浙江大學

本科实验报告

课程名称：计算机网络基础

姓　　名：杨凯

学　　院：计算机学院

专　　业：软件工程

学　　号：3130000495

指导教师：张泉方

2015 年　11 月　16 日

浙江大学实验报告

课程名称：　计算机网络基础　　　　实验类型：　综合性实验

实验项目名称：　网络协议分析

学生姓名：　杨凯　　专业：　软件工程　　学号：3130000495

同组学生姓名：＿＿＿＿＿＿　　指导老师：　张泉方

实验地点：＿＿＿＿＿＿　　实验日期：2015 年 11 月 16 日

一、实验目的和要求

使用包捕获软件捕获网络中的数据包，了解和学习常见网络应用和协议交互过程、数据包格式等

二、实验内容和原理

安装网络包捕获软件，观察网络中的数据包

三、主要仪器设备

Wireshark 软件、联网的 PC 机

四、操作方法和实验步骤

a) 安装网络包捕获软件 Ethereal

b) 配置网络包捕获软件,捕获所有机器的数据包

c) 观察捕获到的数据包,并对照解析结果和原始数据包,了解你捕获到了哪些类型的数据包,每种类型的数据包对应到什么协议,每种数据包的格式

大致如何。

d) 配置网络包捕获软件,只捕获特定 IP 或特定类型的包

e) 跟踪一次 HTTP 会话,用浏览器打开一个网页,学习浏览器和 Web 服务器之间是如何通信的

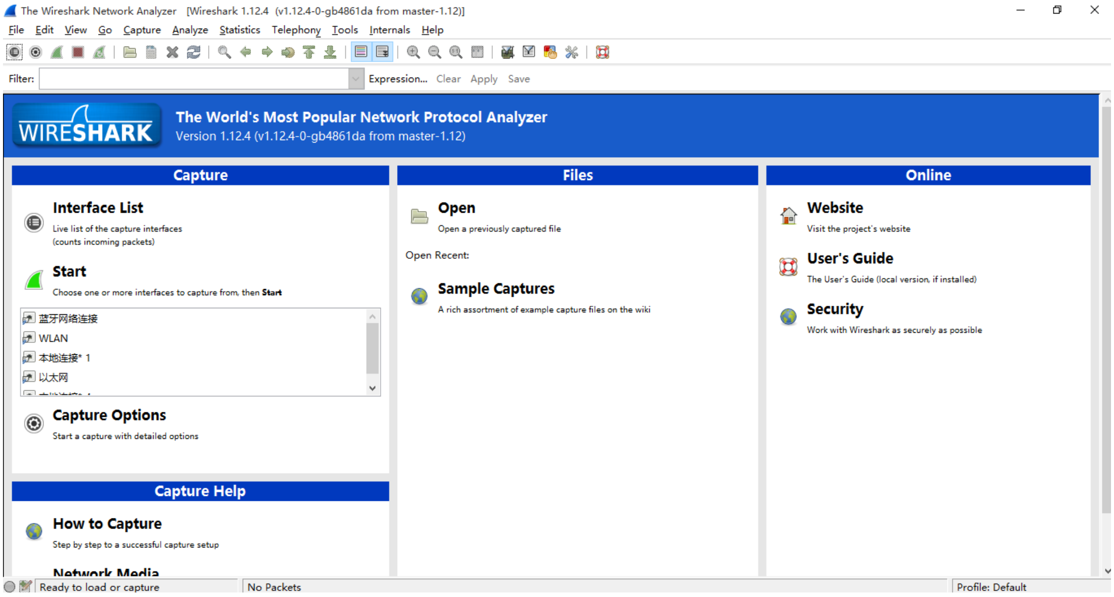
f) 跟踪一次 FTP 会话,用 FTP 工具下载一个文件,学习 FTP 工具和 FTP 服务器之间是如何传递文件的

g) 跟踪一次 SMTP 会话,用 Outlook 发送一封邮件,学习邮件是如何传递到服务器的

五、实验数据记录与处理

5.1 使用 Wireshark 软件

1.运行抓包软件 Wireshark



The World's Most Popular Network Protocol Analyzer
Version 1.12.4 (v1.12.4-0-gb4861da from master-1.12)

Live list of the capture interfaces (counts incoming packets)

Choose one or more interfaces to capture from, then **Start**

Start a capture with detailed options

Step by step to a successful capture setup

Open a previously captured file

A rich assortment of example capture files on the wiki

Visit the project's website

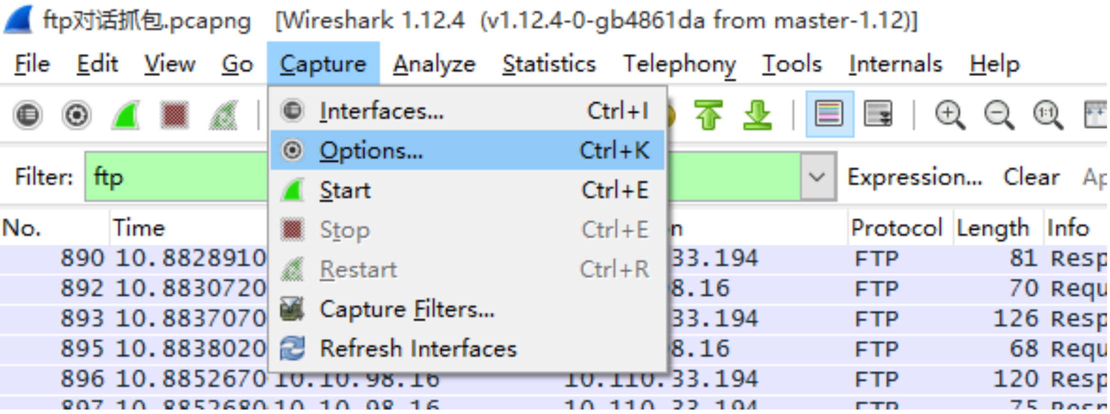
The User's Guide (local version, if installed)

Work with Wireshark as securely as possible

Ready to load or capture

No Packets

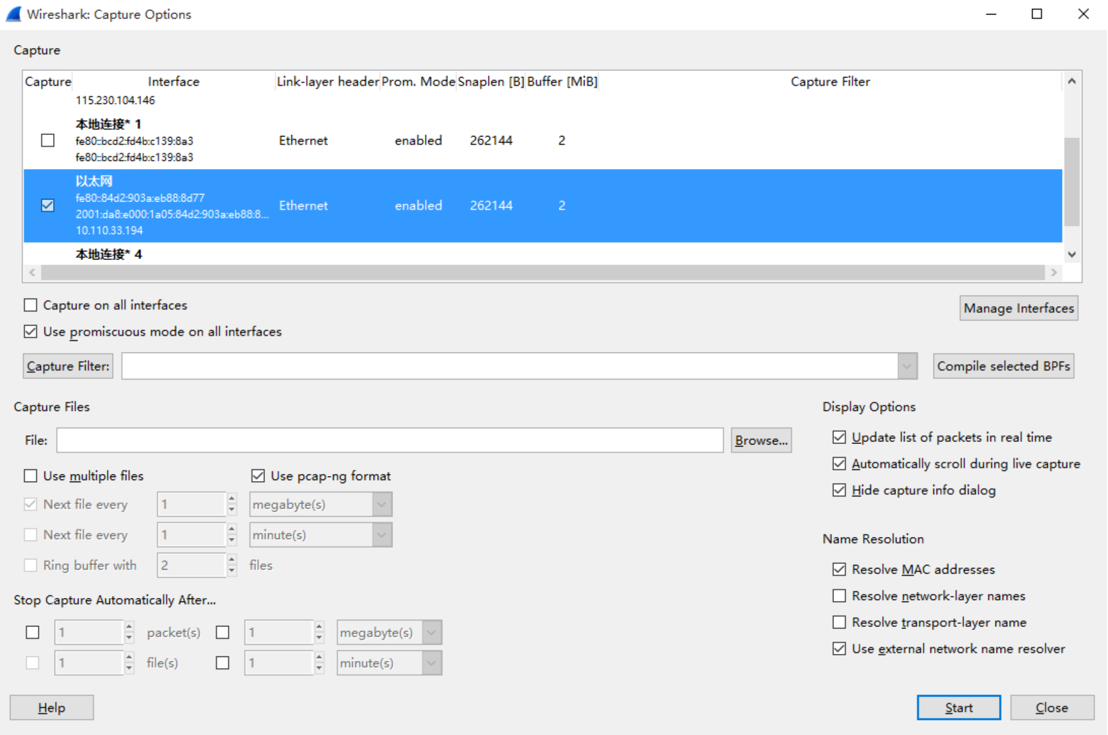
2.点击 Capture->Option


ftp对话抓包.pcapng [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces
Expression... Clear Ap

Filter: ftp

```
No.   Time                     n         Protocol Length Info
  890 10.8828910            33.194       FTP        81 Resp
  892 10.8830720            8.16         FTP        70 Requ
  893 10.8837070            33.194       FTP       126 Resp
  895 10.8838020            8.16         FTP        68 Requ
  896 10.8852670 10.10.98.16  10.110.33.194  FTP   120 Resp
```

3.设置想要抓包的网卡，和抓包的协议类型，点击 start 开始抓包


Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
	115.230.104.146					
□	**本地连接* 1** fe80::bcd2:fd4b:c139:8a3 fe80::bcd2:fd4b:c139:8a3	Ethernet	enabled	262144	2	
☑	**以太网** fe80::84d2:903a:eb88:8d77 2001:da8:e000:1a05:84d2:903a:eb88:8... 10.110.33.194	Ethernet	enabled	262144	2	
	本地连接* 4					

□ Capture on all interfaces

☑ Use promiscuous mode on all interfaces

Capture Filter:

Capture Files

File:

□ Use multiple files ☑ Use pcap-ng format

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

□ Ring buffer with 2 files

Stop Capture Automatically After...

□ 1 packet(s) □ 1 megabyte(s)

□ 1 file(s) □ 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatically scroll during live capture

☑ Hide capture info dialog

Name Resolution

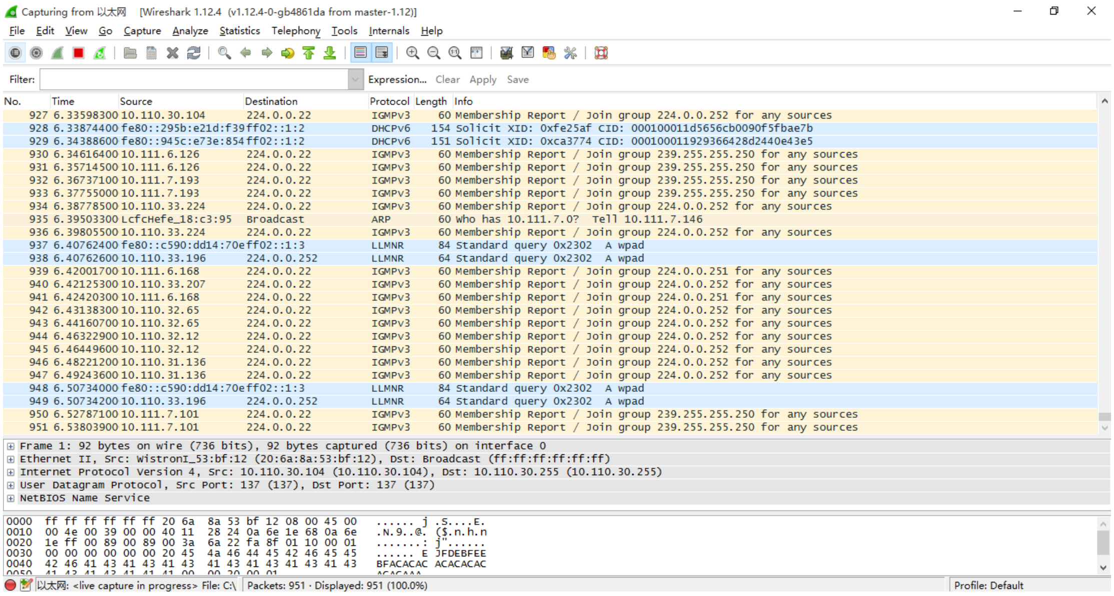
☑ Resolve MAC addresses

□ Resolve network-layer names

□ Resolve transport-layer name

☑ Use external network name resolver

3.不设置 filter，默认抓取所有类型的数据包

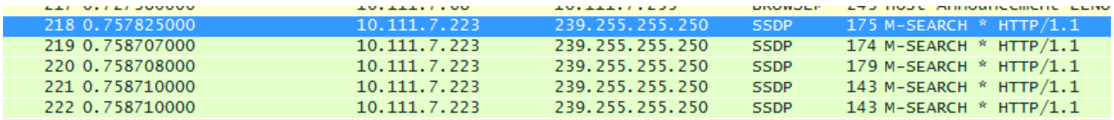

Capturing from 以太网 [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time       Source                Destination  Protocol Length Info
  927 6.33598300 10.110.30.104         224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  928 6.33874400 fe80::295b:e21d:f39ff02::1:2       DHCPv6   154 Solicit XID: 0xfe25af CID: 000100011d5656cb0090f5fbae7b
  929 6.34388600 fe80::945c:e73e:854ff02::1:2       DHCPv6   151 Solicit XID: 0xca3774 CID: 00010001192936642 8d2440e43e5
  930 6.34616400 10.111.6.126          224.0.0.22   IGMPv3    60 Membership Report / Join group 239.255.255.250 for any sources
  931 6.35714500 10.111.6.126          224.0.0.22   IGMPv3    60 Membership Report / Join group 239.255.255.250 for any sources
  932 6.36737100 10.111.7.193          224.0.0.22   IGMPv3    60 Membership Report / Join group 239.255.255.250 for any sources
  933 6.37755000 10.111.7.193          224.0.0.22   IGMPv3    60 Membership Report / Join group 239.255.255.250 for any sources
  934 6.38778500 10.110.33.224         224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  935 6.39503300 LcfcHefe_18:c3:95     Broadcast    ARP       60 Who has 10.111.7.0?  Tell 10.111.7.146
  936 6.39805500 10.110.33.224         224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  937 6.40762400 fe80::c590:dd14:70eff02::1:3       LLMNR     84 Standard query 0x2302  A wpad
  938 6.40762600 10.110.33.196         224.0.0.252  LLMNR     64 Standard query 0x2302  A wpad
  939 6.42001700 10.111.6.168          224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.251 for any sources
  940 6.42125300 10.110.33.207         224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  941 6.42420300 10.111.6.168          224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.251 for any sources
  942 6.43138300 10.110.32.65          224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  943 6.44160700 10.110.32.65          224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  944 6.46322900 10.110.32.12          224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  945 6.46449600 10.110.32.12          224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  946 6.48221200 10.110.31.136         224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  947 6.49243600 10.110.31.136         224.0.0.22   IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
  948 6.50734000 fe80::c590:dd14:70eff02::1:3       LLMNR     84 Standard query 0x2302  A wpad
  949 6.50734200 10.110.33.196         224.0.0.252  LLMNR     64 Standard query 0x2302  A wpad
  950 6.52787100 10.111.7.101          224.0.0.22   IGMPv3    60 Membership Report / Join group 239.255.255.250 for any sources
  951 6.53803900 10.111.7.101          224.0.0.22   IGMPv3    60 Membership Report / Join group 239.255.255.250 for any sources

⊞ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
⊞ Ethernet II, Src: WistronI_53:bf:12 (20:6a:8a:53:bf:12), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 10.110.30.104 (10.110.30.104), Dst: 10.110.30.255 (10.110.30.255)
⊞ User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
⊞ NetBIOS Name Service

0000  ff ff ff ff ff ff 20 6a  8a 53 bf 12 08 00 45 00   ...... j .S....E.
0010  00 4e 00 39 00 00 40 11  28 24 0a 6e 1e 68 0a 6e   .N.9..@. ($.n.h.n
0020  1e ff 00 89 00 89 00 3a  6a 22 fa 8f 01 10 00 01   .......: j"......
0030  00 00 00 00 00 00 20 45  4a 46 44 45 42 46 45 45   ...... E JFDEBFEE
0040  42 46 41 43 41 43 41 43  41 43 41 43 41 43 41 43   BFACACAC ACACACAC

以太网: <live capture in progress> File: C:\   Packets: 951 · Displayed: 951 (100.0%)   Profile: Default
```

5.2 抓包分析

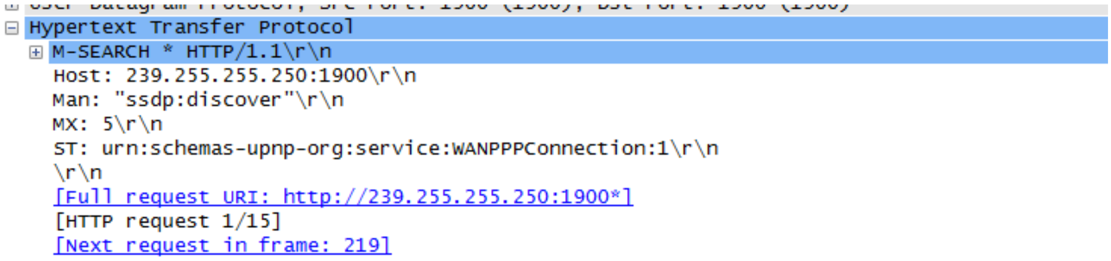
1.SSDP

简单服务发现协议，提供了在局域网络内部发现设备机制



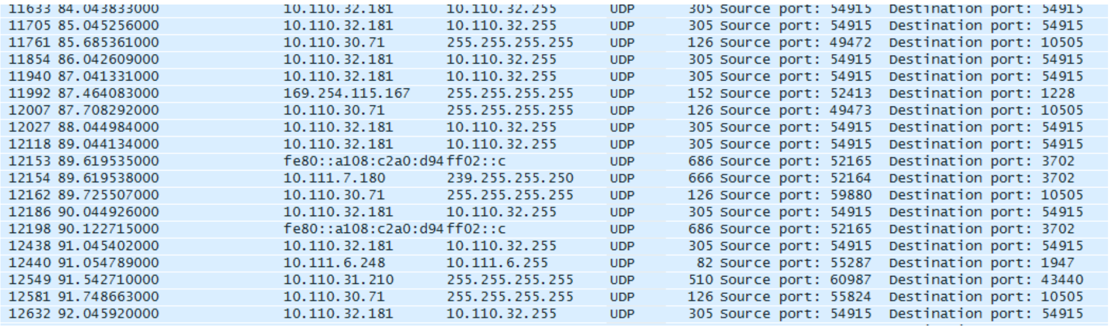
```
218 0.757825000     10.111.7.223     239.255.255.250    SSDP     175 M-SEARCH * HTTP/1.1
219 0.758707000     10.111.7.223     239.255.255.250    SSDP     174 M-SEARCH * HTTP/1.1
220 0.758708000     10.111.7.223     239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
221 0.758710000     10.111.7.223     239.255.255.250    SSDP     143 M-SEARCH * HTTP/1.1
222 0.758710000     10.111.7.223     239.255.255.250    SSDP     143 M-SEARCH * HTTP/1.1
```

数据包结构



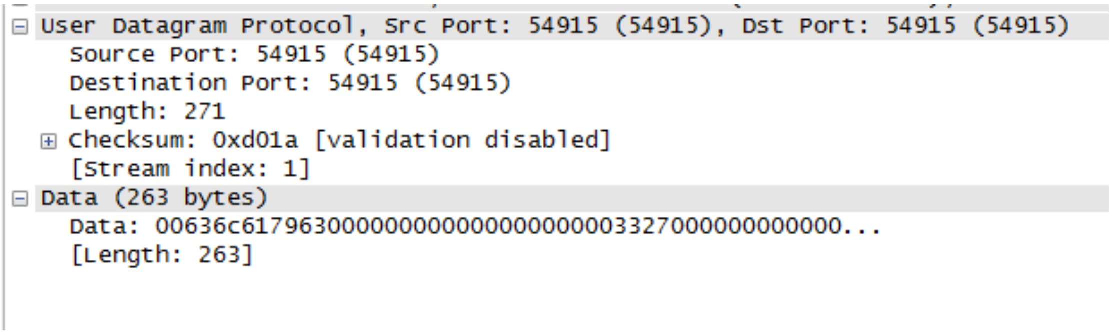
```
⊟ Hypertext Transfer Protocol
  ⊞ M-SEARCH * HTTP/1.1\r\n
    Host: 239.255.255.250:1900\r\n
    Man: "ssdp:discover"\r\n
    MX: 5\r\n
    ST: urn:schemas-upnp-org:service:WANPPPConnection:1\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 1/15]
    [Next request in frame: 219]
```

2.UDP 协议



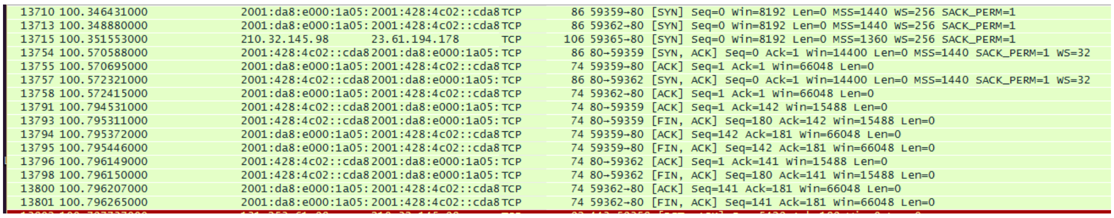
```
11633 84.043833000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
11705 85.045256000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
11761 85.685361000    10.110.30.71         255.255.255.255    UDP    126 Source port: 49472  Destination port: 10505
11854 86.042609000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
11940 87.041331000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
11992 87.464083000    169.254.115.167      255.255.255.255    UDP    152 Source port: 52413  Destination port: 1228
12007 87.708292000    10.110.30.71         255.255.255.255    UDP    126 Source port: 49473  Destination port: 10505
12027 88.044984000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
12118 89.044134000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
12153 89.619535000    fe80::a108:c2a0:d94 ff02::c             UDP    686 Source port: 52165  Destination port: 3702
12154 89.619538000    10.111.7.180         239.255.255.250    UDP    666 Source port: 52164  Destination port: 3702
12162 89.725507000    10.110.30.71         255.255.255.255    UDP    126 Source port: 59880  Destination port: 10505
12186 90.044926000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
12198 90.122715000    fe80::a108:c2a0:d94 ff02::c             UDP    686 Source port: 52165  Destination port: 3702
12438 91.045402000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
12440 91.054789000    10.111.6.248         10.111.6.255       UDP     82 Source port: 55287  Destination port: 1947
12549 91.542710000    10.110.31.210        255.255.255.255    UDP    510 Source port: 60987  Destination port: 43440
12581 91.748663000    10.110.30.71         255.255.255.255    UDP    126 Source port: 55824  Destination port: 10505
12632 92.045920000    10.110.32.181        10.110.32.255      UDP    305 Source port: 54915  Destination port: 54915
```

数据包结构



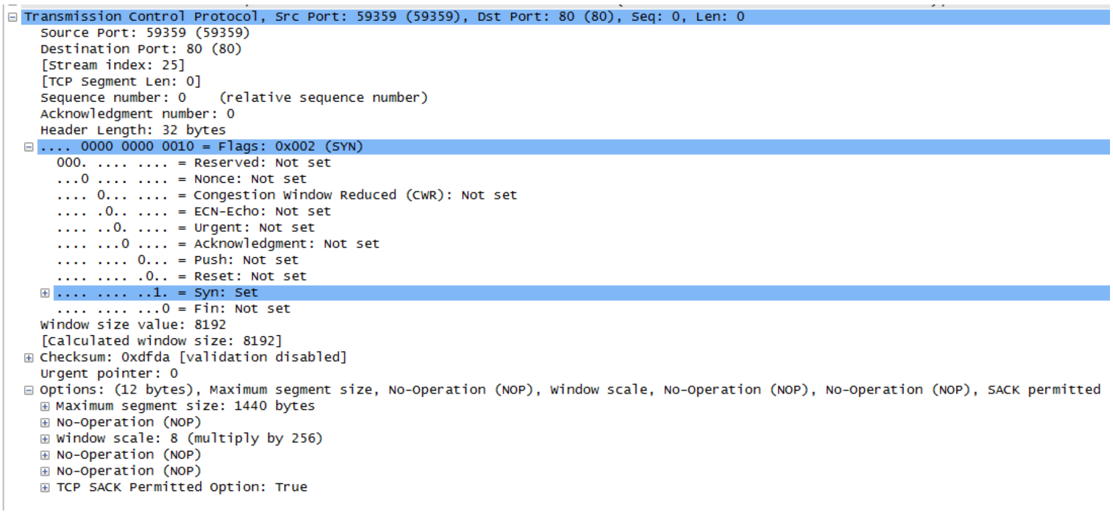
```
⊟ User Datagram Protocol, Src Port: 54915 (54915), Dst Port: 54915 (54915)
    Source Port: 54915 (54915)
    Destination Port: 54915 (54915)
    Length: 271
  ⊞ Checksum: 0xd01a [validation disabled]
    [Stream index: 1]
⊟ Data (263 bytes)
    Data: 00636c6179630000000000000000000003327000000000000...
    [Length: 263]
```

3.TCP 协议



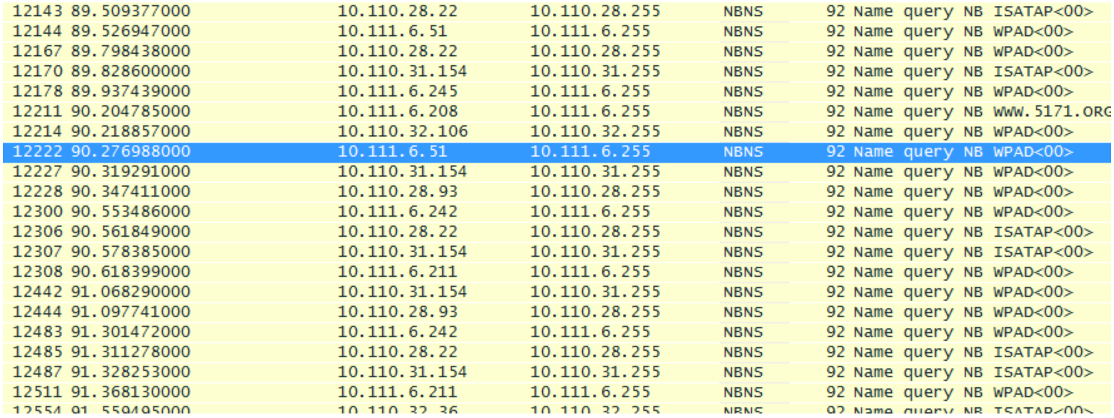
```
13710 100.346431000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     86 59359→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
13713 100.348880000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     86 59362→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
13715 100.351553000    210.32.145.98       23.61.194.178       TCP    106 59365→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=256 SACK_PERM=1
13754 100.570588000    2001:428:4c02::cda8 2001:da8:e000:1a05: TCP     86 80→59359 [SYN, ACK] Seq=0 Ack=1 Win=14400 Len=0 MSS=1440 SACK_PERM=1 WS=32
13755 100.570695000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     74 59359→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
13757 100.572321000    2001:428:4c02::cda8 2001:da8:e000:1a05: TCP     86 80→59362 [SYN, ACK] Seq=0 Ack=1 Win=14400 Len=0 MSS=1440 SACK_PERM=1 WS=32
13758 100.572415000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     74 59362→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
13791 100.794531000    2001:428:4c02::cda8 2001:da8:e000:1a05: TCP     74 80→59359 [ACK] Seq=1 Ack=142 Win=15488 Len=0
13793 100.795311000    2001:428:4c02::cda8 2001:da8:e000:1a05: TCP     74 80→59359 [FIN, ACK] Seq=180 Ack=142 Win=15488 Len=0
13794 100.795372000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     74 59359→80 [ACK] Seq=142 Ack=181 Win=66048 Len=0
13795 100.795446000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     74 59359→80 [FIN, ACK] Seq=142 Ack=181 Win=66048 Len=0
13796 100.796149000    2001:428:4c02::cda8 2001:da8:e000:1a05: TCP     74 80→59362 [ACK] Seq=1 Ack=141 Win=15488 Len=0
13798 100.796150000    2001:428:4c02::cda8 2001:da8:e000:1a05: TCP     74 80→59362 [FIN, ACK] Seq=180 Ack=141 Win=15488 Len=0
13800 100.796207000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     74 59362→80 [ACK] Seq=141 Ack=181 Win=66048 Len=0
13801 100.796265000    2001:da8:e000:1a05: 2001:428:4c02::cda8 TCP     74 59362→80 [FIN, ACK] Seq=141 Ack=181 Win=66048 Len=0
```

数据包结构



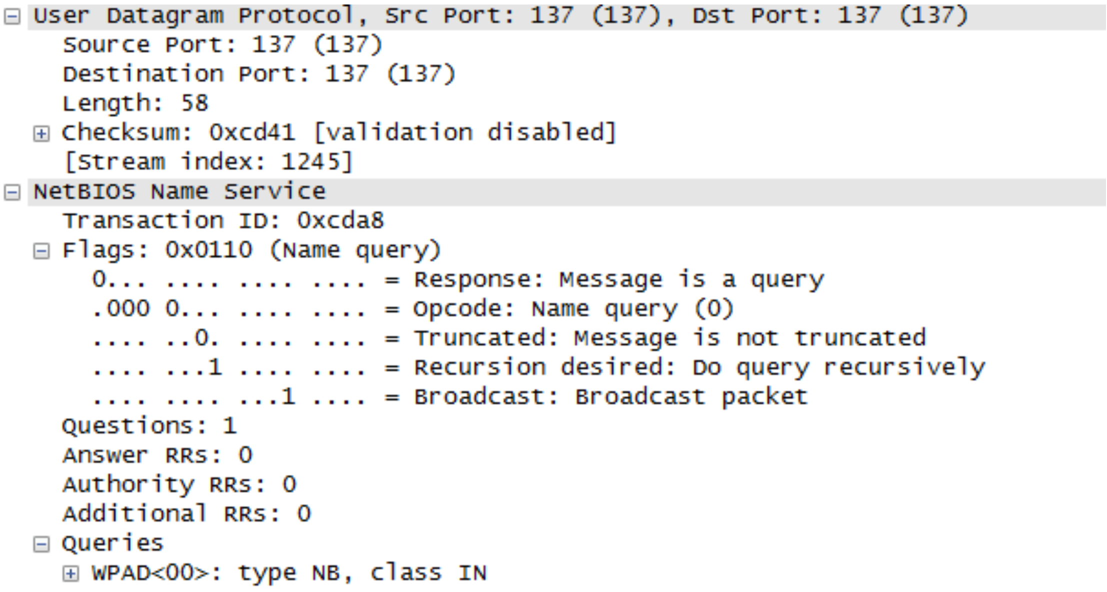
```
⊟ Transmission Control Protocol, Src Port: 59359 (59359), Dst Port: 80 (80), Seq: 0, Len: 0
    Source Port: 59359 (59359)
    Destination Port: 80 (80)
    [Stream index: 25]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
  ⊟ .... 0000 0000 0010 = Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ⊞ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
    Window size value: 8192
    [Calculated window size: 8192]
  ⊞ Checksum: 0xdfda [validation disabled]
    Urgent pointer: 0
  ⊟ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    ⊞ Maximum segment size: 1440 bytes
    ⊞ No-Operation (NOP)
    ⊞ Window scale: 8 (multiply by 256)
    ⊞ No-Operation (NOP)
    ⊞ No-Operation (NOP)
    ⊞ TCP SACK Permitted Option: True
```

4.NBNS 协议



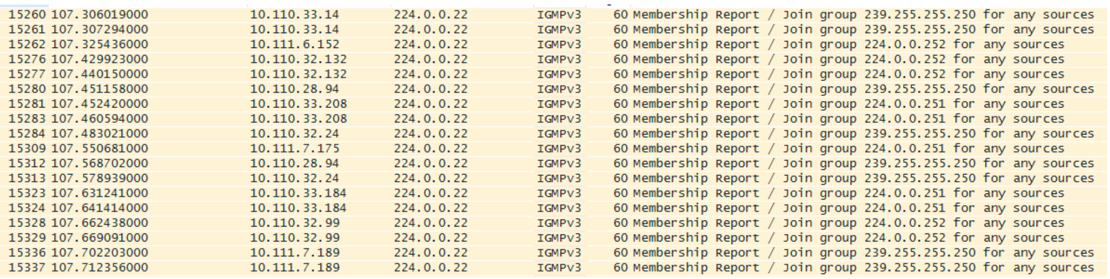
```
12143 89.509377000        10.110.28.22     10.110.28.255    NBNS    92 Name query NB ISATAP<00>
12144 89.526947000        10.111.6.51      10.111.6.255     NBNS    92 Name query NB WPAD<00>
12167 89.798438000        10.110.28.22     10.110.28.255    NBNS    92 Name query NB WPAD<00>
12170 89.828600000        10.110.31.154    10.110.31.255    NBNS    92 Name query NB ISATAP<00>
12178 89.937439000        10.111.6.245     10.111.6.255     NBNS    92 Name query NB WPAD<00>
12211 90.204785000        10.111.6.208     10.111.6.255     NBNS    92 Name query NB WWW.5171.ORG
12214 90.218857000        10.110.32.106    10.110.32.255    NBNS    92 Name query NB WPAD<00>
12222 90.276988000        10.111.6.51      10.111.6.255     NBNS    92 Name query NB WPAD<00>
12227 90.319291000        10.110.31.154    10.110.31.255    NBNS    92 Name query NB WPAD<00>
12228 90.347411000        10.110.28.93     10.110.28.255    NBNS    92 Name query NB WPAD<00>
12300 90.553486000        10.111.6.242     10.111.6.255     NBNS    92 Name query NB WPAD<00>
12306 90.561849000        10.110.28.22     10.110.28.255    NBNS    92 Name query NB ISATAP<00>
12307 90.578385000        10.110.31.154    10.110.31.255    NBNS    92 Name query NB ISATAP<00>
12308 90.618399000        10.111.6.211     10.111.6.255     NBNS    92 Name query NB WPAD<00>
12442 91.068290000        10.110.31.154    10.110.31.255    NBNS    92 Name query NB WPAD<00>
12444 91.097741000        10.110.28.93     10.110.28.255    NBNS    92 Name query NB WPAD<00>
12483 91.301472000        10.111.6.242     10.111.6.255     NBNS    92 Name query NB WPAD<00>
12485 91.311278000        10.110.28.22     10.110.28.255    NBNS    92 Name query NB ISATAP<00>
12487 91.328253000        10.110.31.154    10.110.31.255    NBNS    92 Name query NB ISATAP<00>
12511 91.368130000        10.111.6.211     10.111.6.255     NBNS    92 Name query NB WPAD<00>
12554 91.559495000        10.110.32.36     10.110.32.255    NBNS    92 Name query NB ISATAP<00>
```

数据包结构



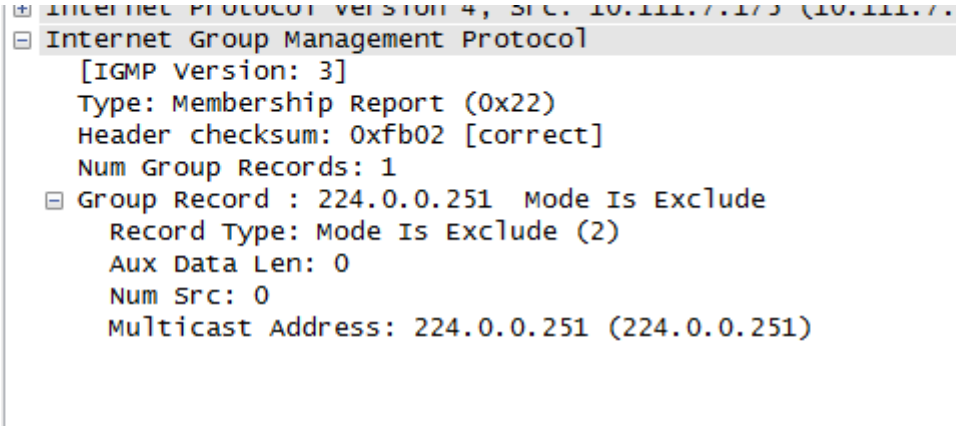
```
⊟ User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
    Source Port: 137 (137)
    Destination Port: 137 (137)
    Length: 58
  ⊞ Checksum: 0xcd41 [validation disabled]
    [Stream index: 1245]
⊟ NetBIOS Name Service
    Transaction ID: 0xcda8
  ⊟ Flags: 0x0110 (Name query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Name query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... ...1 .... = Broadcast: Broadcast packet
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ WPAD<00>: type NB, class IN
```

5. IGMPv3 协议



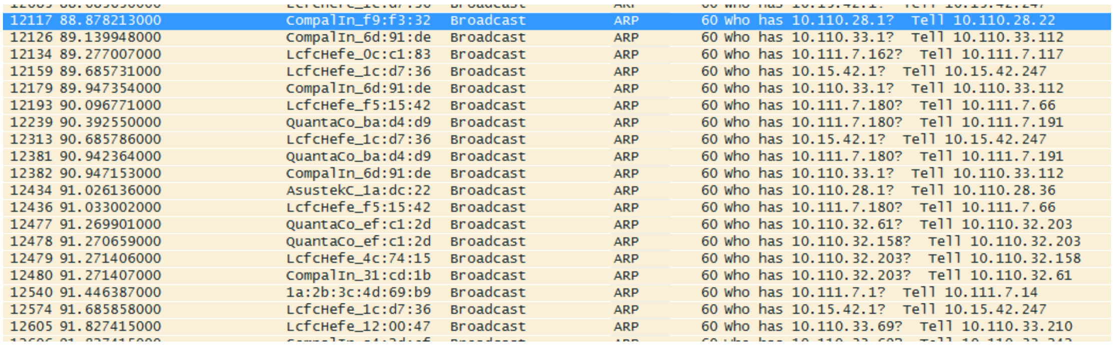
```
15260 107.306019000   10.110.33.14    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
15261 107.307294000   10.110.33.14    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
15262 107.325436000   10.111.6.152    224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
15276 107.429923000   10.110.32.132   224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
15277 107.440150000   10.110.32.132   224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
15280 107.451158000   10.110.28.94    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
15281 107.452420000   10.110.33.208   224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
15283 107.460594000   10.110.33.208   224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
15284 107.483021000   10.110.32.24    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
15309 107.550681000   10.111.7.175    224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
15312 107.568702000   10.110.28.94    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
15313 107.578939000   10.110.32.24    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
15323 107.631241000   10.110.33.184   224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
15324 107.641414000   10.110.33.184   224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
15328 107.662438000   10.110.32.99    224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
15329 107.669091000   10.110.32.99    224.0.0.22   IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
15336 107.702203000   10.111.7.189    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
15337 107.712356000   10.111.7.189    224.0.0.22   IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
```

数据包结构



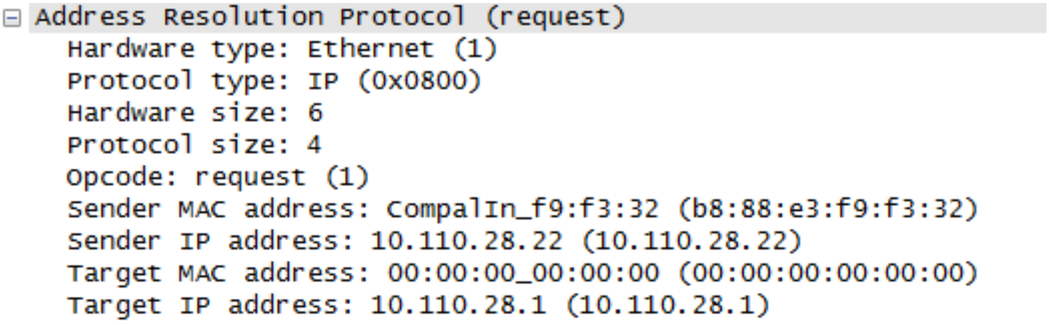
```
⊞ Internet Protocol Version 4, Src: 10.111.7.175 (10.111.7.
⊟ Internet Group Management Protocol
    [IGMP Version: 3]
    Type: Membership Report (0x22)
    Header checksum: 0xfb02 [correct]
    Num Group Records: 1
  ⊟ Group Record : 224.0.0.251  Mode Is Exclude
      Record Type: Mode Is Exclude (2)
      Aux Data Len: 0
      Num Src: 0
      Multicast Address: 224.0.0.251 (224.0.0.251)
```

6.ARP 协议



```
12117 88.878213000   CompalIn_f9:f3:32   Broadcast   ARP   60 Who has 10.110.28.1?  Tell 10.110.28.22
12126 89.139948000   CompalIn_6d:91:de   Broadcast   ARP   60 Who has 10.110.33.1?  Tell 10.110.33.112
12134 89.277007000   LcfcHefe_0c:c1:83   Broadcast   ARP   60 Who has 10.111.7.162?  Tell 10.111.7.117
12159 89.685731000   LcfcHefe_1c:d7:36   Broadcast   ARP   60 Who has 10.15.42.1?  Tell 10.15.42.247
12179 89.947354000   CompalIn_6d:91:de   Broadcast   ARP   60 Who has 10.110.33.1?  Tell 10.110.33.112
12193 90.096771000   LcfcHefe_f5:15:42   Broadcast   ARP   60 Who has 10.111.7.180?  Tell 10.111.7.66
12239 90.392550000   QuantaCo_ba:d4:d9   Broadcast   ARP   60 Who has 10.111.7.180?  Tell 10.111.7.191
12313 90.685786000   LcfcHefe_1c:d7:36   Broadcast   ARP   60 Who has 10.15.42.1?  Tell 10.15.42.247
12381 90.942364000   QuantaCo_ba:d4:d9   Broadcast   ARP   60 Who has 10.111.7.180?  Tell 10.111.7.191
12382 90.947153000   CompalIn_6d:91:de   Broadcast   ARP   60 Who has 10.110.33.1?  Tell 10.110.33.112
12434 91.026136000   AsustekC_1a:dc:22   Broadcast   ARP   60 Who has 10.110.28.1?  Tell 10.110.28.36
12436 91.033002000   LcfcHefe_f5:15:42   Broadcast   ARP   60 Who has 10.111.7.180?  Tell 10.111.7.66
12477 91.269901000   QuantaCo_ef:c1:2d   Broadcast   ARP   60 Who has 10.110.32.61?  Tell 10.110.32.203
12478 91.270659000   QuantaCo_ef:c1:2d   Broadcast   ARP   60 Who has 10.110.32.158?  Tell 10.110.32.203
12479 91.271406000   LcfcHefe_4c:74:15   Broadcast   ARP   60 Who has 10.110.32.203?  Tell 10.110.32.158
12480 91.271407000   CompalIn_31:cd:1b   Broadcast   ARP   60 Who has 10.110.32.203?  Tell 10.110.32.61
12540 91.446387000   1a:2b:3c:4d:69:b9   Broadcast   ARP   60 Who has 10.111.7.1?  Tell 10.111.7.14
12574 91.685858000   LcfcHefe_1c:d7:36   Broadcast   ARP   60 Who has 10.15.42.1?  Tell 10.15.42.247
12605 91.827415000   LcfcHefe_12:00:47   Broadcast   ARP   60 Who has 10.110.33.69?  Tell 10.110.33.210
```

数据包结构

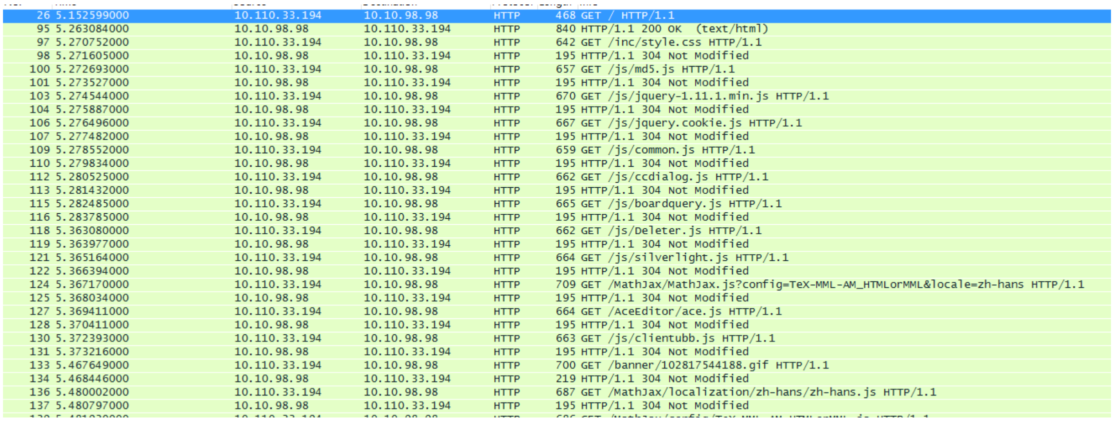


```
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: CompalIn_f9:f3:32 (b8:88:e3:f9:f3:32)
    Sender IP address: 10.110.28.22 (10.110.28.22)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.110.28.1 (10.110.28.1)
```

5.3 跟踪 HTTP 对话

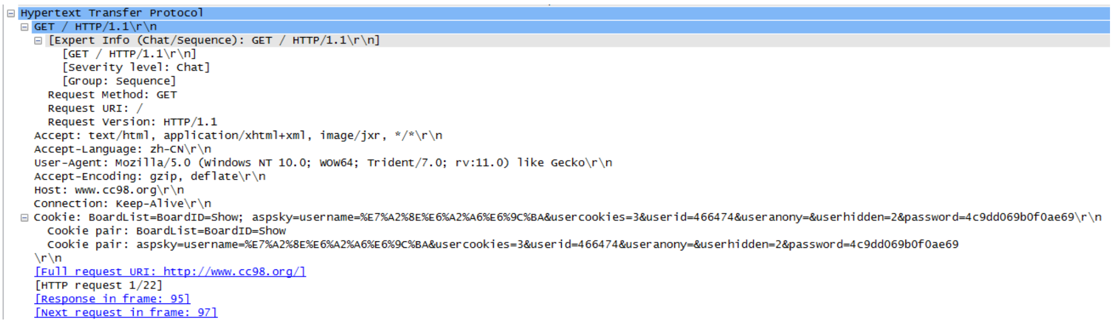
设置捕获条件为 http ip.dst == 10.10.98.98||ip.src == 10.10.98.98，筛选采用 http 协议，source 或 destination 为 10.10.98.98（cc98 的 ip 地址）的数据包

1.HTTP 对话截图（访问 cc98 网站）



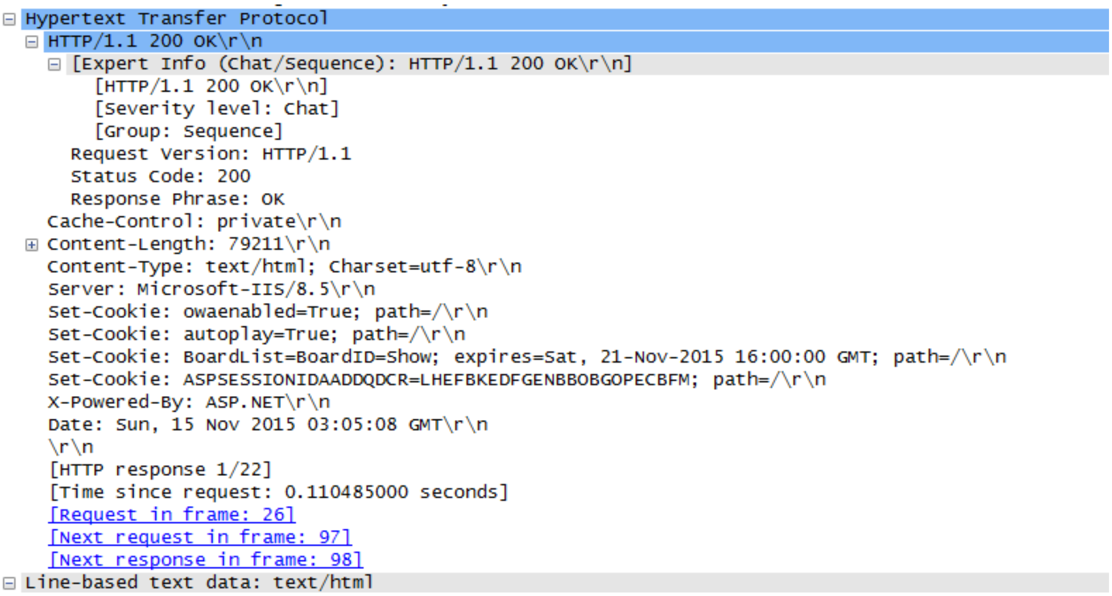
```
 26 5.152599000   10.110.33.194   10.10.98.98     HTTP   468 GET / HTTP/1.1
 95 5.263084000   10.10.98.98     10.110.33.194   HTTP   840 HTTP/1.1 200 OK  (text/html)
 97 5.270752000   10.110.33.194   10.10.98.98     HTTP   642 GET /inc/style.css HTTP/1.1
 98 5.271605000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
100 5.272693000   10.110.33.194   10.10.98.98     HTTP   657 GET /js/md5.js HTTP/1.1
101 5.273527000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
103 5.274544000   10.110.33.194   10.10.98.98     HTTP   670 GET /js/jquery-1.11.1.min.js HTTP/1.1
104 5.275887000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
106 5.276496000   10.110.33.194   10.10.98.98     HTTP   667 GET /js/jquery.cookie.js HTTP/1.1
107 5.277482000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
109 5.278552000   10.110.33.194   10.10.98.98     HTTP   659 GET /js/common.js HTTP/1.1
110 5.279834000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
112 5.280525000   10.110.33.194   10.10.98.98     HTTP   662 GET /js/ccdialog.js HTTP/1.1
113 5.281432000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
115 5.282485000   10.110.33.194   10.10.98.98     HTTP   665 GET /js/boardquery.js HTTP/1.1
116 5.283785000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
118 5.363080000   10.110.33.194   10.10.98.98     HTTP   662 GET /js/Deleter.js HTTP/1.1
119 5.363977000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
121 5.365164000   10.110.33.194   10.10.98.98     HTTP   664 GET /js/silverlight.js HTTP/1.1
122 5.366394000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
124 5.367170000   10.110.33.194   10.10.98.98     HTTP   709 GET /MathJax/MathJax.js?config=TeX-MML-AM_HTMLorMML&locale=zh-hans HTTP/1.1
125 5.368034000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
127 5.369411000   10.110.33.194   10.10.98.98     HTTP   664 GET /AceEditor/ace.js HTTP/1.1
128 5.370411000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
130 5.372393000   10.110.33.194   10.10.98.98     HTTP   663 GET /js/clientubb.js HTTP/1.1
131 5.373216000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
133 5.467649000   10.110.33.194   10.10.98.98     HTTP   700 GET /banner/102817544188.gif HTTP/1.1
134 5.468446000   10.10.98.98     10.110.33.194   HTTP   219 HTTP/1.1 304 Not Modified
136 5.480002000   10.110.33.194   10.10.98.98     HTTP   687 GET /MathJax/localization/zh-hans/zh-hans.js HTTP/1.1
137 5.480797000   10.10.98.98     10.110.33.194   HTTP   195 HTTP/1.1 304 Not Modified
```

2.首先，浏览器向服务器请求网页

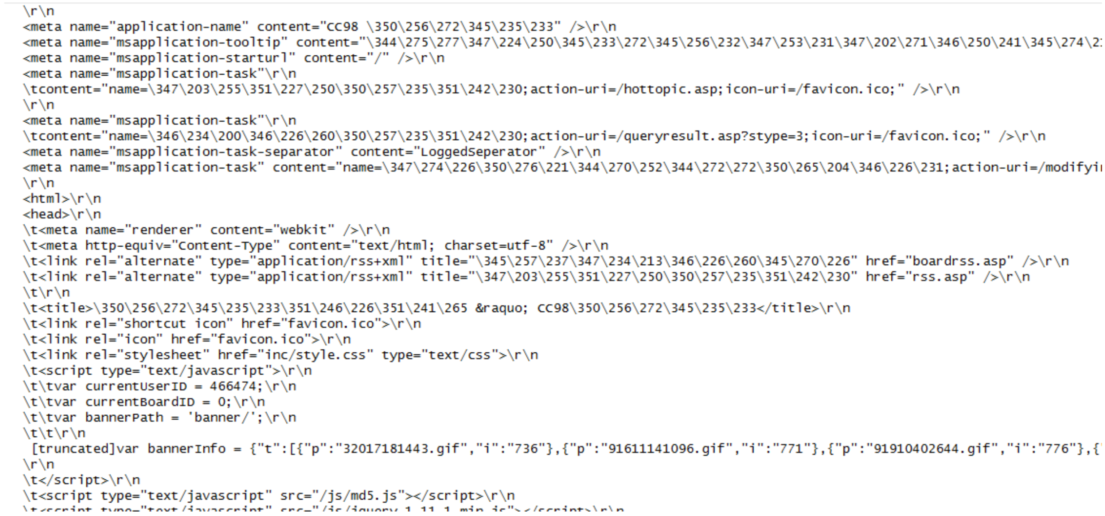


```
⊟ Hypertext Transfer Protocol
  ⊟ GET / HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: zh-CN\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: www.cc98.org\r\n
    Connection: Keep-Alive\r\n
  ⊟ Cookie: BoardList=BoardID=Show; aspsky=username=%E7%A2%8E%E6%A2%A6%E6%9C%BA&usercookies=3&userid=466474&useranony=&userhidden=2&password=4c9dd069b0f0ae69\r\n
      Cookie pair: BoardList=BoardID=Show
      Cookie pair: aspsky=username=%E7%A2%8E%E6%A2%A6%E6%9C%BA&usercookies=3&userid=466474&useranony=&userhidden=2&password=4c9dd069b0f0ae69
    \r\n
    [Full request URI: http://www.cc98.org/]
    [HTTP request 1/22]
    [Response in frame: 95]
    [Next request in frame: 97]
```

3.服务器响应请求，并发送网页数据

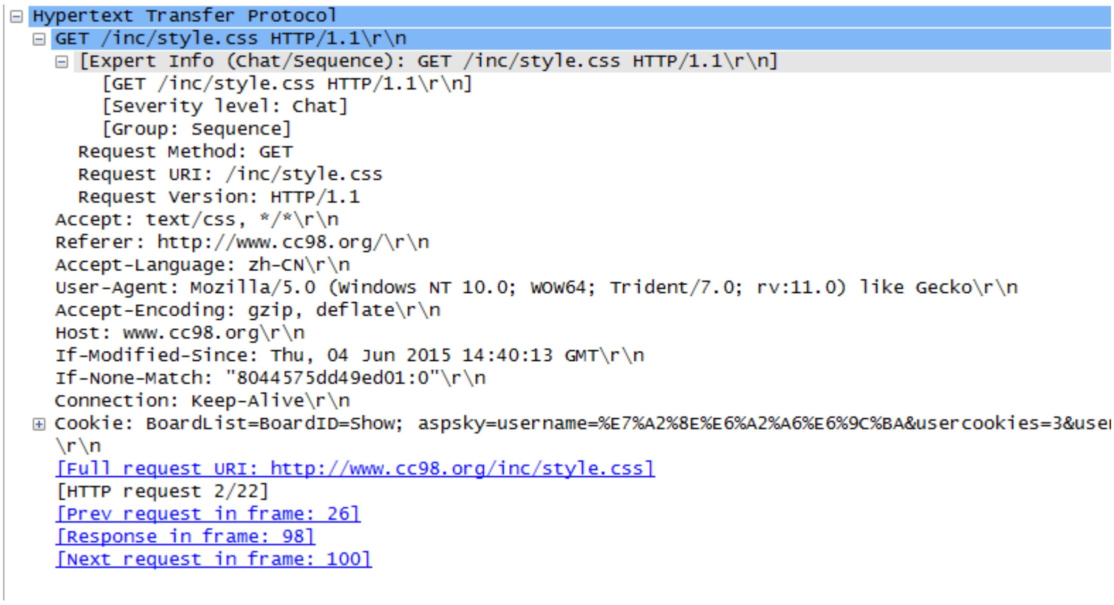


```
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Cache-Control: private\r\n
  ⊞ Content-Length: 79211\r\n
    Content-Type: text/html; Charset=utf-8\r\n
    Server: Microsoft-IIS/8.5\r\n
    Set-Cookie: owaenabled=True; path=/\r\n
    Set-Cookie: autoplay=True; path=/\r\n
    Set-Cookie: BoardList=BoardID=Show; expires=Sat, 21-Nov-2015 16:00:00 GMT; path=/\r\n
    Set-Cookie: ASPSESSIONIDAADDQDCR=LHEFBKEDFGENBBOBGOPECBFM; path=/\r\n
    X-Powered-By: ASP.NET\r\n
    Date: Sun, 15 Nov 2015 03:05:08 GMT\r\n
    \r\n
    [HTTP response 1/22]
    [Time since request: 0.110485000 seconds]
    [Request in frame: 26]
    [Next request in frame: 97]
    [Next response in frame: 98]
⊟ Line-based text data: text/html
```



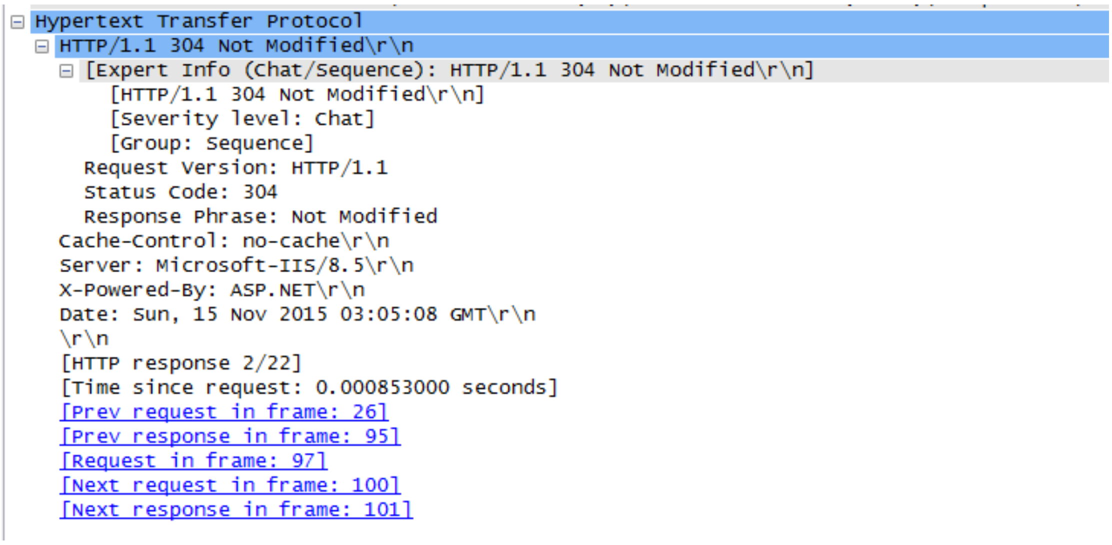
```
\r\n
<meta name="application-name" content="CC98 \350\256\272\345\235\233" />\r\n
<meta name="msapplication-tooltip" content="\344\275\277\347\224\250\345\233\272\345\256\232\347\253\231\347\202\271\346\250\241\345\274\2
<meta name="msapplication-starturl" content="/" />\r\n
<meta name="msapplication-task"\r\n
\tcontent="name=\347\203\255\351\227\250\350\257\235\351\242\230;action-uri=/hottopic.asp;icon-uri=/favicon.ico;" />\r\n
\r\n
<meta name="msapplication-task"\r\n
\tcontent="name=\346\234\200\346\226\260\350\257\235\351\242\230;action-uri=/queryresult.asp?stype=3;icon-uri=/favicon.ico;" />\r\n
<meta name="msapplication-task-separator" content="LoggedSeperator" />\r\n
<meta name="msapplication-task" content="name=\347\274\226\350\276\221\344\270\252\344\272\272\350\265\204\346\226\231;action-uri=/modifyi
\r\n
<html>\r\n
<head>\r\n
\t<meta name="renderer" content="webkit" />\r\n
\t<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />\r\n
\t<link rel="alternate" type="application/rss+xml" title="\345\257\237\347\234\213\346\226\260\345\270\226" href="boardrss.asp" />\r\n
\t<link rel="alternate" type="application/rss+xml" title="\347\203\255\351\227\250\350\257\235\351\242\230" href="rss.asp" />\r\n
\t\r\n
\t<title>\350\256\272\345\235\233\351\246\226\351\241\265 &raquo; CC98\350\256\272\345\235\233</title>\r\n
\t<link rel="shortcut icon" href="favicon.ico">\r\n
\t<link rel="icon" href="favicon.ico">\r\n
\t<link rel="stylesheet" href="inc/style.css" type="text/css">\r\n
\t<script type="text/javascript">\r\n
\t\tvar currentUserID = 466474;\r\n
\t\tvar currentBoardID = 0;\r\n
\t\tvar bannerPath = 'banner/';\r\n
\t\t\r\n
 [truncated]var bannerInfo = {"t":[{"p":"32017181443.gif","i":"736"},{"p":"91611141096.gif","i":"771"},{"p":"91910402644.gif","i":"776"},{
\r\n
\t</script>\r\n
\t<script type="text/javascript" src="/js/md5.js"></script>\r\n
\t<script type="text/javascript" src="/js/jquery-1.11.1.min.js"></script>\r\n
```

4.浏览器向服务器请求样式表文件(CSS)



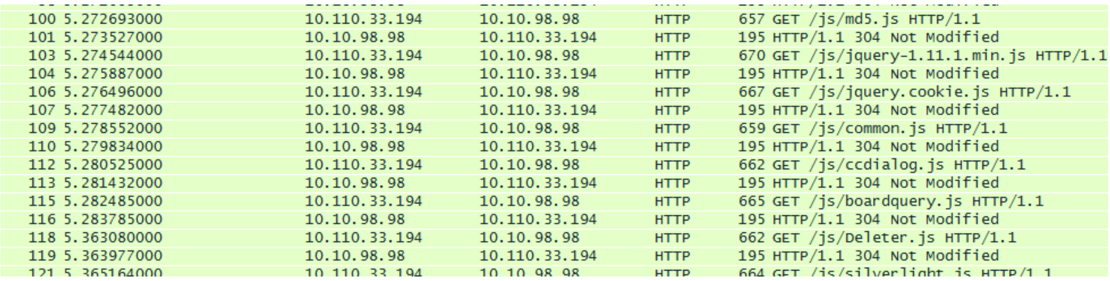
```
⊟ Hypertext Transfer Protocol
  ⊟ GET /inc/style.css HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /inc/style.css HTTP/1.1\r\n]
        [GET /inc/style.css HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /inc/style.css
      Request Version: HTTP/1.1
    Accept: text/css, */*\r\n
    Referer: http://www.cc98.org/\r\n
    Accept-Language: zh-CN\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: www.cc98.org\r\n
    If-Modified-Since: Thu, 04 Jun 2015 14:40:13 GMT\r\n
    If-None-Match: "8044575dd49ed01:0"\r\n
    Connection: Keep-Alive\r\n
  ⊞ Cookie: BoardList=BoardID=Show; aspsky=username=%E7%A2%8E%E6%A2%A6%E6%9C%BA&usercookies=3&use
    \r\n
    [Full request URI: http://www.cc98.org/inc/style.css]
    [HTTP request 2/22]
    [Prev request in frame: 26]
    [Response in frame: 98]
    [Next request in frame: 100]
```

5.服务器响应 CSS 文件自上次获取之后并没有改变，所以浏览器可以使用缓存的 CSS 文件



```
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 304 Not Modified\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 304
      Response Phrase: Not Modified
    Cache-Control: no-cache\r\n
    Server: Microsoft-IIS/8.5\r\n
    X-Powered-By: ASP.NET\r\n
    Date: Sun, 15 Nov 2015 03:05:08 GMT\r\n
    \r\n
    [HTTP response 2/22]
    [Time since request: 0.000853000 seconds]
    [Prev request in frame: 26]
    [Prev response in frame: 95]
    [Request in frame: 97]
    [Next request in frame: 100]
    [Next response in frame: 101]
```

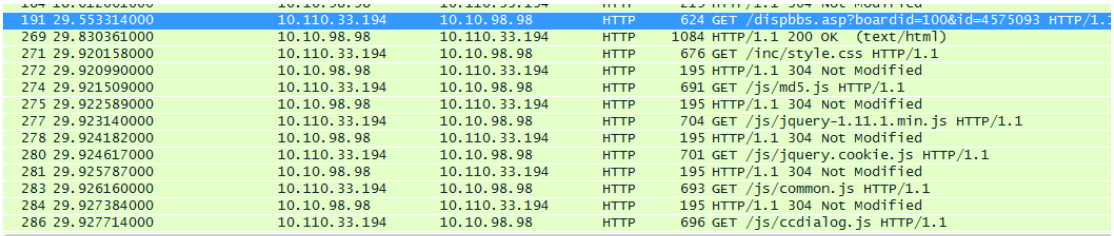
6.接着浏览器向服务器请求 javascript 脚本文件，服务器响应自上次获取后没有改变，可以使用缓存文件



```
100 5.272693000    10.110.33.194    10.10.98.98      HTTP    657 GET /js/md5.js HTTP/1.1
101 5.273527000    10.10.98.98      10.110.33.194    HTTP    195 HTTP/1.1 304 Not Modified
103 5.274544000    10.110.33.194    10.10.98.98      HTTP    670 GET /js/jquery-1.11.1.min.js HTTP/1.1
104 5.275887000    10.10.98.98      10.110.33.194    HTTP    195 HTTP/1.1 304 Not Modified
106 5.276496000    10.110.33.194    10.10.98.98      HTTP    667 GET /js/jquery.cookie.js HTTP/1.1
107 5.277482000    10.10.98.98      10.110.33.194    HTTP    195 HTTP/1.1 304 Not Modified
109 5.278552000    10.110.33.194    10.10.98.98      HTTP    659 GET /js/common.js HTTP/1.1
110 5.279834000    10.10.98.98      10.110.33.194    HTTP    195 HTTP/1.1 304 Not Modified
112 5.280525000    10.110.33.194    10.10.98.98      HTTP    662 GET /js/ccdialog.js HTTP/1.1
113 5.281432000    10.10.98.98      10.110.33.194    HTTP    195 HTTP/1.1 304 Not Modified
115 5.282485000    10.110.33.194    10.10.98.98      HTTP    665 GET /js/boardquery.js HTTP/1.1
116 5.283785000    10.10.98.98      10.110.33.194    HTTP    195 HTTP/1.1 304 Not Modified
118 5.363080000    10.110.33.194    10.10.98.98      HTTP    662 GET /js/Deleter.js HTTP/1.1
119 5.363977000    10.10.98.98      10.110.33.194    HTTP    195 HTTP/1.1 304 Not Modified
121 5.365164000    10.110.33.194    10.10.98.98      HTTP    664 GET /js/silverlight.js HTTP/1.1
```

至此，cc98 的首页已经完全被加载完毕

7.接着，点击 cc98 首页热门话题链接，又开始了新的一轮 HTTP 对话

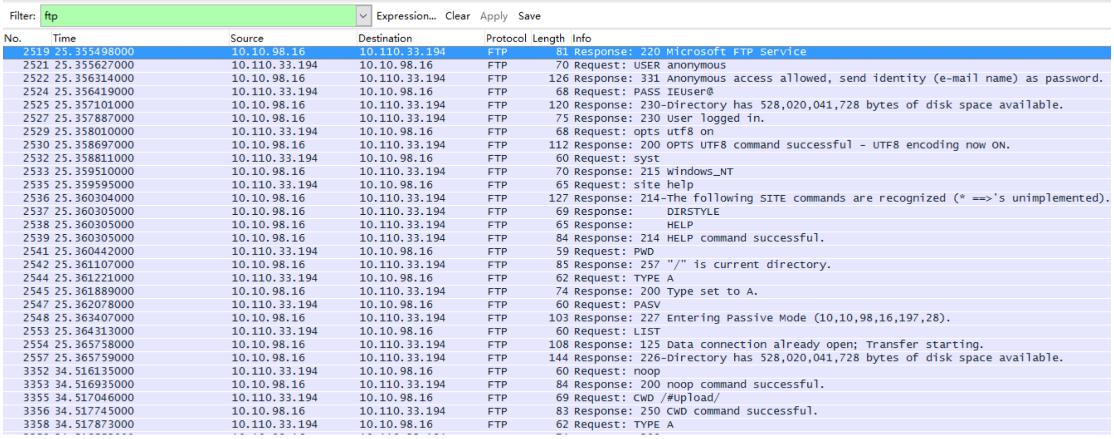


```
191 29.553314000    10.110.33.194    10.10.98.98      HTTP     624 GET /dispbbs.asp?boardid=100&id=4575093 HTTP/1.
269 29.830361000    10.10.98.98      10.110.33.194    HTTP    1084 HTTP/1.1 200 OK  (text/html)
271 29.920158000    10.110.33.194    10.10.98.98      HTTP     676 GET /inc/style.css HTTP/1.1
272 29.920990000    10.10.98.98      10.110.33.194    HTTP     195 HTTP/1.1 304 Not Modified
274 29.921509000    10.110.33.194    10.10.98.98      HTTP     691 GET /js/md5.js HTTP/1.1
275 29.922589000    10.10.98.98      10.110.33.194    HTTP     195 HTTP/1.1 304 Not Modified
277 29.923140000    10.110.33.194    10.10.98.98      HTTP     704 GET /js/jquery-1.11.1.min.js HTTP/1.1
278 29.924182000    10.10.98.98      10.110.33.194    HTTP     195 HTTP/1.1 304 Not Modified
280 29.924617000    10.110.33.194    10.10.98.98      HTTP     701 GET /js/jquery.cookie.js HTTP/1.1
281 29.925787000    10.10.98.98      10.110.33.194    HTTP     195 HTTP/1.1 304 Not Modified
283 29.926160000    10.110.33.194    10.10.98.98      HTTP     693 GET /js/common.js HTTP/1.1
284 29.927384000    10.10.98.98      10.110.33.194    HTTP     195 HTTP/1.1 304 Not Modified
286 29.927714000    10.110.33.194    10.10.98.98      HTTP     696 GET /js/ccdialog.js HTTP/1.1
```

5.4 跟踪 FTP 对话

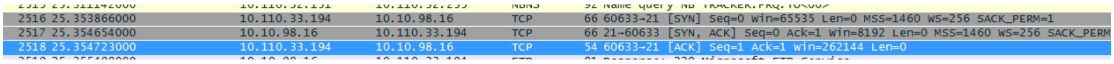
设置筛选条件为 ftp 筛选采用 ftp 协议的数据包

对话截图



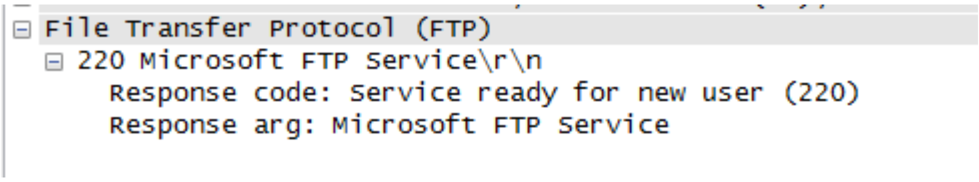
```
No.  Time          Source           Destination      Protocol Length Info
2519 25.355498000  10.10.98.16      10.110.33.194    FTP       81 Response: 220 Microsoft FTP Service
2521 25.355627000  10.110.33.194    10.10.98.16      FTP       70 Request: USER anonymous
2522 25.356314000  10.10.98.16      10.110.33.194    FTP      126 Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
2524 25.356419000  10.110.33.194    10.10.98.16      FTP       68 Request: PASS IEUser@
2525 25.357101000  10.10.98.16      10.110.33.194    FTP      120 Response: 230-Directory has 528,020,041,728 bytes of disk space available.
2527 25.357887000  10.10.98.16      10.110.33.194    FTP       75 Response: 230 User logged in.
2529 25.358010000  10.110.33.194    10.10.98.16      FTP       68 Request: opts utf8 on
2530 25.358697000  10.10.98.16      10.110.33.194    FTP      112 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
2532 25.358811000  10.110.33.194    10.10.98.16      FTP       60 Request: syst
2533 25.359510000  10.10.98.16      10.110.33.194    FTP       70 Response: 215 Windows_NT
2535 25.359595000  10.110.33.194    10.10.98.16      FTP       65 Request: site help
2536 25.360304000  10.10.98.16      10.110.33.194    FTP      127 Response: 214-The following SITE commands are recognized (* ==>'s unimplemented).
2537 25.360305000  10.10.98.16      10.110.33.194    FTP       69 Response:     DIRSTYLE
2538 25.360305000  10.10.98.16      10.110.33.194    FTP       65 Response:     HELP
2539 25.360305000  10.10.98.16      10.110.33.194    FTP       84 Response: 214 HELP command successful.
2541 25.360442000  10.110.33.194    10.10.98.16      FTP       59 Request: PWD
2542 25.361107000  10.10.98.16      10.110.33.194    FTP       85 Response: 257 "/" is current directory.
2544 25.361221000  10.110.33.194    10.10.98.16      FTP       62 Request: TYPE A
2545 25.361889000  10.10.98.16      10.110.33.194    FTP       74 Response: 200 Type set to A.
2547 25.362078000  10.110.33.194    10.10.98.16      FTP       60 Request: PASV
2548 25.363407000  10.10.98.16      10.110.33.194    FTP      103 Response: 227 Entering Passive Mode (10,10,98,16,197,28).
2553 25.364313000  10.110.33.194    10.10.98.16      FTP       60 Request: LIST
2554 25.365758000  10.10.98.16      10.110.33.194    FTP      108 Response: 125 Data connection already open; Transfer starting.
2557 25.365759000  10.10.98.16      10.110.33.194    FTP      144 Response: 226-Directory has 528,020,041,728 bytes of disk space available.
3352 34.516135000  10.110.33.194    10.10.98.16      FTP       60 Request: noop
3353 34.516935000  10.10.98.16      10.110.33.194    FTP       84 Response: 200 noop command successful.
3355 34.517046000  10.110.33.194    10.10.98.16      FTP       69 Request: CWD /#Upload/
3356 34.517745000  10.10.98.16      10.110.33.194    FTP       83 Response: 250 CWD command successful.
3358 34.517873000  10.110.33.194    10.10.98.16      FTP       62 Request: TYPE A
```

1.首先通过 TCP 协议三次握手建立起与 FTP 服务器的连接



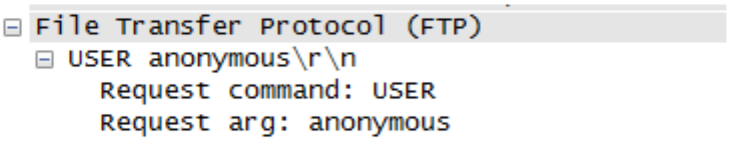
```
2516 25.353866000    10.110.33.194    10.10.98.16      TCP    66 60633→21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2517 25.354654000    10.10.98.16      10.110.33.194    TCP    66 21→60633 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2518 25.354723000    10.110.33.194    10.10.98.16      TCP    54 60633→21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
```

FTP 服务器响应该服务器相关信息



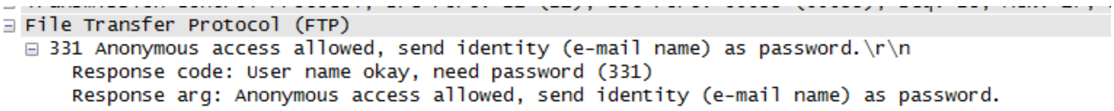
```
⊟ File Transfer Protocol (FTP)
  ⊟ 220 Microsoft FTP Service\r\n
      Response code: Service ready for new user (220)
      Response arg: Microsoft FTP Service
```

2.本地向 FTP 服务器发出登录请求，采用匿名登陆方式



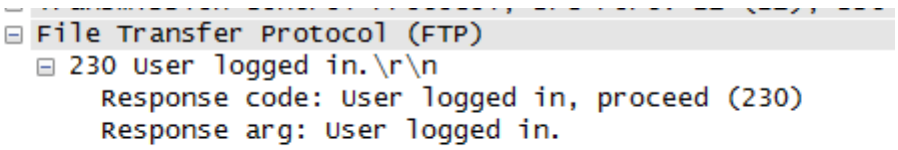
```
⊟ File Transfer Protocol (FTP)
  ⊟ USER anonymous\r\n
      Request command: USER
      Request arg: anonymous
```

3.FTP 服务器响应匿名登陆检查通过



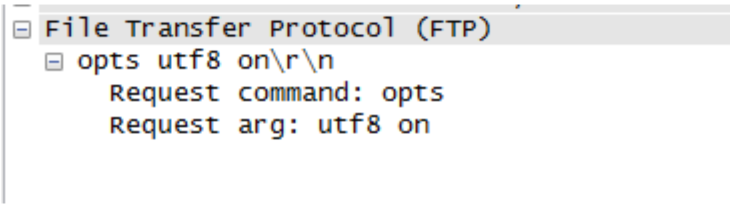
```
⊟ File Transfer Protocol (FTP)
  ⊟ 331 Anonymous access allowed, send identity (e-mail name) as password.\r\n
      Response code: User name okay, need password (331)
      Response arg: Anonymous access allowed, send identity (e-mail name) as password.
```

4.FTP 服务器响应用户已经登录



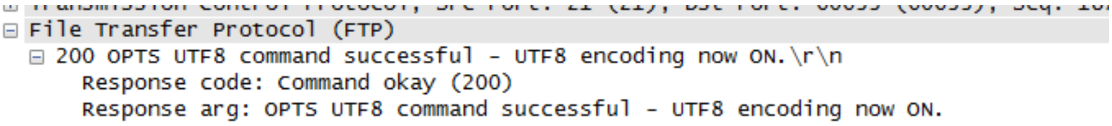
```
⊟ File Transfer Protocol (FTP)
  ⊟ 230 User logged in.\r\n
      Response code: User logged in, proceed (230)
      Response arg: User logged in.
```

5.本地请求采用 utf8 编码方式



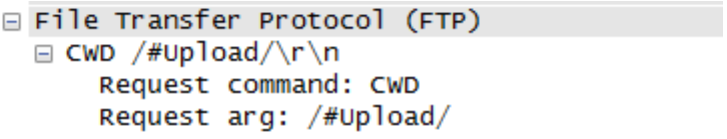
```
⊟ File Transfer Protocol (FTP)
  ⊟ opts utf8 on\r\n
      Request command: opts
      Request arg: utf8 on
```

6.FTP 服务器响应已经开启 utf8 编码模式



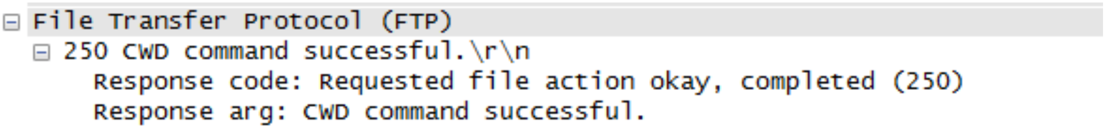
```
⊟ File Transfer Protocol (FTP)
  ⊟ 200 OPTS UTF8 command successful - UTF8 encoding now ON.\r\n
      Response code: Command okay (200)
      Response arg: OPTS UTF8 command successful - UTF8 encoding now ON.
```

7.本地请求进入/#Upload/目录



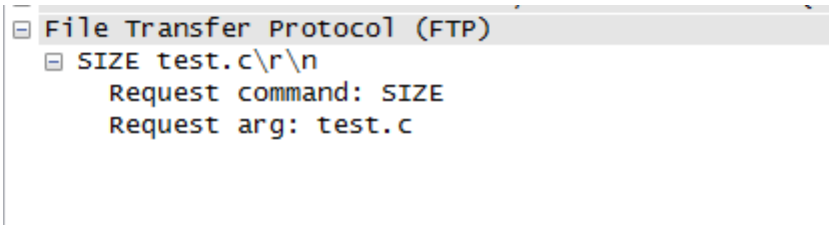
```
⊟ File Transfer Protocol (FTP)
  ⊟ CWD /#Upload/\r\n
      Request command: CWD
      Request arg: /#Upload/
```

8.服务器响应成功进入该目录



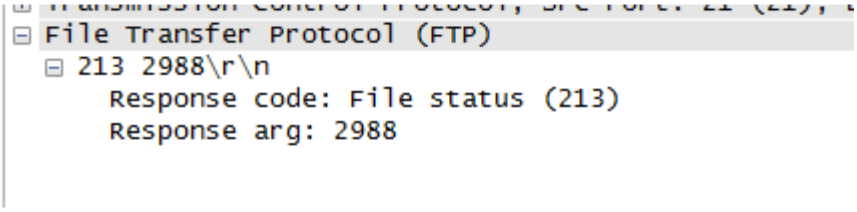
```
⊟ File Transfer Protocol (FTP)
  ⊟ 250 CWD command successful.\r\n
      Response code: Requested file action okay, completed (250)
      Response arg: CWD command successful.
```

9.本地请求 test.c 文件大小



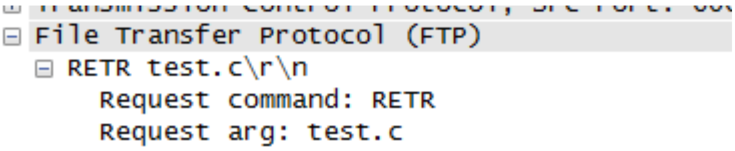
```
⊟ File Transfer Protocol (FTP)
  ⊟ SIZE test.c\r\n
      Request command: SIZE
      Request arg: test.c
```

10.FTP 服务器响应文件大小为 2988 字节



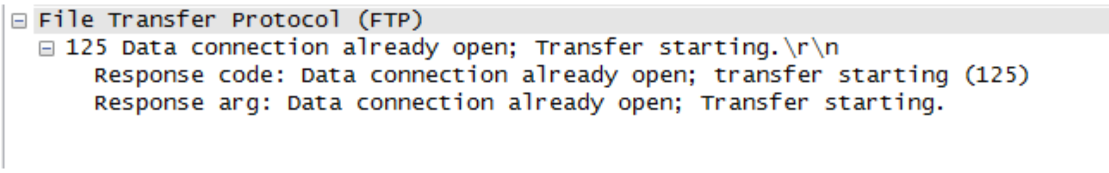
```
File Transfer Protocol (FTP)
  213 2988\r\n
    Response code: File status (213)
    Response arg: 2988
```

11.本地请求该文件



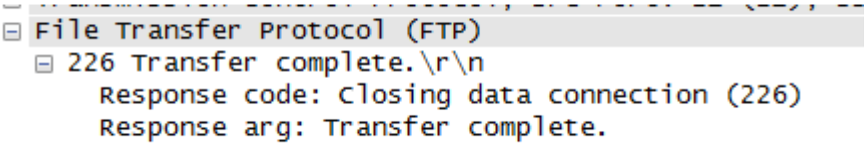
```
File Transfer Protocol (FTP)
  RETR test.c\r\n
    Request command: RETR
    Request arg: test.c
```

12.FTP 服务器响应数据连接已经打开开始传送数据



```
File Transfer Protocol (FTP)
  125 Data connection already open; Transfer starting.\r\n
    Response code: Data connection already open; transfer starting (125)
    Response arg: Data connection already open; Transfer starting.
```

12.FTP 服务器发送数据传送完成，关闭数据连接

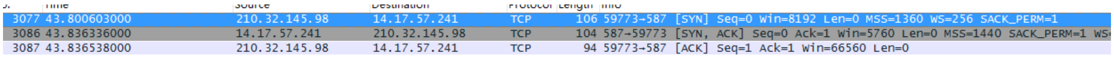


```
File Transfer Protocol (FTP)
  226 Transfer complete.\r\n
    Response code: Closing data connection (226)
    Response arg: Transfer complete.
```

5.5 SMTP 会话分析

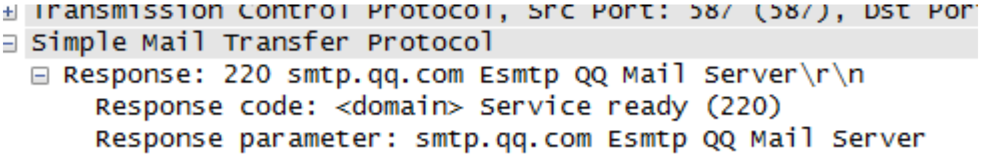
筛选条件 smtp 筛选采用 smtp 协议会话的数据包

1.客户端与服务器通过 TCP 协议三次握手建立连接



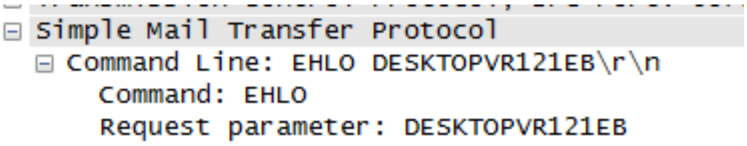
```
3077 43.800603000  210.32.145.98   14.17.57.241    TCP   106 59773→587 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=256 SACK_PERM=1
3086 43.836336000  14.17.57.241    210.32.145.98   TCP   104 587→59773 [SYN, ACK] Seq=0 Ack=1 Win=5760 Len=0 MSS=1440 SACK_PERM=1 WS
3087 43.836538000  210.32.145.98   14.17.57.241    TCP    94 59773→587 [ACK] Seq=1 Ack=1 Win=66560 Len=0
```

2.服务器响应，连接已经建立



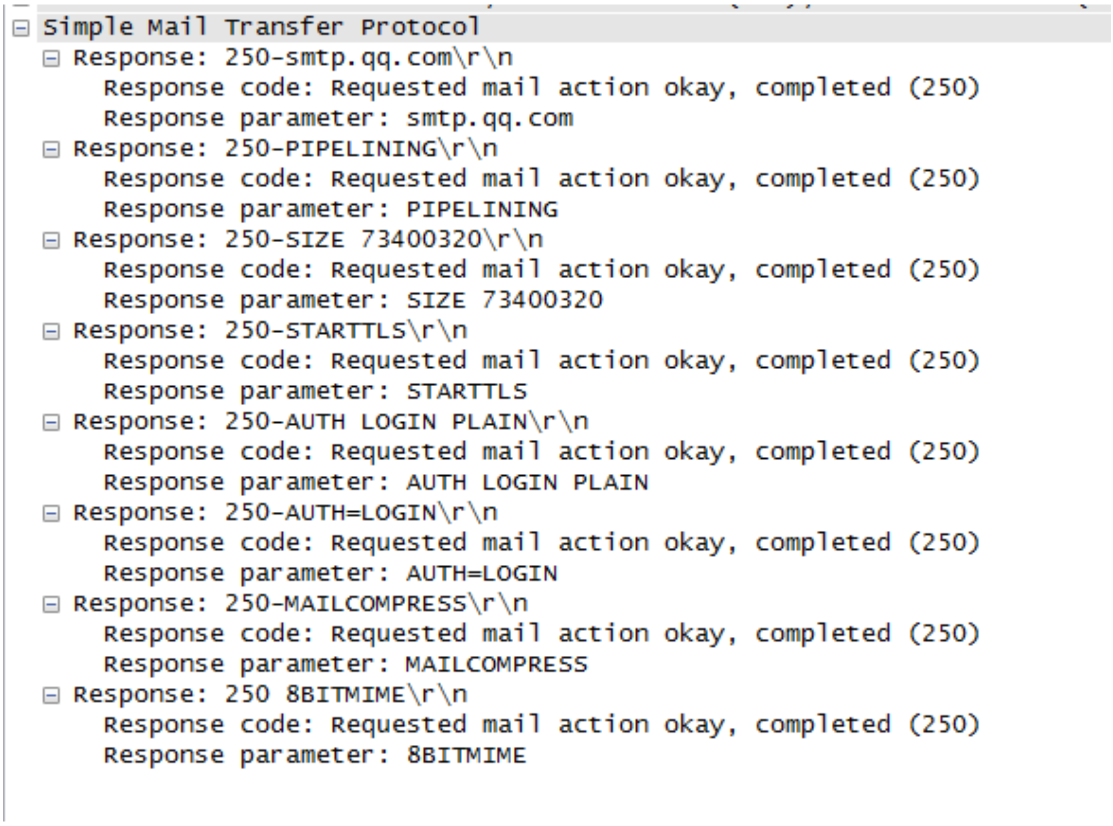
```
Transmission Control Protocol, Src Port: 587 (587), Dst Por
Simple Mail Transfer Protocol
  Response: 220 smtp.qq.com Esmtp QQ Mail Server\r\n
    Response code: <domain> Service ready (220)
    Response parameter: smtp.qq.com Esmtp QQ Mail Server
```

3.客户端向服务器发送 EHLO 命令，并加上本机主机名 DESKTOPVR121EB



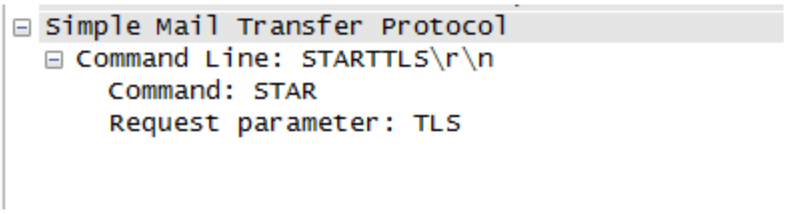
```
Simple Mail Transfer Protocol
  Command Line: EHLO DESKTOPVR121EB\r\n
    Command: EHLO
    Request parameter: DESKTOPVR121EB
```

4.服务器响应回复，250 表明服务器可用



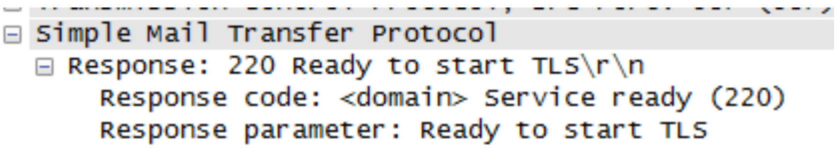
```
⊟ Simple Mail Transfer Protocol
  ⊟ Response: 250-smtp.qq.com\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: smtp.qq.com
  ⊟ Response: 250-PIPELINING\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: PIPELINING
  ⊟ Response: 250-SIZE 73400320\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: SIZE 73400320
  ⊟ Response: 250-STARTTLS\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: STARTTLS
  ⊟ Response: 250-AUTH LOGIN PLAIN\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: AUTH LOGIN PLAIN
  ⊟ Response: 250-AUTH=LOGIN\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: AUTH=LOGIN
  ⊟ Response: 250-MAILCOMPRESS\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: MAILCOMPRESS
  ⊟ Response: 250 8BITMIME\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: 8BITMIME
```

5.客户端请求将纯文本通信协议升级为 TLS 加密连接



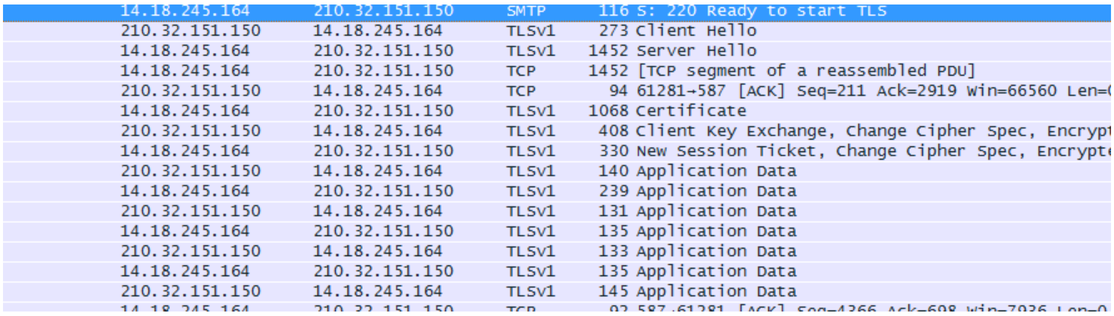
```
⊟ Simple Mail Transfer Protocol
  ⊟ Command Line: STARTTLS\r\n
      Command: STAR
      Request parameter: TLS
```

6.服务器端响应可以进行 TLS 传递数据



```
⊟ Simple Mail Transfer Protocol
  ⊟ Response: 220 Ready to start TLS\r\n
      Response code: <domain> Service ready (220)
      Response parameter: Ready to start TLS
```

7.客户端和服务器端开始通过 TLS 传递数据

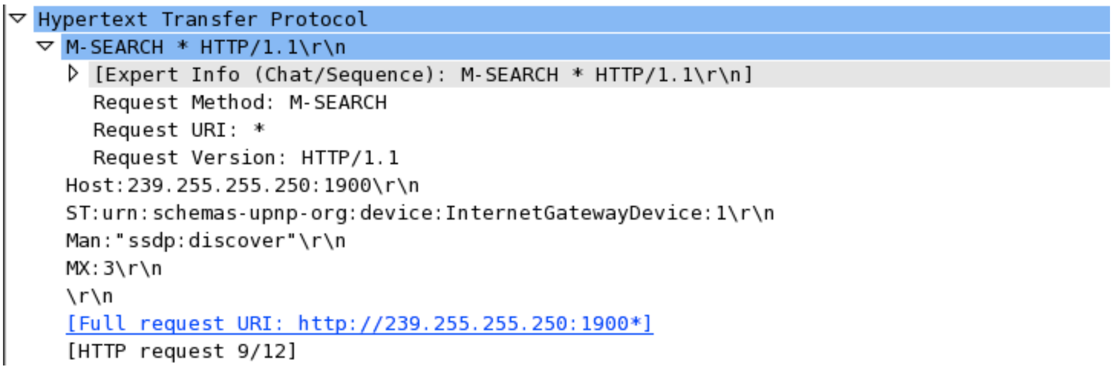


```
14.18.245.164    210.32.151.150   SMTP     116 S: 220 Ready to start TLS
210.32.151.150   14.18.245.164    TLSv1    273 Client Hello
14.18.245.164    210.32.151.150   TLSv1   1452 Server Hello
14.18.245.164    210.32.151.150   TCP     1452 [TCP segment of a reassembled PDU]
210.32.151.150   14.18.245.164    TCP       94 61281→587 [ACK] Seq=211 Ack=2919 Win=66560 Len=(
14.18.245.164    210.32.151.150   TLSv1   1068 Certificate
210.32.151.150   14.18.245.164    TLSv1    408 Client Key Exchange, Change Cipher Spec, Encrypt
14.18.245.164    210.32.151.150   TLSv1    330 New Session Ticket, Change Cipher Spec, Encrypte
210.32.151.150   14.18.245.164    TLSv1    140 Application Data
14.18.245.164    210.32.151.150   TLSv1    239 Application Data
210.32.151.150   14.18.245.164    TLSv1    131 Application Data
14.18.245.164    210.32.151.150   TLSv1    135 Application Data
210.32.151.150   14.18.245.164    TLSv1    133 Application Data
14.18.245.164    210.32.151.150   TLSv1    135 Application Data
210.32.151.150   14.18.245.164    TLSv1    145 Application Data
14.18.245.164    210.32.151.150   TCP       92 587→61281 [ACK] Seq=4366 Ack=698 Win=7936 Len=0
```

六、实验结果分析

1. SSDP 数据包分析

SSDP 简单服务发现协议，是应用层协议，是构成 UPnP（通用即插即用）技术的核心协议之一。它为网络客户端（network client）提供了一种发现网络服务（network services）的机制，采用基于通知和发现路由的多播方式实现。



```
▽ Hypertext Transfer Protocol
  ▽ M-SEARCH * HTTP/1.1\r\n
    ▷ [Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]
      Request Method: M-SEARCH
      Request URI: *
      Request Version: HTTP/1.1
    Host:239.255.255.250:1900\r\n
    ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
    Man:"ssdp:discover"\r\n
    MX:3\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 9/12]
```

HOST：设置为协议保留多播地址和端口，必须是：239.255.255.250:1900

MAN：设置协议查询的类型，必须是：ssdp:discover

MX：设置设备响应最长等待时间。设备响应在 0 和这个值之间随机选择响应延迟的值，这样可以为控制点响应平衡网络负载。

ST：设置服务查询的目标，它必须是下面的类型：

-ssdp:all 搜索所有设备和服务

-upnp:rootdevice 仅搜索网络中的根设备

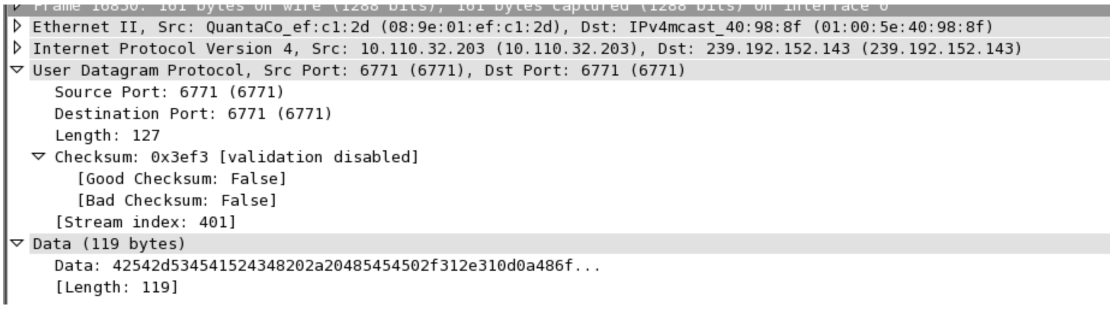
-uuid:device-UUID 查询 UUID 标识的设备

-urn:schemas-upnp-org:device:device-Type:version 查询 device-Type 字段指定的设备类型，设备类型和版本由 UPNP 组织定义。

-urn:schemas-upnp-org:service:service-Type:version 查询 service-Type 字段指定的服务类型，服务类型和版本由 UPNP 组织定义。

2.UDP 数据包分析

UDP 协议全称是用户数据报协议，是一种无连接的协议



```
▷ Frame 10830: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0
▷ Ethernet II, Src: QuantaCo_ef:c1:2d (08:9e:01:ef:c1:2d), Dst: IPv4mcast_40:98:8f (01:00:5e:40:98:8f)
▷ Internet Protocol Version 4, Src: 10.110.32.203 (10.110.32.203), Dst: 239.192.152.143 (239.192.152.143)
▽ User Datagram Protocol, Src Port: 6771 (6771), Dst Port: 6771 (6771)
    Source Port: 6771 (6771)
    Destination Port: 6771 (6771)
    Length: 127
  ▽ Checksum: 0x3ef3 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
    [Stream index: 401]
▽ Data (119 bytes)
    Data: 42542d534541524348202a20485454502f312e310d0a486f...
    [Length: 119]
```

数据包底层基于以太网和 IP 协议

Source:源端口号

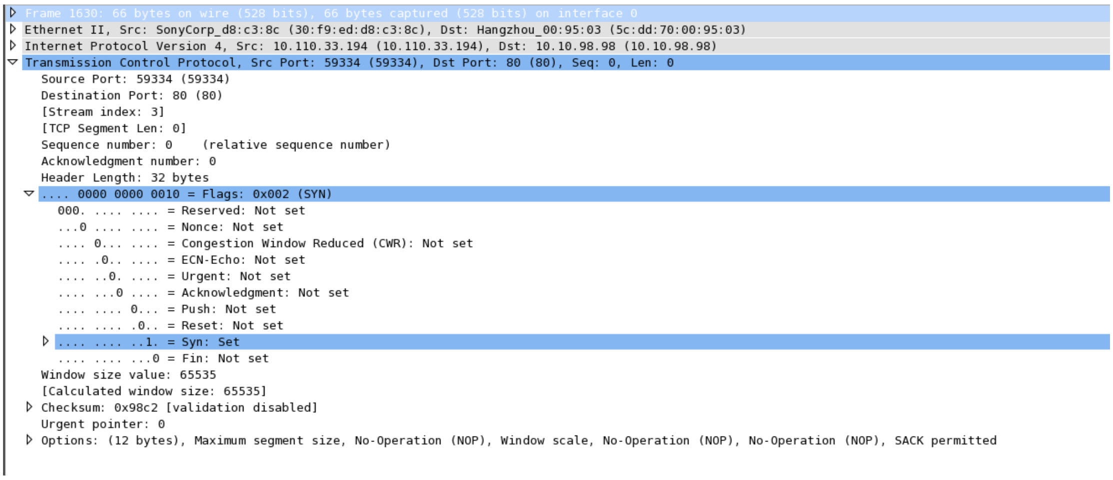
Destination Port:目标端口号

Length:数据包长度

Checksum:校验值

3.TCP 协议

TCP 是一种面向连接的、可靠的、基于字节流的传输层通信协议



```
▷ Frame 1630: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Ethernet II, Src: SonyCorp_d8:c3:8c (30:f9:ed:d8:c3:8c), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)
▷ Internet Protocol Version 4, Src: 10.110.33.194 (10.110.33.194), Dst: 10.10.98.98 (10.10.98.98)
▽ Transmission Control Protocol, Src Port: 59334 (59334), Dst Port: 80 (80), Seq: 0, Len: 0
    Source Port: 59334 (59334)
    Destination Port: 80 (80)
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
  ▽ .... 0000 0000 0010 = Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▷ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
    Window size value: 65535
    [Calculated window size: 65535]
  ▷ Checksum: 0x98c2 [validation disabled]
    Urgent pointer: 0
  ▷ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

数据包底层基于以太网协议和 IPv4 协议

TCP 报头主要包含

Source Port 是源端口，16 位。

Destination Port 是目的端口，16 位。

Sequence Number 是发送数据包中的第一个字节的序列号，32 位。

Acknowledgment Number 是确认序列号，32 位。

Data Offset 是数据偏移，4 位，该字段的值是 TCP 首部（包括选项）长度除以 4。

标志位： 6 位，URG 表示 Urgent Pointer 字段有意义：

ACK 表示 Acknowledgment Number 字段有意义

PSH 表示 Push 功能，RST 表示复位 TCP 连接

SYN 表示 SYN 报文（在建立 TCP 连接的时候使用）

FIN 表示没有数据需要发送了（在关闭 TCP 连接的时候使用）

Window 表示接收缓冲区的空闲空间，16 位，用来告诉 TCP 连接对端自己能够接收的最大数据长度。

Checksum 是校验和，16 位。

七、讨论、心得

当我在查阅资料是发现网上资料的抓包 STMP 对话的资料中邮件客户端与服务器还是都是直接采用 smtp 交换用户名、密码和邮件信息等。而我利用 outlook 和 foxmail 两种邮件客户端均显示，客户端利用 smtp 进行简单的连接确认之后，随即对话就升级为 TLSv1 对普通文本协议加密通信了，表明现在的邮件客户端相比以往更加重视数据的安全性