782944653	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=2949 Ack=520 Win=64128 Len=0 TStamp=1103219445 TSecr=1988650852
55	3.793436761	192.168.1.71	192.168.1.183	DNS	152	Standard query response 0xc62e A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com CNAME gce-beacons.gcp
56	3.806036693	192.168.1.71	192.168.1.183	DNS	136	Standard query response 0xc12b AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com CNAME gce-beacons
118	9.093961317	202.117.1.13	192.168.1.183	TLSv1.2	97	Encrypted Alert
119	9.093962965	202.117.1.13	192.168.1.183	TCP	66	443 - 53174 [FIN, ACK] Seq=551 Ack=2949 Win=64128 Len=0 TStamp=1988655853 TSecr=1103219445
120	9.093963120	202.117.1.13	192.168.1.183	TCP	66	[TCP Retransmission] 443 - 53174 [FIN, ACK] Seq=551 Ack=2949 Win=64128 Len=0 TStamp=1988655992 TSecr=1103219445
121	9.094058741	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [ACK] Seq=2949 Ack=551 Win=64128 Len=0 TStamp=1103224756 TSecr=1988655853
122	9.094411765	192.168.1.183	202.117.1.13	TCP	78	53174 - 443 [ACK] Seq=2949 Ack=552 Win=64128 Len=0 TStamp=1103224756 TSecr=1988655992 SLE=551 SRE=552
123	9.130160180	202.117.1.13	192.168.1.183	TCP	97	[TCP Spurious Retransmission] 443 - 53174 [FIN, PSH, ACK] Seq=520 Ack=2949 Win=64128 Len=31 TStamp=1988656264
124	9.130223610	192.168.1.183	202.117.1.13	TCP	78	[TCP Dup ACK 122#] 53174 - 443 [ACK] Seq=2949 Ack=552 Win=64128 Len=0 TStamp=1103224792 TSecr=1988656264 SLE=3
127	10.588692290	192.168.1.183	202.117.1.13	TCP	66	53174 - 443 [RST, ACK] Seq=2949 Ack=552 Win=64128 Len=0 TStamp=1103226251 TSecr=1988656264

如图所示，图片显示了通过chrome浏览器访问 [www.xjtu.edu.cn](http://www.xjtu.edu.cn) 地址的整个过程。具体的报文协议内容以及TCP连接建立过程将在后续章节分析。

## HTTP协议

在第二次报文捕获过程中，使用地址 <http://202.117.1.13> 直接访问学校主页。在添加过滤器后，

捕获所得报文如下图所示：

No.	Time	Source	Destination	Protocol	Length	Info
19	4.214975308	192.168.1.183	202.117.1.13	TCP	74	40186 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1104852516 TSectr=0 WS=128
20	4.215062693	192.168.1.183	202.117.1.13	TCP	74	40200 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1104852517 TSectr=0 WS=128
22	4.308072808	202.117.1.13	192.168.1.183	TCP	74	80 → 40186 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1360 SACK_PERM TStamp=110485284041 TSectr=1104852516 WS=128
23	4.308120644	192.168.1.183	202.117.1.13	TCP	66	40186 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1104852610 TSectr=110485284041
24	4.312133859	202.117.1.13	192.168.1.183	TCP	74	80 → 40200 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1360 SACK_PERM TStamp=110485284041 TSectr=1104852517 WS=128
25	4.312190748	192.168.1.183	202.117.1.13	TCP	66	40200 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1104852614 TSectr=110485284041
26	4.335179643	192.168.1.183	202.117.1.13	HTTP	561	GET /system/resource/code/dataInput.jsp?owner=1151962237&e=i&w=1536&h=864&treetid=1001&ref=&pagename=L2l90tGV4Lmpzc...
27	4.383203786	202.117.1.13	192.168.1.183	TCP	66	80 → 40186 [ACK] Seq=1 Ack=496 Win=64768 Len=0 TStamp=11048524116 TSectr=1104852637
32	4.476247794	192.168.1.183	192.168.1.71	DNS	91	Standard query 0xc97b A content-autofill.googleapis.com
33	4.476273571	192.168.1.183	192.168.1.71	DNS	91	Standard query 0x3a7c AAAA content-autofill.googleapis.com
34	4.520872464	202.117.1.13	192.168.1.183	HTTP	475	HTTP/1.1 200 OK
35	4.520910130	192.168.1.183	202.117.1.13	TCP	66	40186 → 80 [ACK] Seq=496 Ack=410 Win=63872 Len=0 TStamp=11048528222 TSectr=11048524253
36	4.538132111	192.168.1.71	192.168.1.183	DNS	91	Standard query response 0x3a7c AAAA content-autofill.googleapis.com
37	4.552015924	192.168.1.71	192.168.1.183	DNS	155	Standard query response 0xc97b A content-autofill.googleapis.com A 142.250.77.10 A 142.250.196.202 A 142.250.198.74...
54	5.549719728	192.168.1.183	192.168.1.71	DNS	76	Standard query 0xc11d A mp.weixin.qq.com
55	5.549742512	192.168.1.183	192.168.1.71	DNS	76	Standard query 0x7018 AAAA mp.weixin.qq.com
56	5.554760931	192.168.1.71	192.168.1.183	DNS	189	Standard query response 0xc11d A mp.weixin.qq.com CNAME mpv6.weixin.qq.com CNAME sz.mp.weixin.qq.com A 183.194.204...
57	5.558081676	192.168.1.71	192.168.1.183	DNS	197	Standard query response 0x7018 AAAA mp.weixin.qq.com CNAME mpv6.weixin.qq.com CNAME sz.mp.weixin.qq.com AAAA 2409:8...
59	5.621233850	192.168.1.183	192.168.1.71	DNS	76	Standard query 0x54bf A news.xjtu.edu.cn
60	5.621292838	192.168.1.183	192.168.1.71	DNS	76	Standard query 0xcd1b AAAA news.xjtu.edu.cn
61	5.628581777	192.168.1.183	192.168.1.71	DNS	104	Standard query response 0xcd1b AAAA news.xjtu.edu.cn AAAA 2001:250:1001:9001::cat75:1372
62	5.663386926	192.168.1.183	192.168.1.71	DNS	92	Standard query response 0x54bf A news.xjtu.edu.cn A 202.117.19.114
75	9.302181195	192.168.1.183	202.117.1.13	TCP	66	40200 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1104857604 TSectr=110485284041
76	9.302210670	192.168.1.183	202.117.1.13	TCP	66	40186 → 80 [FIN, ACK] Seq=496 Ack=410 Win=64128 Len=0 TStamp=1104857604 TSectr=110485284253
78	9.353029203	202.117.1.13	192.168.1.183	TCP	66	80 → 40186 [FIN, ACK] Seq=410 Ack=497 Win=64768 Len=0 TStamp=1104857604 TSectr=110485284041
79	9.353077137	192.168.1.183	202.117.1.13	TCP	66	40186 → 80 [ACK] Seq=497 Ack=411 Win=64128 Len=0 TStamp=1104857655 TSectr=1104857604
80	9.358598890	202.117.1.13	192.168.1.183	TCP	66	80 → 40200 [FIN, ACK] Seq=1 Ack=2 Win=65280 Len=0 TStamp=1104857604 TSectr=1104857604
81	9.358628363	192.168.1.183	202.117.1.13	TCP	66	40200 → 80 [ACK] Seq=2 Ack=2 Win=64256 Len=0 TStamp=1104857660 TSectr=1104857604

此时绿色为TCP与HTTP报文，蓝色为DNS域名解析报文。由于第二次捕获报文直接通过ip地址访问，故不需要再通过DNS域名解析服务获得ip地址，此时域名解析服务大部分来自于浏览器及系统其他需求。

由图中可见两次HTTP报文，一次为请求报文，一次为应答报文。详细内容将在后续章节分析。

## 不同协议报文分析

在wireshark捕获后的内容中，任意一个报文项目还可以查看其具体内容，并通过不同层级表示了网络中不同层的信息。下图是一个DNS报文项目的内容：

Frame 32: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlan0, id 0		91 Standard query 0xc97b A content-autofill.googleapis.com	
> Frame 32: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlan0, id 0		0000 72 b7 26 4d f7 7c 2a 31 b6 92 98 08 00 45 00 r.&Mo  * 1 ... E	
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:1b:6:92:98), Dst: 72:b7:26:4d:f7:f7 (72:b7:26:4d:f7:f7)		0010 00 4d 0f 5f 40 00 40 11 a6 f2 c9 a8 b1 b7 c0 a8 .M_@_0  .....	
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.71		0020 01 47 90 63 00 35 00 39 52 c9 7b 01 00 00 01 .G c 5 9 R {....	
> User Datagram Protocol, Src Port: 36963, Dst Port: 53		0030 00 00 00 00 00 10 63 f6 74 65 6e 74 2d 61 .....c ontent-a	
> Domain Name System (query)		0040 75 74 6f 66 69 6c 9a 67 6f 6f 67 6c 65 61 70 utofill. googleap	
		0050 69 73 03 63 6f 6d 00 00 01 00 00 01 is.com. ....	

其中：

- Frame表示物理层的数据帧概况，具体内容如图，其中Frame Number表示帧编号，Frame Length表示帧大小，Interface id则表示了使用的网卡接口。

```

Frame 32: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlan0, id 0
  Section number: 1
  > Interface id: 0 (wlan0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 6, 2024 16:31:40.984657465 CST
  UTC Arrival Time: Dec 6, 2024 08:31:40.984657465 UTC
  Epoch Arrival Time: 1733473900.984657465
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.061919517 seconds]
  [Time delta from previous displayed frame: 0.093044008 seconds]
  [Time since reference or first frame: 4.476247794 seconds]
  Frame Number: 32
  Frame Length: 91 bytes (728 bits)
  Capture Length: 91 bytes (728 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.71

```

- Ethernet II: 数据链路层以太网帧头部信息, 如图, 包含了源与目的的物理地址及上层使用的网络层协议等信息。

```

> Frame 32: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlan0, id 0
< Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
  > Destination: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
  > Source: Intel_b6:92:98 (7c:2a:31:b6:92:98)
  Type: IPv4 (0x0800)
  [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.71
> User Datagram Protocol, Src Port: 36963, Dst Port: 53
> Domain Name System (query)

```

- Internet Protocol Version 4: 采用的网络层协议, 这里是ipv4协议, 同时包含了ipv4协议的各种头部数据, 如源与目的ip地址, 版本号, 头部长度等, 生存时间 (TTL) 值为64, 表示该数据包可以经过最多64个路由器。协议为UDP (17), 说明该IP数据包承载的是UDP协议的数据。头部校验和0x3e84, 用于校验IP头部的完整性。并且此校验和验证在此报文中被禁用。详细内容如图:

```

> Frame 32: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
< Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.71
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 77
  Identification: 0x0f5f (3935)
  > 010. .... = Flags: 0x2, Don't fragment
  ....0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xa6f2 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.183
  Destination Address: 192.168.1.71
  [Stream index: 8]
> User Datagram Protocol, Src Port: 36963, Dst Port: 53
> Domain Name System (query)

```

- User Datagram Protocol: 表示了DNS协议中用到的传输层协议, 在TCP、HTTP报文

中则为则为TCP协议。如图，包含了UDP协议头部信息，如源与目的端口号，长度。其中Checksum为0x52c9表示校验和，但是在这里并没有被检验。

```
> Frame 32: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.71
< User Datagram Protocol, Src Port: 36963, Dst Port: 53
    └─ Source Port: 36963
    └─ Destination Port: 53
    └─ Length: 57
    └─ Checksum: 0x52c9 [unverified]
        └─ [Checksum Status: Unverified]
    └─ [Stream index: 0]
    └─ [Stream Packet Number: 1]
    └─ [Timestamps]
        └─ UDP payload (49 bytes)
> Domain Name System (query)
```

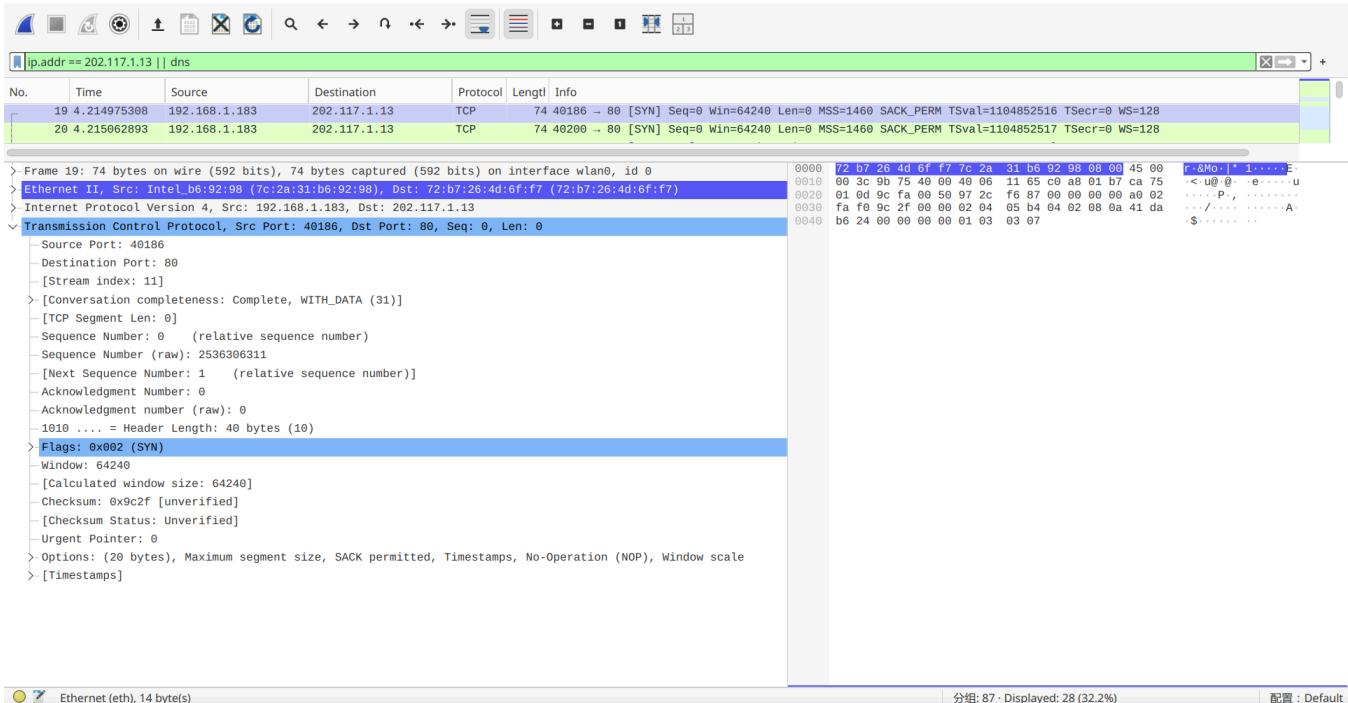
- Domain Name System (query): 表示了应用层的协议，在DNS报文中为DNS协议，在HTTP报文中则为HTTP协议。如下图：

```
> Frame 32: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.71
> User Datagram Protocol, Src Port: 36963, Dst Port: 53
< Domain Name System (query)
    └─ Transaction ID: 0xc97b
    └─ Flags: 0x0100 Standard query
    └─ Questions: 1
    └─ Answer RRs: 0
    └─ Authority RRs: 0
    └─ Additional RRs: 0
    └─ Queries
        └─ [Response In: 37]
```

## TCP

### SYN

如下图为一个TCP SYN报文的协议内容：



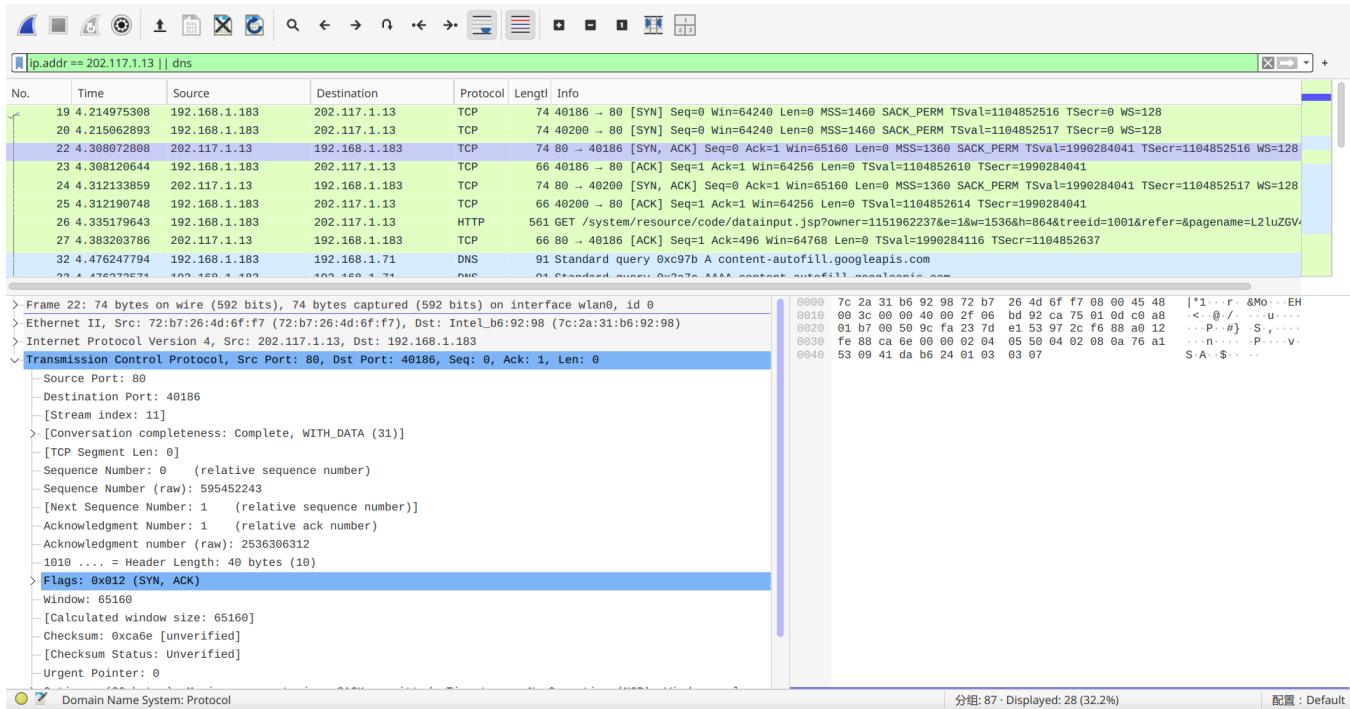
这是一个TCP连接请求包，本地主机（192.168.1.183）向目标服务器（202.117.1.13）的端口80发起连接。其中：

- 时间戳（Time）：4.214975308 — 表示该数据包捕获的时间戳。
- 源IP地址（Source IP）：192.168.1.183 — 表示发送方的IP地址，属于内网。
- 目标IP地址（Destination IP）：202.117.1.13 — 表示接收方的IP地址，属于公网。
- 协议（Protocol）：TCP — 该报文使用TCP协议。
- 报文长度（Length）：74字节 — 该数据包的总大小。
- 源端口（Source Port）：40186 — 这是发送方的源端口。
- 目标端口（Destination Port）：80 — 这是接收方的目标端口，通常为HTTP服务的端口。
- TCP标志（Flags）：[SYN] — 表示该数据包是一个SYN（同步）包，表示这是TCP三次握手的第一步，本地主机请求建立连接。
- 序列号（Seq）：0 — 该数据包的序列号为0。
- 窗口大小（Win）：64240 — 这是接收方的接收窗口大小，表示接收方能够接收的数据量。
- 负载长度（Len）：0 — 该包没有携带数据（SYN包没有有效载荷）。
- 最大报文段大小（MSS）：1460 — 表示接收方希望最大报文段大小为1460字节。
- 选择确认（SACK\_PERM）：表示接收方支持TCP选择性确认（SACK）。
- 时间戳（TStamp）：1104852516 — 这是发送方时间戳，用于TCP的时间戳选项（TS）。

- 时间戳回显 (TSecr) : 0 — 由于这是初始SYN包，因此没有回显的时间戳。
- 窗口缩放因子 (WS) : 128 — 表示接收方的窗口缩放因子，本地主机通过此缩放因子来增加窗口大小。

## [SYN, ACK]

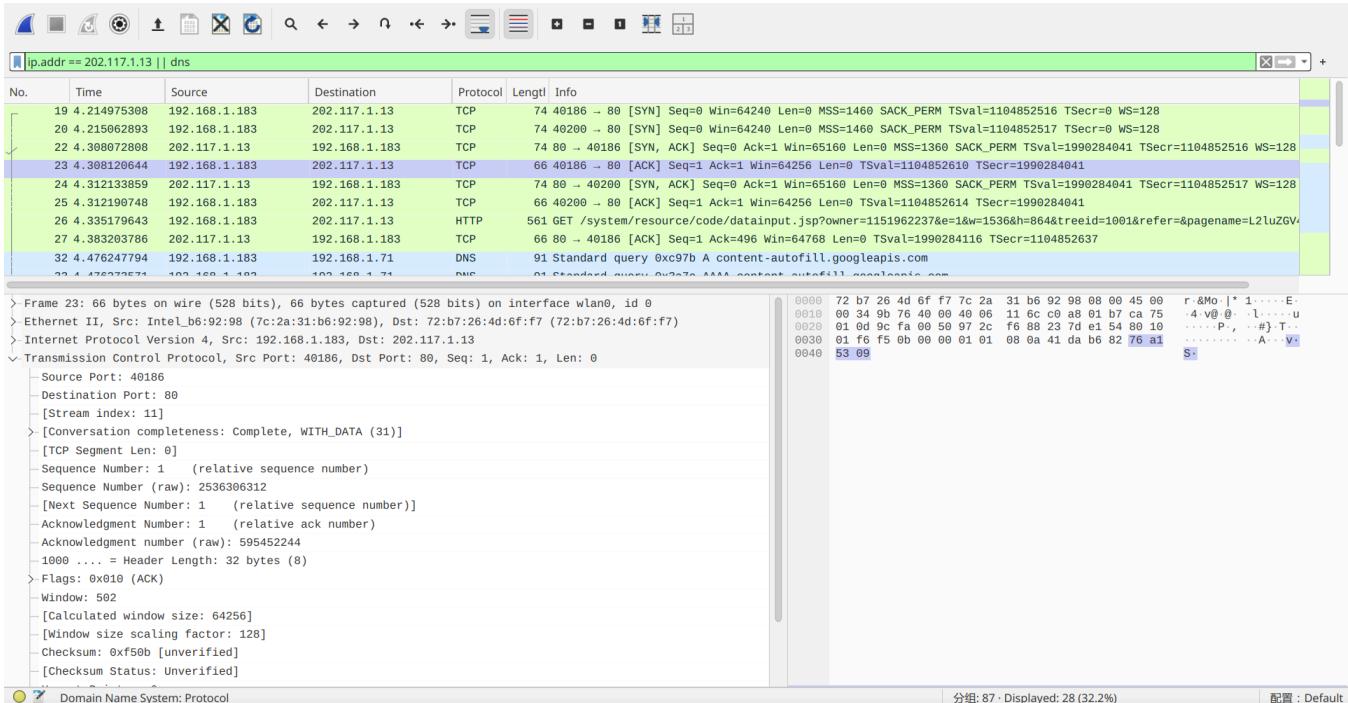
下图为SYN报文的应答报文：



该报文是TCP三次握手的第二步，服务器响应客户端的SYN请求。报文中，序列号 (Seq) 是服务器发送的序列号。确认号 (Ack) 是服务器确认接收到客户端的SYN包，确认号为客户端SYN包的序列号加1。

## ACK

ACK包是对接收到的报文的应答信号，同时也发送了发送方需要发送的数据，如图：



该报文在这里是TCP三次握手的第三步，客户端响应了服务器的SYN、ACK信号，之后TCP连接就正式的建立起来了。

该报文中，在以太网帧头部分指明了源MAC地址和目标MAC地址，在IP头部指明了源ip地址和目标ip地址，在TCP头部则包含以下信息：

- 源端口: 40186 — 发送方的源端口。
- 目标端口: 80 — 接收方的目标端口，与一般的HTTP服务端口相符合。
- 序列号 (Seq) : 1 — 本报文的序列号（相对序列号为1，实际值为2536306312）。
- 确认号 (Ack) : 1 — 本报文的确认号（相对确认号为1，实际值为595452244），表示已成功接收到对方的SYN+ACK包。
- 标志位: 0x010 (ACK) — 这是一个带有确认 (ACK) 标志的TCP包。
- 窗口大小 (Win) : 502 — 发送方的接收窗口大小，表示可以接收的数据量。
- 窗口大小计算值: 64256 — 由于启用了窗口缩放，实际窗口大小为 $502 * 128 = 64256$ 字节。
- 校验和 (Checksum) : 0xf50b — 校验和用于验证数据的完整性。
- 紧急指针 (Urgent Pointer) : 0 — 表示此包没有紧急数据。
- TCP选项:
  - NOP (No-Operation) : 表示填充占位。
  - Timestamps：包含时间戳，用于计算RTT（往返时间）。

## [FIN, ACK]

该报文具体内容如下：

```
> Frame 75: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 202.117.1.13
< Transmission Control Protocol, Src Port: 40200, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 40200
  Destination Port: 80
  [Stream index: 12]
  < [Conversation completeness: Complete, NO_DATA (23)]
  < [TCP Segment Len: 0]
  Sequence Number: 1      (relative sequence number)
  Sequence Number (raw): 2507807721
  [Next Sequence Number: 2      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 2565050866
  1000 .... = Header Length: 32 bytes (8)
  < Flags: 0x011 (FIN, ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x97c8 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  < [Timestamps]
```

在标志位字段除了ACK信号外还附带了FIN标志，出现在TCP连接的终止阶段，标识了TCP连接的关闭过程。发送方（192.168.1.183）发送了一个带有FIN和ACK标志的TCP报文，表示它已完成数据传输，并请求终止连接。之后通过ACK标志确认对方已接收到数据。

## [RST, ACK]

如图：

```

> Frame 127: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 202.117.1.13
< Transmission Control Protocol, Src Port: 53174, Dst Port: 443, Seq: 2949, Ack: 552, Len: 0
  Source Port: 53174
  Destination Port: 443
  [Stream index: 3]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 2949      (relative sequence number)
  Sequence Number (raw): 3494472765
  [Next Sequence Number: 2949      (relative sequence number)]
  Acknowledgment Number: 552      (relative ack number)
  Acknowledgment number (raw): 2666260391
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x014 (RST, ACK)
  Window: 501
  [Calculated window size: 64128]
  [Window size scaling factor: 128]
  Checksum: 0x37f8 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [Timestamps]

```

该Wireshark报文包含一个带有RST（重置连接）和ACK（确认接收数据）标志的TCP报文。客户端（192.168.1.183）向服务器（202.117.1.13）发送了该报文表明它希望重置（关闭）与服务器的连接。这与直接关闭 [www.xjtu.edu.cn](http://www.xjtu.edu.cn) 的网页有关。表明TCP断开连接。

## DNS

下图是捕获到的DNS报文：

6 3.276307826	192.168.1.183	192.168.1.71	DNS	75 Standard query 0xe9bd A www.xjtu.edu.cn
7 3.276338258	192.168.1.183	192.168.1.71	DNS	75 Standard query 0x11be AAAA www.xjtu.edu.cn
8 3.319882481	192.168.1.71	192.168.1.183	DNS	99 Standard query response 0x6732 A api.simplea
9 3.355877287	192.168.1.71	192.168.1.183	DNS	83 Standard query response 0x7530 AAAA api.sim
11 3.389726064	192.168.1.71	192.168.1.183	DNS	91 Standard query response 0xe9bd A www.xjtu.ed

```

> Frame 6: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)
> Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.71
> User Datagram Protocol, Src Port: 50426, Dst Port: 53
< Domain Name System (query)
  Transaction ID: 0xe9bd
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Response In: 11]

```

该报文是DNS查询报文，以太网帧头、IP头部、UDP头部与上述报文差别不大，在DNS部分则包

含以下内容：

- Transaction ID: 0xe9bd 表示该DNS查询的事务ID，用于唯一标识查询请求。
- 标志 (Flags) : 0x0100 Standard query — 表示这是一个标准的查询请求。0x0100表明这是一个普通的查询（非反向查询、非多播查询等）。查询类型为标准查询。
- 问题数量 (Questions) : 1 — 本次DNS查询请求包含一个问题。
- 回答数量 (Answer RRs) : 0 — 由于这是一个查询请求，所以当前没有回答记录。
- 授权数量 (Authority RRs) : 0 — 没有授权记录。
- 附加数量 (Additional RRs) : 0 — 没有附加记录。
- 响应位置: 该DNS查询的响应将在报文11中找到。

## TLS



如图，该报文是一个TLS 1.2的Client Hello消息，表明客户端（192.168.1.183）正在向服务器（202.117.1.13）发起一个安全的TLS连接请求，使用HTTPS（端口443）。其中，第五个条目表示该报文是两个TCP段的重组，一个为1348字节，另一个为697字节。第六个条目是TLS层（Transport Layer Security），具体内容分析如下：

- TLS版本: TLSv1.2 — 表明报文所使用的协议版本。
- 记录层内容：
  - 内容类型: Handshake (22) — 这表明报文的内容是TLS握手协议。

- 版本: TLS 1.0 (0x0301) — 指定TLS协议的版本为1.0。虽然实际使用的是TLS 1.2，但握手中的协商版本通常为1.0。
- 长度: 2040 — 该TLS记录的长度为2040字节。
- 握手协议: Client Hello — 该报文是TLS握手的一部分，表示本地主机发起连接请求。

## HTTP请求与应答报文分析

### GET

	26 4.335179643	192.168.1.183	202.117.1.13	HTTP	561 GET /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1536&h=864&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1	
	27 4.383203786	202.117.1.13	192.168.1.183	TCP	66 80 → 40186 [ACK] Seq=1 Ack=496 Win=64768 Len=0 TSeq=1990284116 TSec=0.000000	
> Frame 26: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface wlan0, id 0						
>- Ethernet II, Src: Intel_b6:92:98 (7c:2a:31:b6:92:98), Dst: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7)						
>- Internet Protocol Version 4, Src: 192.168.1.183, Dst: 202.117.1.13						
>- Transmission Control Protocol, Src Port: 40186, Dst Port: 80, Seq: 1, Ack: 1, Len: 495						
▼ Hypertext Transfer Protocol						
> GET /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1536&h=864&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1						
- Host: 202.117.1.13\r\n						
- Connection: keep-alive\r\n						
- User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/...						
- Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n						
- Referer: http://202.117.1.13/\r\n						
- Accept-Encoding: gzip, deflate\r\n						
- Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n						
- \r\n						
- [Response in frame: 34]						
- [Full request URI: http://202.117.1.13/system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1536&h=864...]						
0040 53 09 47 45 54 20 2f 73 7						
0050 73 6f 75 72 63 65 2f 63 6						
0060 69 6e 70 75 74 2e 6a 73 7						
0070 31 31 35 31 39 36 32 32 3						
0080 3d 31 35 33 36 26 68 3d 3						
0090 69 64 3d 31 30 30 31 26 7						
00a0 61 67 65 6e 61 6d 65 3d 4						
00b0 4c 6d 70 7a 63 41 25 33 4						
00c0 73 69 64 3d 2d 31 20 48 5						
00d0 0a 48 6f 73 74 3a 20 32 3						
00e0 2e 31 33 0d 0a 43 6f 6e 6						
00f0 20 6b 65 65 70 2d 61 6c 6						
0100 72 2d 41 67 65 6e 74 3a 2						
0110 2f 35 2e 30 20 28 58 31 3						
0120 20 78 38 36 5f 36 34 29 2						
0130 62 4b 69 74 2f 35 33 37 2						
0140 4d 4c 2e 29 6c 69 8b 85 2						
0150 43 68 72 6f 6d 65 2f 31 3						
0160 20 53 61 66 61 72 69 2f 3						
0170 41 63 63 65 70 74 3a 20 6						
0180 69 66 2c 69 6d 61 67 65 2						
0190 61 67 65 2f 61 70 6e 67 2						
01a0 76 67 2b 78 6d 6c 2c 69 6						
01b0 2f 2a 3b 71 3d 30 2e 38 0						
01c0 72 3a 20 68 74 74 70 3a 2						

如图为HTTP请求报文，由客户端（192.168.1.183）向学校网站服务器（202.117.1.13）发送。在这个GET请求中，首先指明了请求资源的URL: /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1536&h=864&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1 通过keep-alive参数，表明这是一个持久连接。同时也通过Accept-Encoding和Accept-Language说明了主机的编码方式与偏好的语言。

OK



Frame 34: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface wlan0, id 0  
Ethernet II, Src: 72:b7:26:4d:6f:f7 (72:b7:26:4d:6f:f7), Dst: Intel\_b6:92:98 (7c:2a:31:b6:92:98)  
Internet Protocol Version 4, Src: 202.117.1.13, Dst: 192.168.1.183  
Transmission Control Protocol, Src Port: 80, Dst Port: 40186, Seq: 1, Ack: 496, Len: 409  
HTTP/1.1 200 OK\r\nDate: Fri, 06 Dec 2024 08:31:40 GMT\r\nServer: China Webber /1.1\r\nX-Frame-Options: SAMEORIGIN\r\nCache-Control: no-store\r\nPragma: no-cache\r\nExpires: Thu, 01 Jan 1970 00:00:00 GMT\r\nContent-Type: image/gif; charset=UTF-8\r\nContent-Length: 0\r\nSet-Cookie: JSESSIONID=A52B06BC2AE6F83352DEB607F4ECD5A5; Path=/; HttpOnly\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Language: zh-CN\r\n\r\n[Request in frame: 26]  
[Time since request: 0.185692821 seconds]  
[Request URI: /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1536&h=864&treeid=1001&refer=&pagenumber=1]<br>[Full request URI: http://202.117.1.13/system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1536&h=864&t=1]

该报文是来自服务器的HTTP 200 OK响应，是对上一个客户端请求报文的应答，表示客户端请求成功。服务器返回了一个空的GIF图像（Content-Length为0），并在响应头中包含了一个JSESSIONID cookie，用于会话管理。响应还指示浏览器不缓存内容（Cache-Control: no-store）并通过Keep-Alive保持连接。整个过程表明服务器成功处理了客户端的请求，但没有实际的图像数据返回。

## TCP连接建立报文分析

19 4.214975308	192.168.1.183	202.117.1.13	TCP	74 40186 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1104852516 TSecr=0 WS=128
20 4.215062893	192.168.1.183	202.117.1.13	TCP	74 40200 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1104852517 TSecr=0 WS=128
22 4.308072808	202.117.1.13	192.168.1.183	TCP	74 80 → 40186 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1360 SACK_PERM TStamp=1104852516 WS=128
23 4.308120644	192.168.1.183	202.117.1.13	TCP	66 40186 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1104852610 TSecr=1104852516 WS=128
24 4.312133859	202.117.1.13	192.168.1.183	TCP	74 80 → 40200 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1360 SACK_PERM TStamp=1104852610 TSecr=1104852517 WS=128
25 4.312190748	192.168.1.183	202.117.1.13	TCP	66 40200 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1104852614 TSecr=1104852517 WS=128

如图，图中报文表示了实验过程中访问学校主页时TCP的连接建立过程。由图可见，总共有六条报文，最终建立了两个TCP连接，分别从本地40186和40200端口发出，与目的网站服务器的80端口建立连接。

以40186端口发出的TCP报文为例。在第一条报文中，有本地主机发出SYN报文，指示当前序列号为0,窗口大小为64240,没有确认号。在[SYN, ACK]报文中，目的服务器应答了本地主机的SYN报文，通过Seq指明序列号为0,Ack为1表示收到了本地主机的序列号为0的报文，期望收到序列号为1的报文。最后，本地服务器发出ACK报文，Seq为1,Ack为1，表示收到了服务器发来的确认信号，TCP连接正式建立，并期望从服务器收到序列号为1的报文。

# TCP连接释放报文分析

75 9.302181195	192.168.1.183	202.117.1.13	TCP	66 40200 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1104857604 TSecr=1990284041
76 9.302210670	192.168.1.183	202.117.1.13	TCP	66 40186 → 80 [FIN, ACK] Seq=496 Ack=410 Win=64128 Len=0 TSval=1104857604 TSecr=1990284253
78 9.353029203	202.117.1.13	192.168.1.183	TCP	66 80 → 40186 [FIN, ACK] Seq=410 Ack=497 Win=64768 Len=0 TSval=1990289086 TSecr=1104857604
79 9.353077137	192.168.1.183	202.117.1.13	TCP	66 40186 → 80 [ACK] Seq=497 Ack=411 Win=64128 Len=0 TSval=1104857655 TSecr=1990289086
80 9.358598890	202.117.1.13	192.168.1.183	TCP	66 80 → 40200 [FIN, ACK] Seq=1 Ack=2 Win=65280 Len=0 TSval=1990289087 TSecr=1104857604
81 9.358628363	192.168.1.183	202.117.1.13	TCP	66 40200 → 80 [ACK] Seq=2 Ack=2 Win=64256 Len=0 TSval=1104857660 TSecr=1990289087

如图为TCP连接释放时的报文信息，同样为六条报文，同时终止了两个TCP连接。以本地端口号为40200的TCP连接为例。

本地主机首先向服务器发出FIN断开连接请求报文，同时也使用ACK标志应答了已经接收到的报文，其中，序列号为1,ACK为1。目的服务器在收到本地主机发来的断开连接请求报文后，发出应答报文ACK,此时序列号为1,响应了本地主机的上一条报文，ACK为2表明已收到序列号为1的报文，期望收到序列号为2的报文。此外，该报文除了要应答本地主机的FIN报文外，同时也添加了服务器端的FIN信号，表明服务器的终止连接意愿。最终，本地主机应答了服务器的FIN报文，此时序列号为2,ACK为2,表明成功收到服务器序列号为1的FIN报文，之后40200与服务器80端口的TCP连接成功断开连接。