2015广东省强网杯CTF初赛题之大黑阔writeup

原创

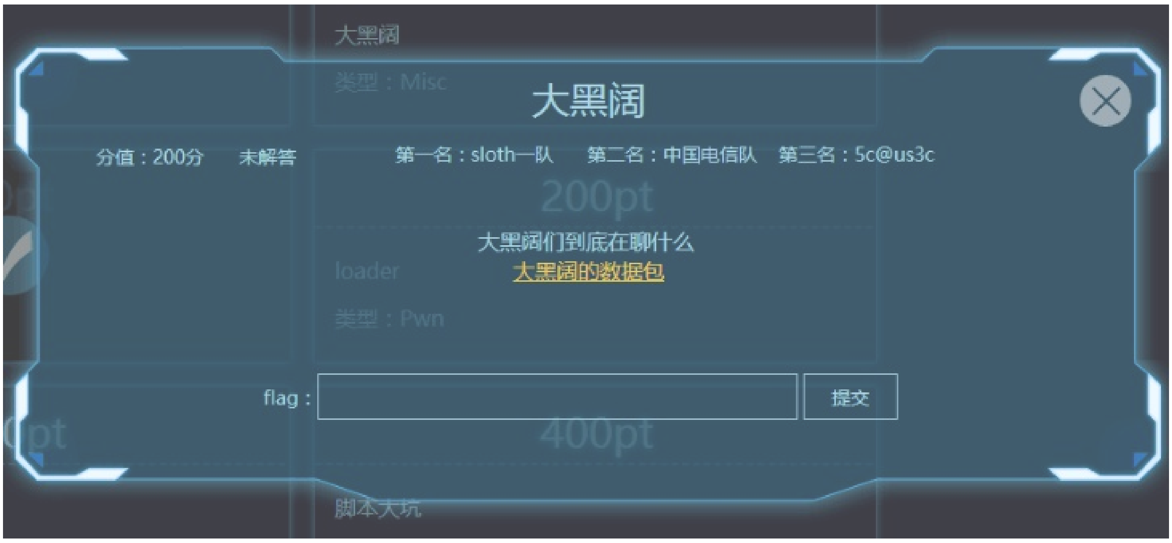
1fragment碎片 于 2016-03-04 19:06:03 发布 6920 收藏

文章标签： wireshark

本文链接：https://blog.csdn.net/sinat_16683257/article/details/50804892

版权

前几天的防火墙与入侵检测课上，老师把广东省强网杯CTF其中的一道初赛题当做实践课的任务，解题时学会了不少东西，觉得挺有趣的，所以记下来，以下writeup仅仅是个人见解



大黑阔

分值：200分 未解答 第一名：sloth一队 第二名：中国电信队 第三名：5c@us3c

大黑阔们到底在聊什么

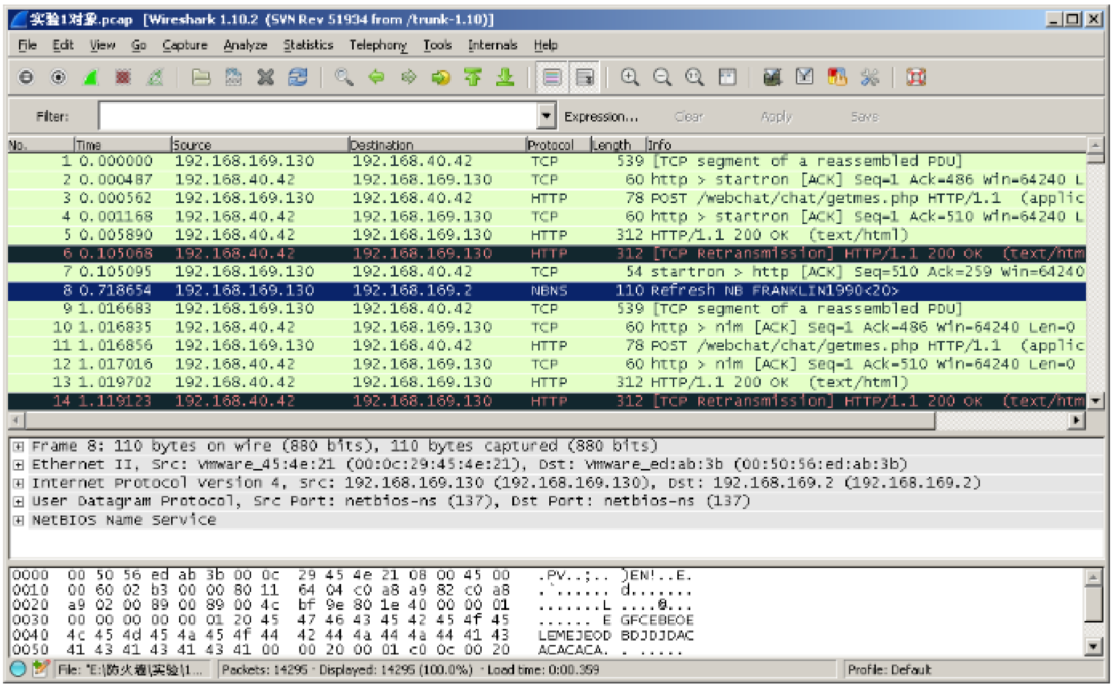
大黑阔的数据包

flag :

- 【**大黑阔的数据包**】是一个.pcap文件

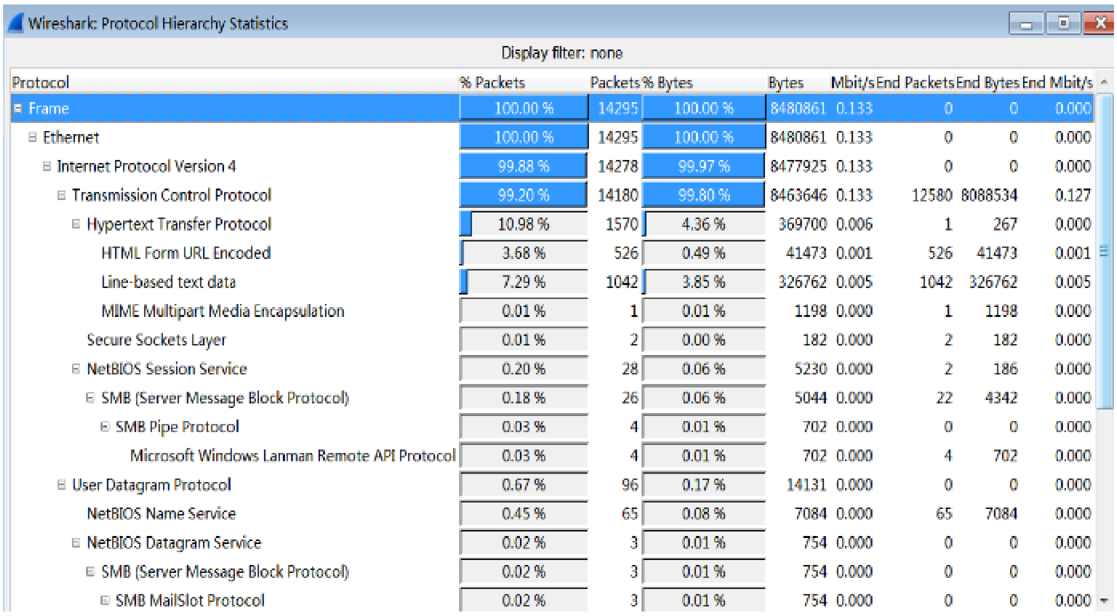
详细步骤如下：

用Wireshark打开.pcap文件。


实验1对象.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.169.130  192.168.40.42    TCP      539 [TCP segment of a reassembled PDU]
   2 0.000487   192.168.40.42    192.168.169.130  TCP       60 http > startron [ACK] Seq=1 Ack=486 Win=64240 L
   3 0.000562   192.168.169.130  192.168.40.42    HTTP      78 POST /webchat/chat/getmes.php HTTP/1.1  (applic
   4 0.001168   192.168.40.42    192.168.169.130  TCP       60 http > startron [ACK] Seq=1 Ack=510 Win=64240 L
   5 0.005890   192.168.40.42    192.168.169.130  HTTP     312 HTTP/1.1 200 OK  (text/html)
   6 0.105068   192.168.40.42    192.168.169.130  HTTP     312 [TCP Retransmission] HTTP/1.1 200 OK  (text/htm
   7 0.105095   192.168.169.130  192.168.40.42    TCP       54 startron > http [ACK] Seq=510 Ack=259 Win=64240
   8 0.718654   192.168.169.130  192.168.169.2    NBNS     110 Refresh NB FRANKLIN1990<20>
   9 1.016683   192.168.169.130  192.168.40.42    TCP      539 [TCP segment of a reassembled PDU]
  10 1.016835   192.168.40.42    192.168.169.130  TCP       60 http > nim [ACK] Seq=1 Ack=486 Win=64240 Len=0
  11 1.016856   192.168.169.130  192.168.40.42    HTTP      78 POST /webchat/chat/getmes.php HTTP/1.1  (applic
  12 1.017016   192.168.40.42    192.168.169.130  TCP       60 http > nim [ACK] Seq=1 Ack=510 Win=64240 Len=0
  13 1.019702   192.168.40.42    192.168.169.130  HTTP     312 HTTP/1.1 200 OK  (text/html)
  14 1.119123   192.168.40.42    192.168.169.130  HTTP     312 [TCP Retransmission] HTTP/1.1 200 OK  (text/htm

⊞ Frame 8: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
⊞ Ethernet II, Src: Vmware_45:4e:21 (00:0c:29:45:4e:21), Dst: Vmware_ed:ab:3b (00:50:56:ed:ab:3b)
⊞ Internet Protocol Version 4, Src: 192.168.169.130 (192.168.169.130), Dst: 192.168.169.2 (192.168.169.2)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
⊞ NetBIOS Name Service

0000  00 50 56 ed ab 3b 00 0c  29 45 4e 21 08 00 45 00   .PV..;.. )EN!..E.
0010  00 60 02 b3 00 00 80 11  64 04 c0 a8 a9 82 c0 a8   .`...... d.......
0020  a9 02 00 89 00 89 00 4c  bf 9e 80 1e 40 00 00 01   .......L ....@...
0030  00 00 00 00 00 01 20 45  47 46 43 45 42 45 4f 45   ...... E GFCEBEOE
0040  4c 45 4d 45 4a 45 4f 44  42 44 4a 44 4a 44 41 43   LEMEJEOD BDJDJDAC
0050  41 43 41 43 41 43 41 00  00 20 00 01 c0 0c 00 20   ACACACA. . .....

File: "E:\防火墙\实验\1...   Packets: 14295 · Displayed: 14295 (100.0%) · Load time: 0:00.359   Profile: Default
```

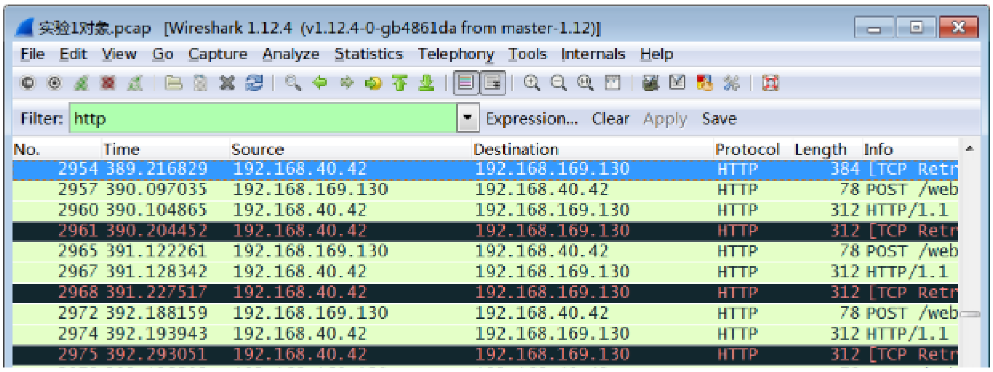
1、**协议统计**：在菜单中选择Statistics，然后选择Protocol Hierarchy，就可以统计出所在数据包中所含的IP协议、应用层协议。



Display filter: none

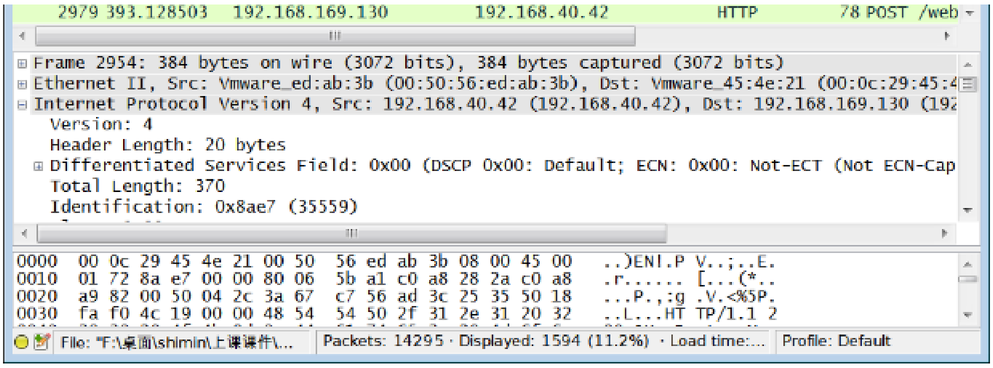
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100.00 %	14295	100.00 %	8480861	0.133	0	0	0.000
⊟ Ethernet	100.00 %	14295	100.00 %	8480861	0.133	0	0	0.000
⊟ Internet Protocol Version 4	99.88 %	14278	99.97 %	8477925	0.133	0	0	0.000
⊟ Transmission Control Protocol	99.20 %	14180	99.80 %	8463646	0.133	12580	8088534	0.127
⊟ Hypertext Transfer Protocol	10.98 %	1570	4.36 %	369700	0.006	1	267	0.000
HTML Form URL Encoded	3.68 %	526	0.49 %	41473	0.001	526	41473	0.001
Line-based text data	7.29 %	1042	3.85 %	326762	0.005	1042	326762	0.005
MIME Multipart Media Encapsulation	0.01 %	1	0.01 %	1198	0.000	1	1198	0.000
Secure Sockets Layer	0.01 %	2	0.00 %	182	0.000	2	182	0.000
⊟ NetBIOS Session Service	0.20 %	28	0.06 %	5230	0.000	2	186	0.000
⊟ SMB (Server Message Block Protocol)	0.18 %	26	0.06 %	5044	0.000	22	4342	0.000
⊟ SMB Pipe Protocol	0.03 %	4	0.01 %	702	0.000	0	0	0.000
Microsoft Windows Lanman Remote API Protocol	0.03 %	4	0.01 %	702	0.000	4	702	0.000
⊟ User Datagram Protocol	0.67 %	96	0.17 %	14131	0.000	0	0	0.000
NetBIOS Name Service	0.45 %	65	0.08 %	7084	0.000	65	7084	0.000
⊟ NetBIOS Datagram Service	0.02 %	3	0.01 %	754	0.000	0	0	0.000
⊟ SMB (Server Message Block Protocol)	0.02 %	3	0.01 %	754	0.000	0	0	0.000
⊟ SMB MailSlot Protocol	0.02 %	3	0.01 %	754	0.000	0	0	0.000

2、**数据过滤**：由于抓包数据看起来比较杂乱，可以根据需求在Filter对话框中输入命令进行过滤。将http包过滤出来。


实验1对象.pcap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http

```
No.   Time        Source           Destination      Protocol Length Info
 2954 389.216829  192.168.40.42    192.168.169.130  HTTP     384 [TCP Retr
 2957 390.097035  192.168.169.130  192.168.40.42    HTTP      78 POST /web
 2960 390.104865  192.168.40.42    192.168.169.130  HTTP     312 HTTP/1.1
 2961 390.204452  192.168.40.42    192.168.169.130  HTTP     312 [TCP Retr
 2965 391.122261  192.168.169.130  192.168.40.42    HTTP      78 POST /web
 2967 391.128342  192.168.40.42    192.168.169.130  HTTP     312 HTTP/1.1
 2968 391.227517  192.168.40.42    192.168.169.130  HTTP     312 [TCP Retr
 2972 392.188159  192.168.169.130  192.168.40.42    HTTP      78 POST /web
 2974 392.193943  192.168.40.42    192.168.169.130  HTTP     312 HTTP/1.1
 2975 392.293051  192.168.40.42    192.168.169.130  HTTP     312 [TCP Retr
```

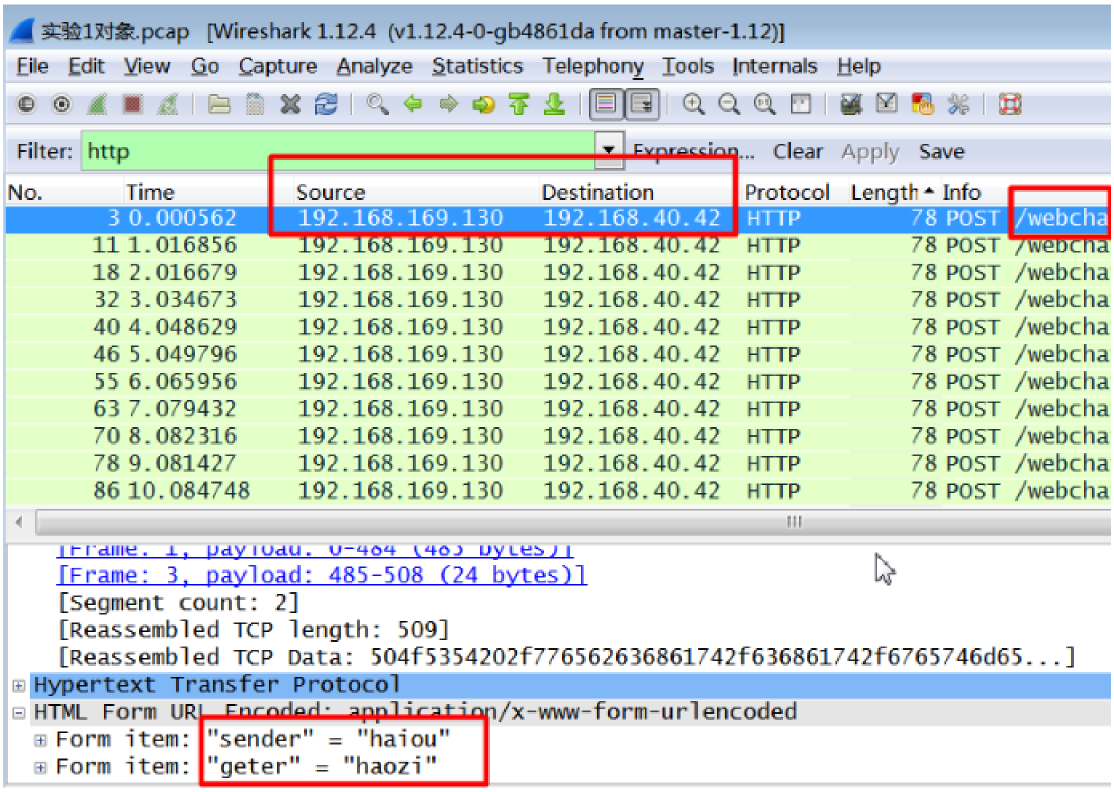


```
2979 393.128503   192.168.169.130        192.168.40.42          HTTP          78 POST /web
```

```
⊞ Frame 2954: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits)
⊞ Ethernet II, Src: Vmware_ed:ab:3b (00:50:56:ed:ab:3b), Dst: Vmware_45:4e:21 (00:0c:29:45:4
⊟ Internet Protocol Version 4, Src: 192.168.40.42 (192.168.40.42), Dst: 192.168.169.130 (192
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Cap
    Total Length: 370
    Identification: 0x8ae7 (35559)
```

```
0000  00 0c 29 45 4e 21 00 50  56 ed ab 3b 08 00 45 00   ..)EN!.P V..;..E.
0010  01 72 8a e7 00 00 80 06  5b a1 c0 a8 28 2a c0 a8   .r...... [...(*..
0020  a9 82 00 50 04 2c 3a 67  c7 56 ad 3c 25 35 50 18   ...P.,:g .V.<%5P.
0030  fa f0 4c 19 00 00 48 54  54 50 2f 31 2e 31 20 32   ..L...HT TP/1.1 2
```

File: "F:\桌面\shimin\上课课件\...
Packets: 14295 · Displayed: 1594 (11.2%) · Load time:...
Profile: Default

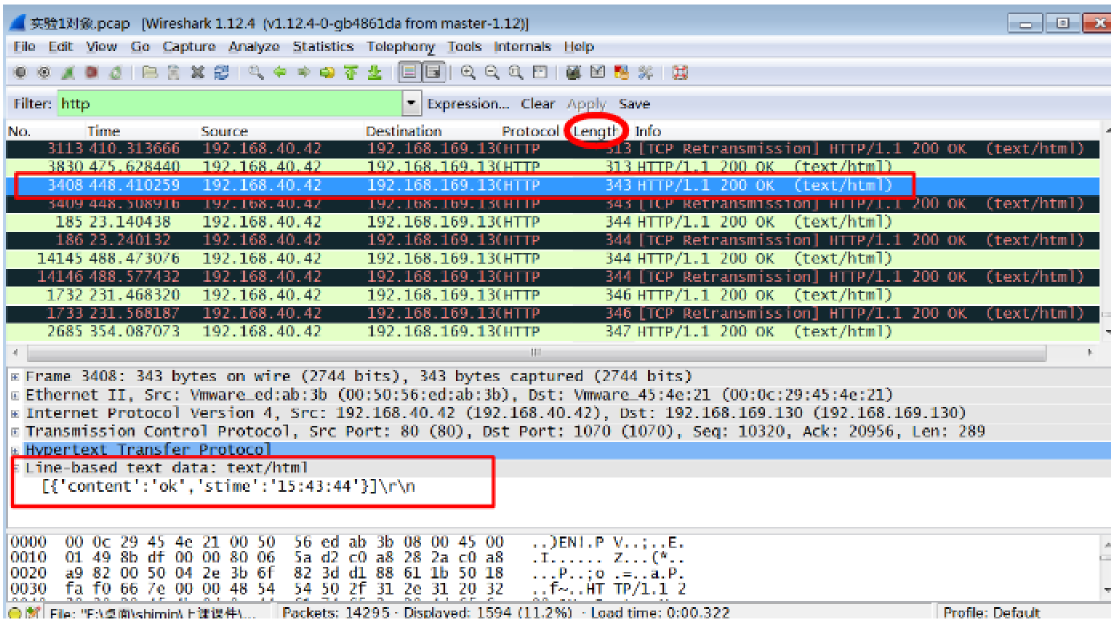


实验1对象.pcap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

```
No.   Time        Source            Destination       Protocol  Length ▲ Info
    3 0.000562    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   11 1.016856    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   18 2.016679    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   32 3.034673    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   40 4.048629    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   46 5.049796    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   55 6.065956    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   63 7.079432    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   70 8.082316    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   78 9.081427    192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
   86 10.084748   192.168.169.130   192.168.40.42     HTTP          78 POST /webcha
```

```
    [Frame: 1, payload: 0-484 (485 bytes)]
    [Frame: 3, payload: 485-508 (24 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 509]
    [Reassembled TCP Data: 504f5354202f77656263686174f636861742f6765746d65...]
⊞ Hypertext Transfer Protocol
⊟ HTML Form URL Encoded: application/x-www-form-urlencoded
  ⊞ Form item: "sender" = "haiou"
  ⊞ Form item: "geter" = "haozi"
```

-分析：可知双方微信聊天的ip地址以及ID。



实验1对象.pcap [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: http
Expression... Clear Apply Save

```
No.     Time          Source           Destination      Protocol Length Info
 3113 410.313666    192.168.40.42    192.168.169.13(HTTP     313 [TCP Retransmission] HTTP/1.1 200 OK  (text/html)
 3830 475.628440    192.168.40.42    192.168.169.13(HTTP     313 HTTP/1.1 200 OK  (text/html)
 3408 448.410259    192.168.40.42    192.168.169.13(HTTP     343 HTTP/1.1 200 OK  (text/html)
 3409 448.508916    192.168.40.42    192.168.169.13(HTTP     343 [TCP Retransmission] HTTP/1.1 200 OK  (text/html)
  185 23.140438     192.168.40.42    192.168.169.13(HTTP     344 HTTP/1.1 200 OK  (text/html)
  186 23.240132     192.168.40.42    192.168.169.13(HTTP     344 [TCP Retransmission] HTTP/1.1 200 OK  (text/html)
14145 488.473076    192.168.40.42    192.168.169.13(HTTP     344 HTTP/1.1 200 OK  (text/html)
14146 488.577432    192.168.40.42    192.168.169.13(HTTP     344 [TCP Retransmission] HTTP/1.1 200 OK  (text/html)
 1732 231.468320    192.168.40.42    192.168.169.13(HTTP     346 HTTP/1.1 200 OK  (text/html)
 1733 231.568187    192.168.40.42    192.168.169.13(HTTP     346 [TCP Retransmission] HTTP/1.1 200 OK  (text/html)
 2685 354.087073    192.168.40.42    192.168.169.13(HTTP     347 HTTP/1.1 200 OK  (text/html)
```

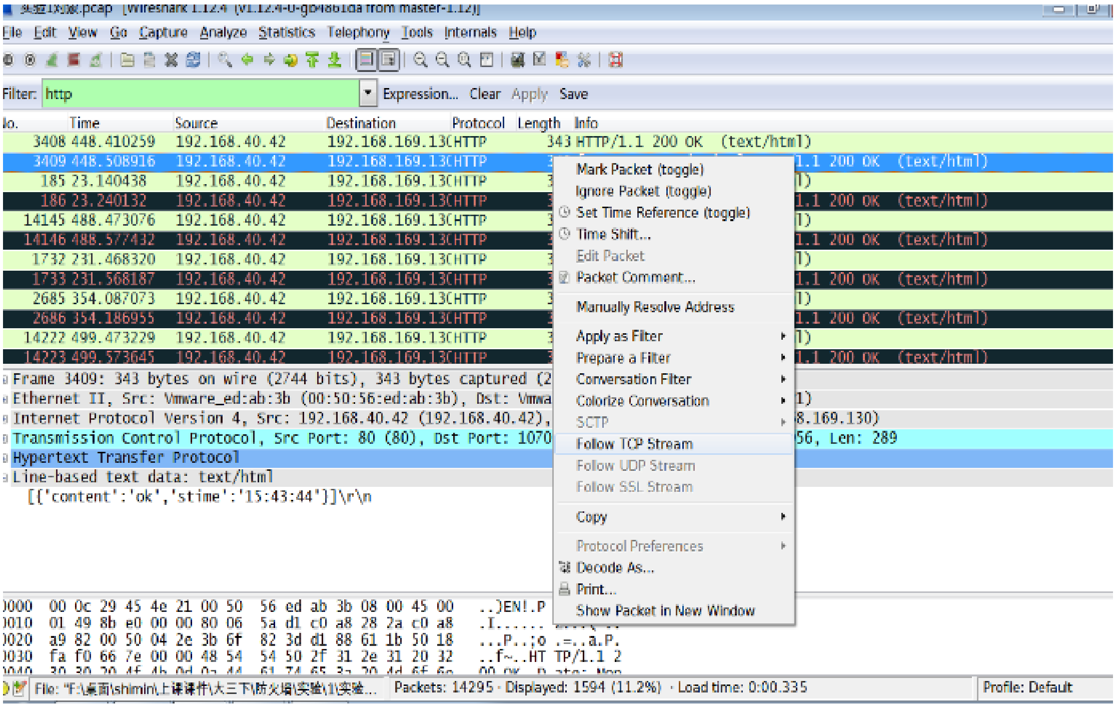
```
⊞ Frame 3408: 343 bytes on wire (2744 bits), 343 bytes captured (2744 bits)
⊞ Ethernet II, Src: Vmware_ed:ab:3b (00:50:56:ed:ab:3b), Dst: Vmware_45:4e:21 (00:0c:29:45:4e:21)
⊞ Internet Protocol Version 4, Src: 192.168.40.42 (192.168.40.42), Dst: 192.168.169.130 (192.168.169.130)
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1070 (1070), Seq: 10320, Ack: 20956, Len: 289
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: text/html
    [{'content':'ok','stime':'15:43:44'}]\r\n
```

```
0000  00 0c 29 45 4e 21 00 50  56 ed ab 3b 08 00 45 00   ..)EN!.P V..;..E.
0010  01 49 8b df 00 00 80 06  5a d2 c0 a8 28 2a c0 a8   .I...... Z...(*..
0020  a9 82 00 50 04 2e 3b 6f  82 3d d1 88 61 1b 50 18   ...P..;o .=..a.P.
0030  fa f0 66 7e 00 00 48 54  54 50 2f 31 2e 31 20 32   ..f~..HT TP/1.1 2
```

File: "F:\桌面\shimin\上课课件\...
Packets: 14295 · Displayed: 1594 (11.2%) · Load time: 0:00.322
Profile: Default

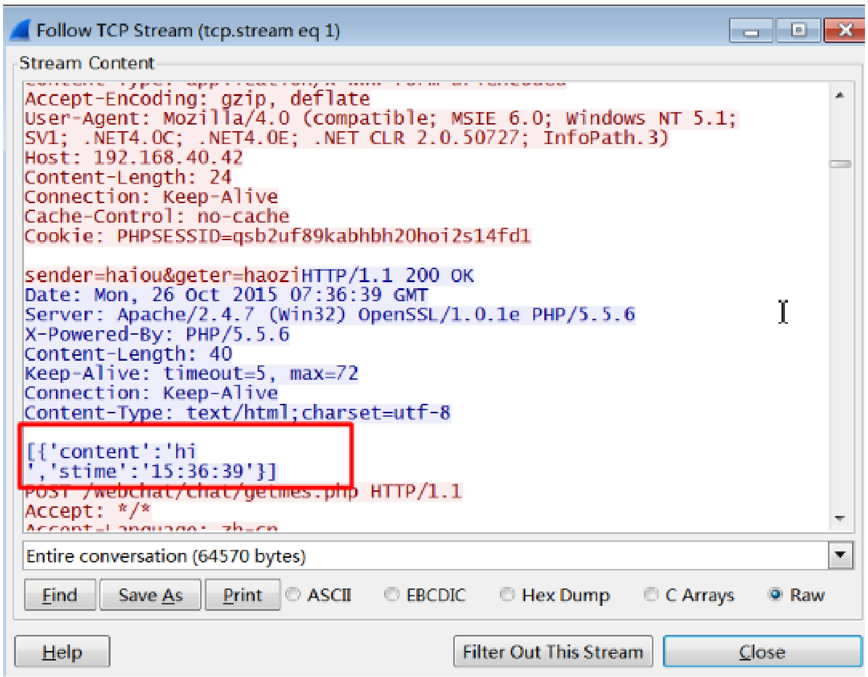
-分析：按Length递增排列分类，点击Length大于343时的包时发现其中含有聊天记录。

3、**使用”Follow TCP Stream”查看Tcp流中的应用层数据。**在包列表中选择一个包，然后选择Wireshark工具栏菜单的”Following TCP Streams”选项(或者使用包列表鼠标右键的上下文菜单)。然后，Wireshark就会创建合适的显示过滤器，并弹出一个对话框显示TCP流的所有数据。流的内容出现的顺序同他们在网络中出现的顺序一致。从A到B的通信标记为红色，从B到A的通信标记为蓝色。非打印字符将会被显示为圆点。



```
No.     Time         Source          Destination      Protocol Length Info
   3408 448.410259   192.168.40.42   192.168.169.13(HTTP        343 HTTP/1.1 200 OK  (text/html)
   3409 448.508916   192.168.40.42   192.168.169.13(HTTP          3 1.1 200 OK  (text/html)
    185 23.140438    192.168.40.42   192.168.169.13(HTTP          3 l)
    186 23.240132    192.168.40.42   192.168.169.13(HTTP          3 1.1 200 OK  (text/html)
  14145 488.473076   192.168.40.42   192.168.169.13(HTTP          3 l)
  14146 488.577432   192.168.40.42   192.168.169.13(HTTP          3 1.1 200 OK  (text/html)
   1732 231.468320   192.168.40.42   192.168.169.13(HTTP          3 l)
   1733 231.568187   192.168.40.42   192.168.169.13(HTTP          3 1.1 200 OK  (text/html)
   2685 354.087073   192.168.40.42   192.168.169.13(HTTP          3 l)
   2686 354.186955   192.168.40.42   192.168.169.13(HTTP          3 1.1 200 OK  (text/html)
  14222 499.473229   192.168.40.42   192.168.169.13(HTTP          3 l)
  14223 499.573645   192.168.40.42   192.168.169.13(HTTP          3 1.1 200 OK  (text/html)

Frame 3409: 343 bytes on wire (2744 bits), 343 bytes captured (2
Ethernet II, Src: Vmware_ed:ab:3b (00:50:56:ed:ab:3b), Dst: Vmwa                                  l)
Internet Protocol Version 4, Src: 192.168.40.42 (192.168.40.42),                                   8.169.130)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1070                                   56, Len: 289
Hypertext Transfer Protocol
Line-based text data: text/html
   [{'content':'ok','stime':'15:43:44'}]\r\n

0000  00 0c 29 45 4e 21 00 50  56 ed ab 3b 08 00 45 00   ..)EN!.P
0010  01 49 8b e0 00 00 80 06  5a d1 c0 a8 28 2a c0 a8   .I......
0020  a9 82 00 50 04 2e 3b 6f  82 3d d1 88 61 1b 50 18   ...P..;o .=..a.P.
0030  fa f0 66 7e 00 00 48 54  54 50 2f 31 2e 31 20 32   ..f~..HT TP/1.1 2
```

File: "F:\桌面\shimin\上课课件\大三下\防火墙\实验\1\实验...   Packets: 14295 · Displayed: 1594 (11.2%) · Load time: 0:00.335   Profile: Default



```
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; InfoPath.3)
Host: 192.168.40.42
Content-Length: 24
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=qsb2uf89kabhbh20hoi2s14fd1

sender=haiou&geter=haoziHTTP/1.1 200 OK
Date: Mon, 26 Oct 2015 07:36:39 GMT
Server: Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.6
X-Powered-By: PHP/5.5.6
Content-Length: 40
Keep-Alive: timeout=5, max=72
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

[{'content':'hi
','stime':'15:36:39'}]
POST /webchat/chat/getmes.php HTTP/1.1
Accept: */*
```

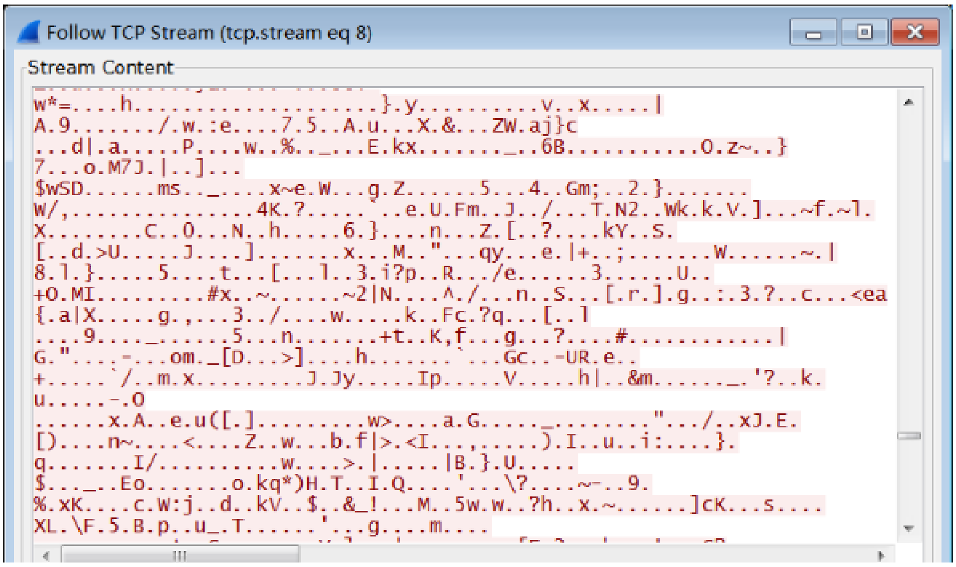
- 分析：截取出如下聊天记录

```
    [{'content':'hi','stime':'15:36:39'}]
    content=i am here what?&sender=haiou&geter=haozi 15:36:48
    [{'content':'next week','stime':'15:37:07'}]
    [{'content':'we can go somewhere to have a rest','stime':'15:37:30'}]
    [{'content':'where are you going ?','stime':'15:38:05'}]
    content=i don't have idea&sender=haiou&geter=haozi
    [{'content':'how about tangshang','stime':'15:38:25'}]
    content=but i was born in tangshan&sender=haiou&geter=haozi
    [{'content':'wow....','stime':'15:38:47'}]
    [{'content':'then how about tianyahaijiao','stime':'15:38:57'}]
    content=sounds like not bad&sender=haiou&geter=haozi
    content=where is that?&sender=haiou&geter=haozi
    [{'content':'i ....do not know','stime':'15:39:30'}]
    [{'content':'but i can check in my map img','stime':'15:39:43'}]
    content=if it is a place with water....&sender=haiou&geter=haozi
    [{'content':'then?','stime':'15:40:06'}]
    content=i can not swim&sender=haiou&geter=haozi
    [{'content':'god....','stime':'15:40:20'}]
    [{'content':'then...you dont want go anywhere?','stime':'15:40:38'}]
    content=i have no idea&sender=haiou&geter=haozi
    [{'content':'how about wangsicong 100?','stime':'15:41:36'}]
    content=what meaning?&sender=haiou&geter=haozi
    [{'content':'how about wangsicong 100?','stime':'15:41:52'}]
    [{'content':'guominlaogong ','stime':'15:42:05'}]
    [{'content':'lol...','stime':'15:42:10'}]
    content=what is 100?&sender=haiou&geter=haoziHTTP/1.1 200 OK
    [{'content':'his family has alot of building..you know..','stime':'15:42:44'}]
    content=yes....&sender=haiou&geter=haozi
    content=but i really do not know the way&sender=haiou&geter=haozi
    content=canyou show me the way in the map?&sender=haiou&geter=haozi
    [{'content':'ok','stime':'15:43:44'}]
    [{'content':'upload to me','stime':'15:43:49'}]
    content=ok&sender=haiou&geter=haozi
    content=see that?&sender=haiou&geter=haoziHTTP/1.1 200 OK
    [{'content':'well! ','stime':'15:44:35'}]
```

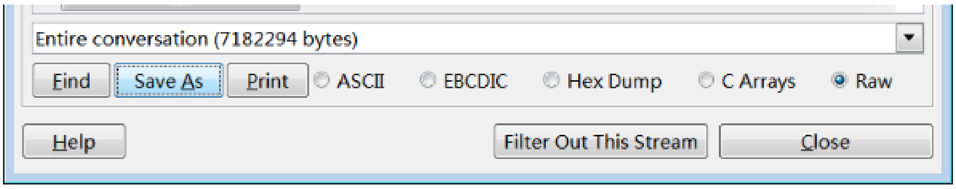
他们聊天的内容是计划下周的出行目的地是“王思聪 100”（他家的建筑），有传图。

4、**还原图片：**利用WinHex软件

（1）将TCP流另存为temp.bin

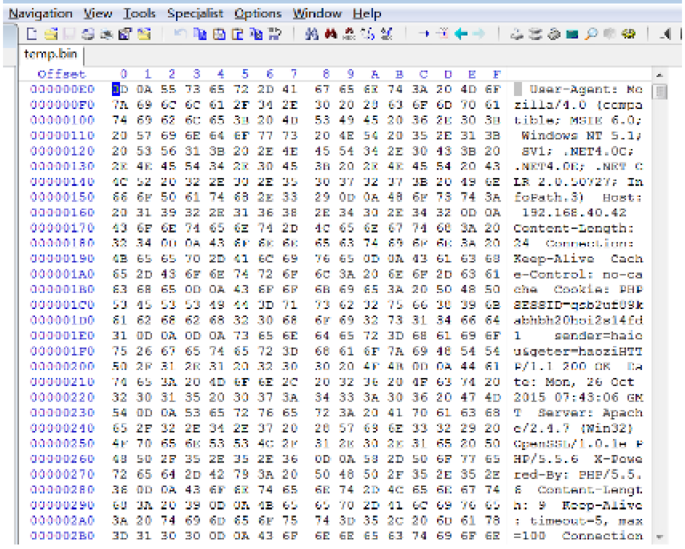


```
w*=....h....................}.y..........v..x.....|
A.9......./.w.:e....7.5..A.u...X.&...ZW.aj}c
...d|.a.....P....w..%.._...E.kx......._..6B...........O.z~..}
7...o.M7J.|..]...
$wSD......ms.._.....x~e.W...g.Z......5...4..Gm;..2.}.......
W/,................4K.?...... ..e.U.Fm..J../...T.N2..Wk.k.V.]...~f.~l.
X........C..O...N..h.....6.}....n...Z.[..?....kY..S.
[..d.>U.....J....]........x...M.."...qy...e.|+..;.......W......~.|
8.l.}.....5....t...[...l..3.i?p..R.../e......3......U..
+O.MI.........#x..~.......~2|N....^./...n..S...[.r.].g..:.3.?..c...<ea
{.a|X.....g.,...3../....w.....k..Fc.?q...[..l
....9...._......5...n.......+t..K,f...g...?....#.............|
G."....-...om._[D...>]....h....... ...Gc..-UR.e..
+.....`/..m.x..........J.Jy.....Ip.....V.....h|..&m......_.'?..k.
u.....-.O
.......x.A..e.u([.].........w>....a.G...._.........."..../..xJ.E.
[)....n~....<....Z..w...b.f|>.<I...,......).I..u..i:....}.
q.......I/..........w....>.|.....|B.}.U.....
$..._..Eo........o.kq*)H.T..I.Q....'...\?....~-..9.
%.xK....c.W:j..d..kV..$..&_!...M..5w.w..?h..x.~......]cK...s....
XL.\F.5.B.p..u_.T......'...g....m....
```



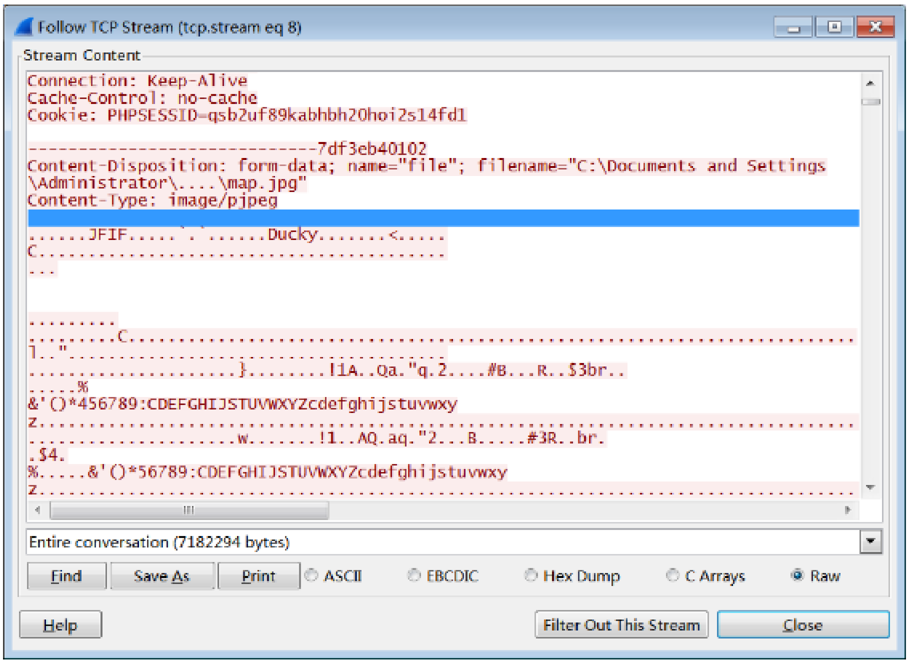
（2）利用WinHex从保存的原始文件中将上传的图片还原出来

将保存的temp.bin用WinHex打开，可以看到文件中包含HTTP请求信息以及我们的图片信息，还有文件结尾的尾部信息。需要确定图片文件的原始信息头和尾，并去掉多余的部分。



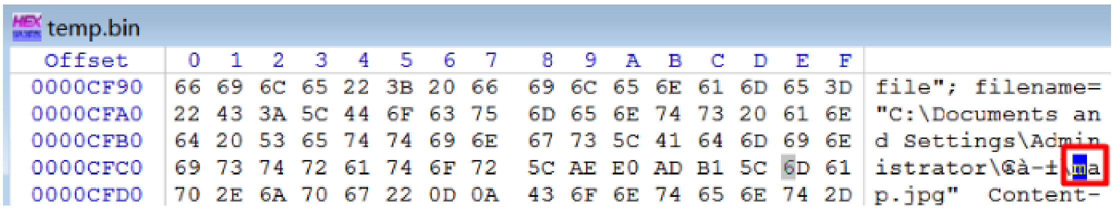
```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000E0   0D 0A 55 73 65 72 2D 41  67 65 6E 74 3A 20 4D 6F    User-Agent: Mo
000000F0   7A 69 6C 6C 61 2F 34 2E  30 20 28 63 6F 6D 70 61  zilla/4.0 (compa
00000100   74 69 62 6C 65 3B 20 4D  53 49 45 20 36 2E 30 3B  tible; MSIE 6.0;
00000110   20 57 69 6E 64 6F 77 73  20 4E 54 20 35 2E 31 3B   Windows NT 5.1;
00000120   20 53 56 31 3B 20 2E 4E  45 54 34 2E 30 43 3B 20   SV1; .NET4.0C;
00000130   2E 4E 45 54 34 2E 30 45  3B 20 2E 4E 45 54 20 43  .NET4.0E; .NET C
00000140   4C 52 20 32 2E 30 2E 35  30 37 32 37 3B 20 49 6E  LR 2.0.50727; In
00000150   66 6F 50 61 74 68 2E 33  29 0D 0A 48 6F 73 74 3A  foPath.3)  Host:
00000160   20 31 39 32 2E 31 36 38  2E 34 30 2E 34 32 0D 0A   192.168.40.42
00000170   43 6F 6E 74 65 6E 74 2D  4C 65 6E 67 74 68 3A 20  Content-Length:
00000180   32 34 0D 0A 43 6F 6E 6E  65 63 74 69 6F 6E 3A 20  24  Connection:
00000190   4B 65 65 70 2D 41 6C 69  76 65 0D 0A 43 61 63 68  Keep-Alive  Cach
000001A0   65 2D 43 6F 6E 74 72 6F  6C 3A 20 6E 6F 2D 63 61  e-Control: no-ca
000001B0   63 68 65 0D 0A 43 6F 6F  6B 69 65 3A 20 50 48 50  che  Cookie: PHP
000001C0   53 45 53 53 49 44 3D 71  73 62 32 75 66 38 39 6B  SESSID=qsb2uf89k
000001D0   61 62 68 62 68 32 30 68  6F 69 32 73 31 34 66 64  abhbh20hoi2s14fd
000001E0   31 0D 0A 0D 0A 73 65 6E  64 65 72 3D 68 61 69 6F  1    sender=haio
000001F0   75 26 67 65 74 65 72 3D  68 61 6F 7A 69 48 54 54  u&geter=haoziHTT
00000200   50 2F 31 2E 31 20 32 30  30 20 4F 4B 0D 0A 44 61  P/1.1 200 OK  Da
00000210   74 65 3A 20 4D 6F 6E 2C  20 32 36 20 4F 63 74 20  te: Mon, 26 Oct
00000220   32 30 31 35 20 30 37 3A  34 33 3A 30 36 20 47 4D  2015 07:43:06 GM
00000230   54 0D 0A 53 65 72 76 65  72 3A 20 41 70 61 63 68  T  Server: Apach
00000240   65 2F 32 2E 34 2E 37 20  28 57 69 6E 33 32 29 20  e/2.4.7 (Win32)
00000250   4F 70 65 6E 53 53 4C 2F  31 2E 30 2E 31 65 20 50  OpenSSL/1.0.1e P
00000260   48 50 2F 35 2E 35 2E 36  0D 0A 58 2D 50 6F 77 65  HP/5.5.6  X-Powe
00000270   72 65 64 2D 42 79 3A 20  50 48 50 2F 35 2E 35 2E  red-By: PHP/5.5.
00000280   36 0D 0A 43 6F 6E 74 65  6E 74 2D 4C 65 6E 67 74  6  Content-Lengt
00000290   68 3A 20 39 0D 0A 4B 65  65 70 2D 41 6C 69 76 65  h: 9  Keep-Alive
000002A0   3A 20 74 69 6D 65 6F 75  74 3D 35 2C 20 6D 61 78  : timeout=5, max
000002B0   3D 31 30 30 0D 0A 43 6F  6E 6E 65 63 74 69 6F 6E  =100  Connection
```

回到Wireshark中，会看到我们刚才的数据流中关于图片的头部分。

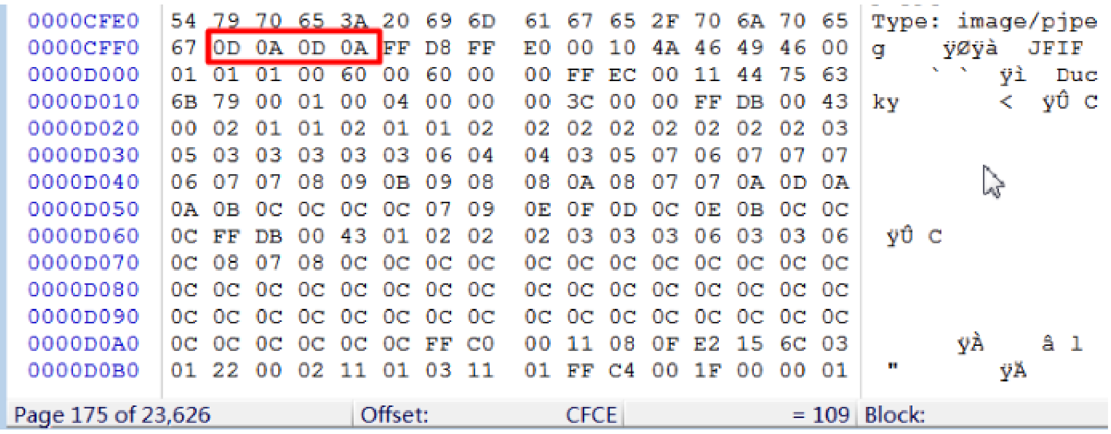


```
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=qsb2uf89kabhbh20hoi2s14fd1

-----------------------------7df3eb40102
Content-Disposition: form-data; name="file"; filename="C:\Documents and Settings
\Administrator\....\map.jpg"
Content-Type: image/pjpeg

......JFIF.....`.`......Ducky.......<.....
C.........................................
...


..........
.........C........................................................................
l.."......................................
.......................}........!1A..Qa."q.2....#B...R..$3br..
.....%
&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxy
z.................................................................................
.......................w.......!1..AQ.aq."2...B.....#3R..br.
.$4.
%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxy
z.................................................................................
```

在Content-Type: image/pjpeg后面有两个换行符，在原始文件中换行符用十六进制表示是 “0D 0A”，因为有两个，所以我们在图片名字map.jpg附近寻找“0D 0A 0D 0A”，后面的部分就表示图片的开始。



```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0000CF90    66 69 6C 65 22 3B 20 66  69 6C 65 6E 61 6D 65 3D  file"; filename=
0000CFA0    22 43 3A 5C 44 6F 63 75  6D 65 6E 74 73 20 61 6E  "C:\Documents an
0000CFB0    64 20 53 65 74 74 69 6E  67 73 5C 41 64 6D 69 6E  d Settings\Admin
0000CFC0    69 73 74 72 61 74 6F 72  5C AE E0 AD B1 5C 6D 61  istrator\®à-±\ma
0000CFD0    70 2E 6A 70 67 22 0D 0A  43 6F 6E 74 65 6E 74 2D  p.jpg"  Content-
```

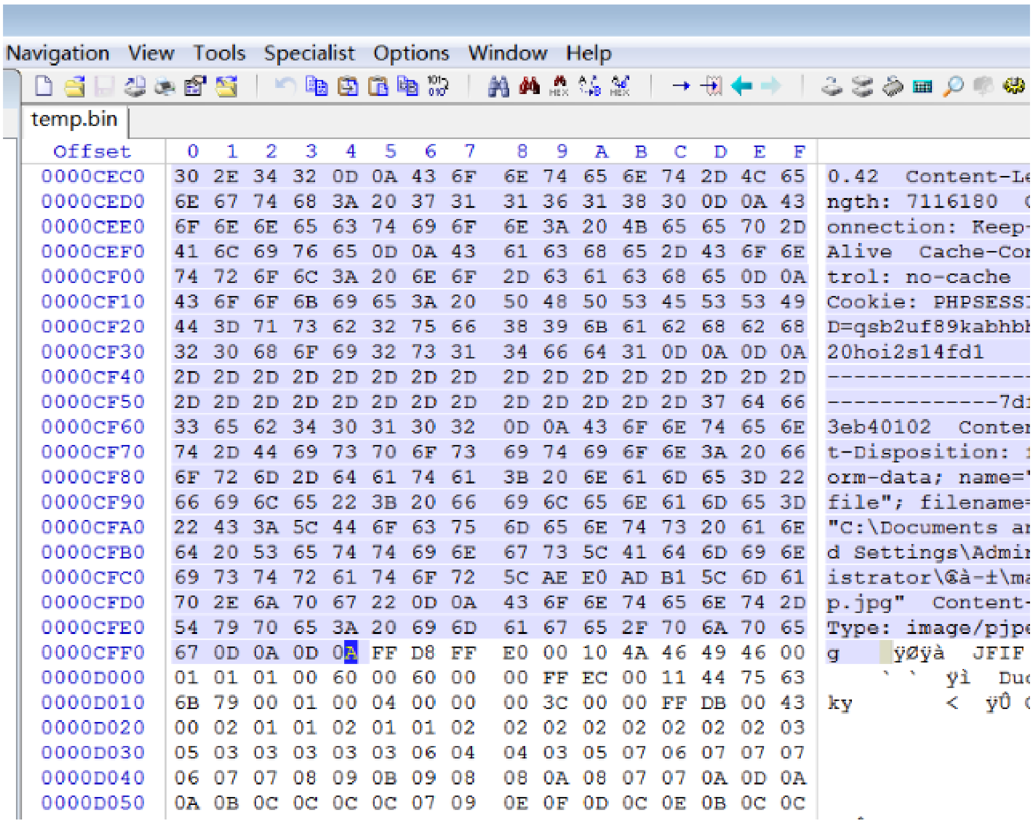


```
0000CFE0  54 79 70 65 3A 20 69 6D  61 67 65 2F 70 6A 70 65  Type: image/pjpe
0000CFF0  67 0D 0A 0D 0A FF D8 FF  E0 00 10 4A 46 49 46 00  g    ÿØÿà  JFIF
0000D000  01 01 01 00 60 00 60 00  00 FF EC 00 11 44 75 63      ` `  ÿì  Duc
0000D010  6B 79 00 01 00 04 00 00  00 3C 00 00 FF DB 00 43  ky        <  ÿÛ C
0000D020  00 02 01 01 02 01 01 02  02 02 02 02 02 02 02 03
0000D030  05 03 03 03 03 03 06 04  04 03 05 07 06 07 07 07
0000D040  06 07 07 08 09 0B 09 08  08 0A 08 07 07 0A 0D 0A
0000D050  0A 0B 0C 0C 0C 0C 07 09  0E 0F 0D 0C 0E 0B 0C 0C
0000D060  0C FF DB 00 43 01 02 02  02 03 03 03 06 03 03 06   ÿÛ C
0000D070  0C 08 07 08 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
0000D080  0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
0000D090  0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
0000D0A0  0C 0C 0C 0C 0C 0C FF C0  00 11 08 0F E2 15 6C 03        ÿÀ    â l
0000D0B0  01 22 00 02 11 01 03 11  01 FF C4 00 1F 00 00 01   "        ÿÄ
Page 175 of 23,626    Offset:    CFCE    = 109  Block:
```

需要去掉图片以上的部分。在00000000偏移处点击alt+1，表示选块开始。

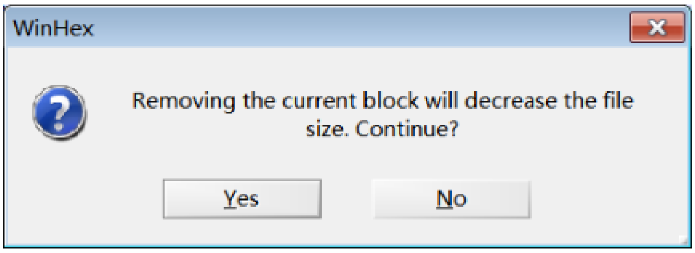
在到的“0D 0A 0D 0A”处的最后一个0A处点击alt+2.表示选块结束。

这时候，就选中了图片之前的多余部分。



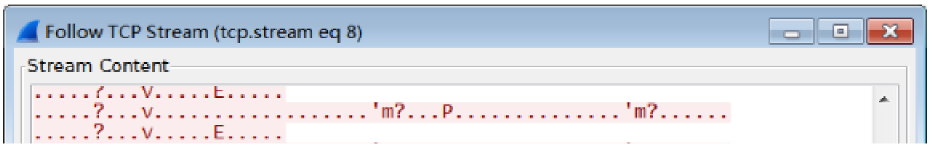
```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0000CEC0  30 2E 34 32 0D 0A 43 6F  6E 74 65 6E 74 2D 4C 65  0.42  Content-Le
0000CED0  6E 67 74 68 3A 20 37 31  31 36 31 38 30 0D 0A 43  ngth: 7116180  C
0000CEE0  6F 6E 6E 65 63 74 69 6F  6E 3A 20 4B 65 65 70 2D  onnection: Keep-
0000CEF0  41 6C 69 76 65 0D 0A 43  61 63 68 65 2D 43 6F 6E  Alive  Cache-Con
0000CF00  74 72 6F 6C 3A 20 6E 6F  2D 63 61 63 68 65 0D 0A  trol: no-cache
0000CF10  43 6F 6F 6B 69 65 3A 20  50 48 50 53 45 53 53 49  Cookie: PHPSESSI
0000CF20  44 3D 71 73 62 32 75 66  38 39 6B 61 62 68 62 68  D=qsb2uf89kabhbh
0000CF30  32 30 68 6F 69 32 73 31  34 66 64 31 0D 0A 0D 0A  20hoi2s14fd1
0000CF40  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  ----------------
0000CF50  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 37 64 66  -------------7df
0000CF60  33 65 62 34 30 31 30 32  0D 0A 43 6F 6E 74 65 6E  3eb40102  Conten
0000CF70  74 2D 44 69 73 70 6F 73  69 74 69 6F 6E 3A 20 66  t-Disposition: f
0000CF80  6F 72 6D 2D 64 61 74 61  3B 20 6E 61 6D 65 3D 22  orm-data; name="
0000CF90  66 69 6C 65 22 3B 20 66  69 6C 65 6E 61 6D 65 3D  file"; filename=
0000CFA0  22 43 3A 5C 44 6F 63 75  6D 65 6E 74 73 20 61 6E  "C:\Documents an
0000CFB0  64 20 53 65 74 74 69 6E  67 73 5C 41 64 6D 69 6E  d Settings\Admin
0000CFC0  69 73 74 72 61 74 6F 72  5C AE E0 AD B1 5C 6D 61  istrator\®à-±\ma
0000CFD0  70 2E 6A 70 67 22 0D 0A  43 6F 6E 74 65 6E 74 2D  p.jpg"  Content-
0000CFE0  54 79 70 65 3A 20 69 6D  61 67 65 2F 70 6A 70 65  Type: image/pjpe
0000CFF0  67 0D 0A 0D 0A FF D8 FF  E0 00 10 4A 46 49 46 00  g    ÿØÿà  JFIF
0000D000  01 01 01 00 60 00 60 00  00 FF EC 00 11 44 75 63      ` `  ÿì  Duc
0000D010  6B 79 00 01 00 04 00 00  00 3C 00 00 FF DB 00 43  ky        <  ÿÛ C
0000D020  00 02 01 01 02 01 01 02  02 02 02 02 02 02 02 03
0000D030  05 03 03 03 03 03 06 04  04 03 05 07 06 07 07 07
0000D040  06 07 07 08 09 0B 09 08  08 0A 08 07 07 0A 0D 0A
0000D050  0A 0B 0C 0C 0C 0C 07 09  0E 0F 0D 0C 0E 0B 0C 0C
```

按下delete键，将文件中的多余头部确认删除。

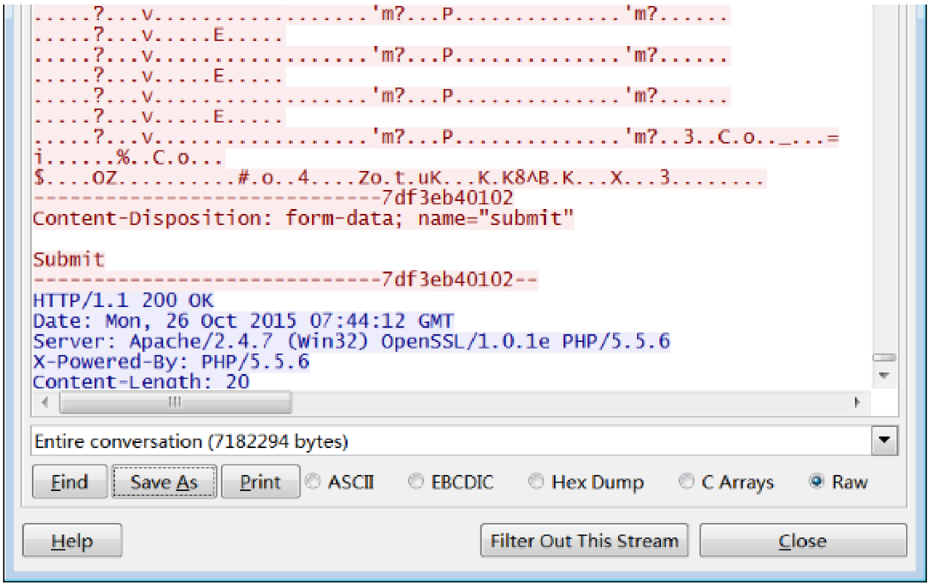


Removing the current block will decrease the file size. Continue?

回到wireshark中，看看图片传送完毕之后的尾部部分。可以看到，这次是一个换行符，后面有些文件结束标志“————”。

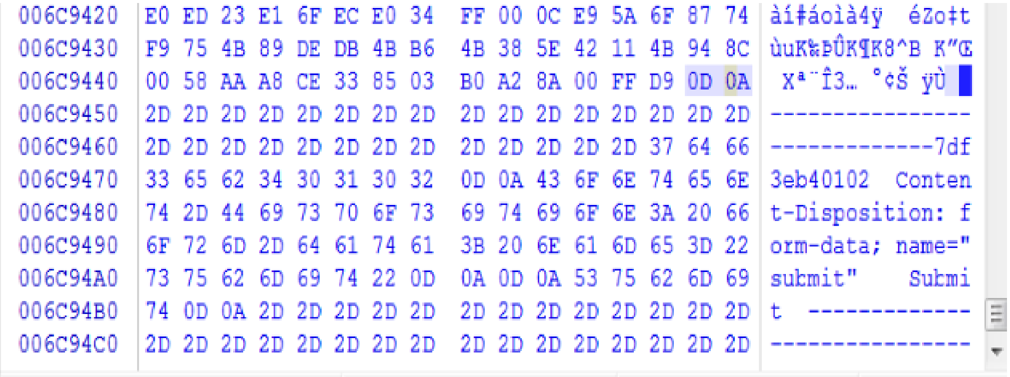


```
....../...V.....E.....
......?...V.....................'m?...P...............'m?......
......?...V.....E.....
```

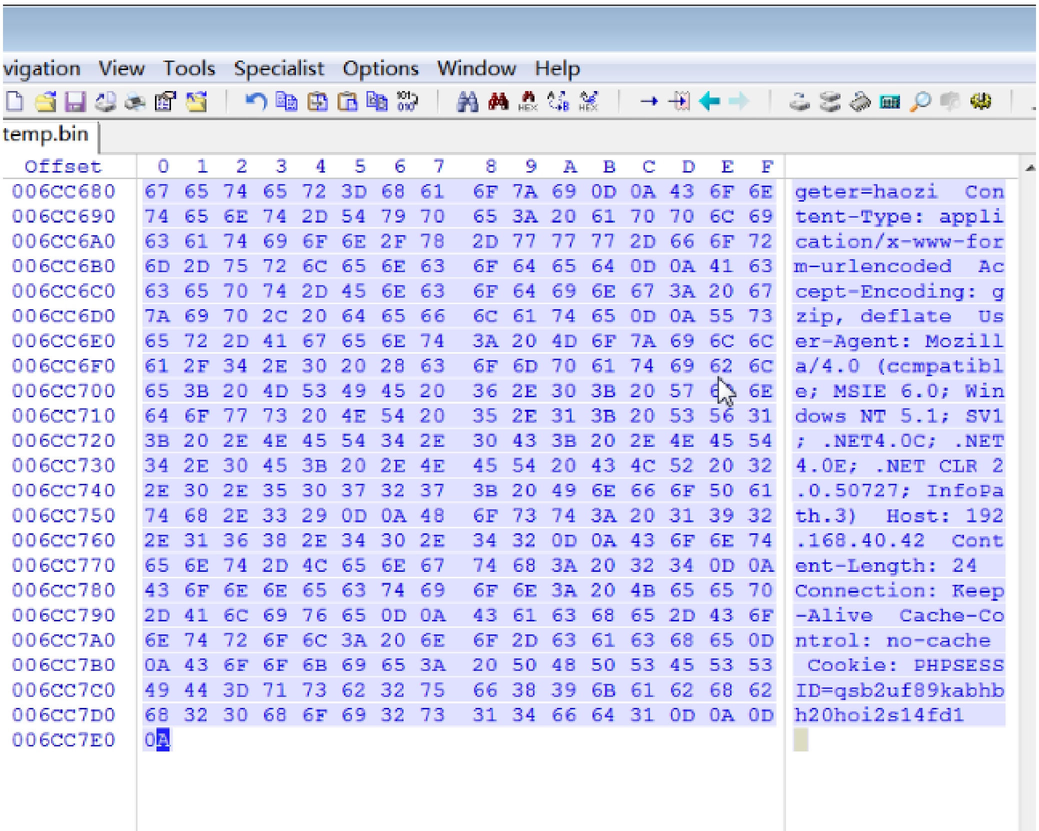


```
.....?...v...................'m?...P..............'m?......
.....?...v.....E.....
.....?...v...................'m?...P..............'m?......
.....?...v.....E.....
.....?...v...................'m?...P..............'m?......
.....?...v.....E.....
.....?...v...................'m?...P..............'m?..3..C.o.._...=
i......%..C.o...
$....OZ..........#.o..4....Zo.t.uK...K.K8^B.K...X...3........
-----------------------------7df3eb40102
Content-Disposition: form-data; name="submit"

Submit
-----------------------------7df3eb40102--
HTTP/1.1 200 OK
Date: Mon, 26 Oct 2015 07:44:12 GMT
Server: Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.6
X-Powered-By: PHP/5.5.6
Content-Length: 20
```

同样在原始文件中删除它们。

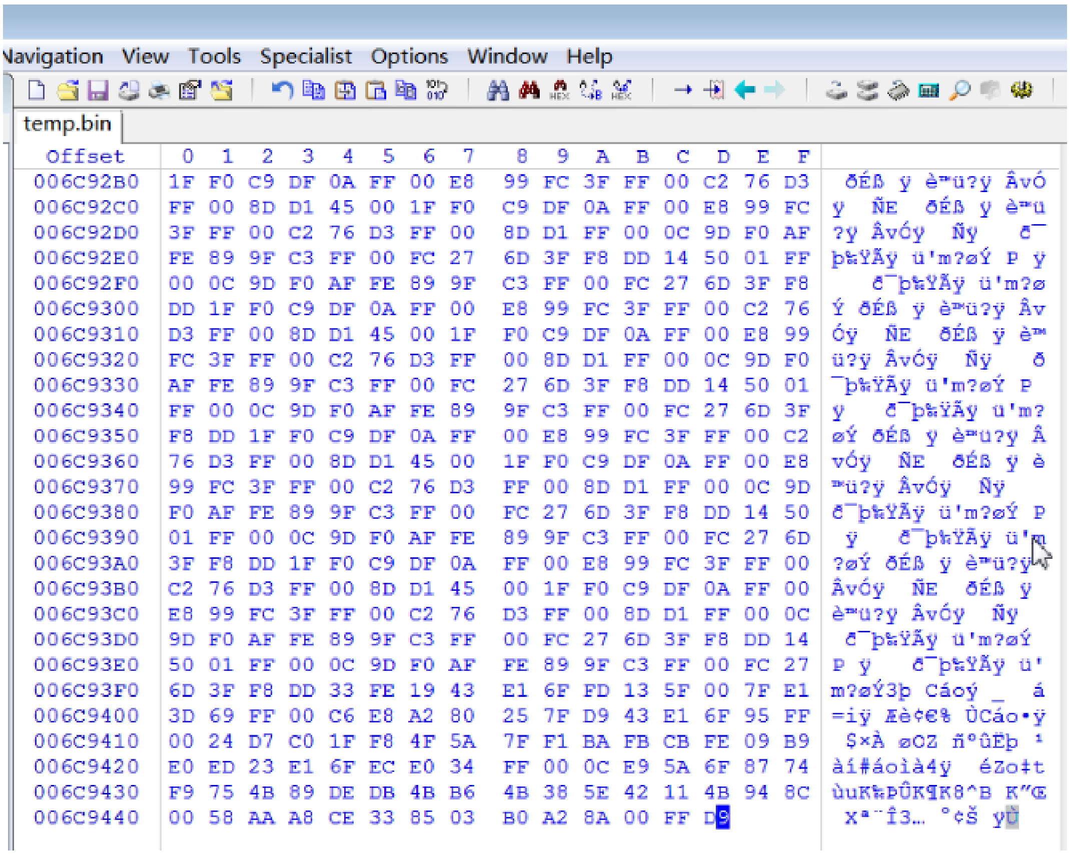


```
006C9420  E0 ED 23 E1 6F EC E0 34  FF 00 0C E9 5A 6F 87 74  àí#áoìà4ÿ éZo‡t
006C9430  F9 75 4B 89 DE DB 4B B6  4B 38 5E 42 11 4B 94 8C  ùuK‰ÞÛK¶K8^B K”Œ
006C9440  00 58 AA A8 CE 33 85 03  B0 A2 8A 00 FF D9 0D 0A   Xª¨Î3… °¢Š ÿÙ
006C9450  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  ----------------
006C9460  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 37 64 66  -------------7df
006C9470  33 65 62 34 30 31 30 32  0D 0A 43 6F 6E 74 65 6E  3eb40102  Conten
006C9480  74 2D 44 69 73 70 6F 73  69 74 69 6F 6E 3A 20 66  t-Disposition: f
006C9490  6F 72 6D 2D 64 61 74 61  3B 20 6E 61 6D 65 3D 22  orm-data; name="
006C94A0  73 75 62 6D 69 74 22 0D  0A 0D 0A 53 75 62 6D 69  submit"    Submi
006C94B0  74 0D 0A 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  t  -------------
006C94C0  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  ----------------
```

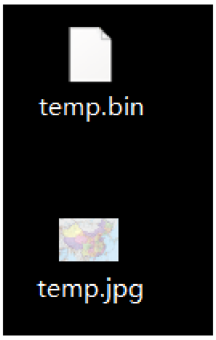


```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
006CC680  67 65 74 65 72 3D 68 61  6F 7A 69 0D 0A 43 6F 6E  geter=haozi  Con
006CC690  74 65 6E 74 2D 54 79 70  65 3A 20 61 70 70 6C 69  tent-Type: appli
006CC6A0  63 61 74 69 6F 6E 2F 78  2D 77 77 77 2D 66 6F 72  cation/x-www-for
006CC6B0  6D 2D 75 72 6C 65 6E 63  6F 64 65 64 0D 0A 41 63  m-urlencoded  Ac
006CC6C0  63 65 70 74 2D 45 6E 63  6F 64 69 6E 67 3A 20 67  cept-Encoding: g
006CC6D0  7A 69 70 2C 20 64 65 66  6C 61 74 65 0D 0A 55 73  zip, deflate  Us
006CC6E0  65 72 2D 41 67 65 6E 74  3A 20 4D 6F 7A 69 6C 6C  er-Agent: Mozill
006CC6F0  61 2F 34 2E 30 20 28 63  6F 6D 70 61 74 69 62 6C  a/4.0 (compatibl
006CC700  65 3B 20 4D 53 49 45 20  36 2E 30 3B 20 57 69 6E  e; MSIE 6.0; Win
006CC710  64 6F 77 73 20 4E 54 20  35 2E 31 3B 20 53 56 31  dows NT 5.1; SV1
006CC720  3B 20 2E 4E 45 54 34 2E  30 43 3B 20 2E 4E 45 54  ; .NET4.0C; .NET
006CC730  34 2E 30 45 3B 20 2E 4E  45 54 20 43 4C 52 20 32  4.0E; .NET CLR 2
006CC740  2E 30 2E 35 30 37 32 37  3B 20 49 6E 66 6F 50 61  .0.50727; InfoPa
006CC750  74 68 2E 33 29 0D 0A 48  6F 73 74 3A 20 31 39 32  th.3)  Host: 192
006CC760  2E 31 36 38 2E 34 30 2E  34 32 0D 0A 43 6F 6E 74  .168.40.42  Cont
006CC770  65 6E 74 2D 4C 65 6E 67  74 68 3A 20 32 34 0D 0A  ent-Length: 24
006CC780  43 6F 6E 6E 65 63 74 69  6F 6E 3A 20 4B 65 65 70  Connection: Keep
006CC790  2D 41 6C 69 76 65 0D 0A  43 61 63 68 65 2D 43 6F  -Alive  Cache-Co
006CC7A0  6E 74 72 6F 6C 3A 20 6E  6F 2D 63 61 63 68 65 0D  ntrol: no-cache
006CC7B0  0A 43 6F 6F 6B 69 65 3A  20 50 48 50 53 45 53 53   Cookie: PHPSESS
006CC7C0  49 44 3D 71 73 62 32 75  66 38 39 6B 61 62 68 62  ID=qsb2uf89kabhb
006CC7D0  68 32 30 68 6F 69 32 73  31 34 66 64 31 0D 0A 0D  h20hoi2s14fd1
006CC7E0  0A
```

这时文件中就仅仅是原始图片的内容了，如下，将文件另存为test.jpg。



```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
006C92B0   1F F0 C9 DF 0A FF 00 E8  99 FC 3F FF 00 C2 76 D3   ðÉß ÿ è™ü?ÿ Âvó
006C92C0   FF 00 8D D1 45 00 1F F0  C9 DF 0A FF 00 E8 99 FC  ÿ  ÑE  ðÉß ÿ è™ü
006C92D0   3F FF 00 C2 76 D3 FF 00  8D D1 FF 00 0C 9D F0 AF  ?ÿ ÂvÓÿ  Ñÿ   ð¯
006C92E0   FE 89 9F C3 FF 00 FC 27  6D 3F F8 DD 14 50 01 FF  þ‰ŸÃÿ ü'm?øÝ P ÿ
006C92F0   00 0C 9D F0 AF FE 89 9F  C3 FF 00 FC 27 6D 3F F8     ð¯þ‰ŸÃÿ ü'm?ø
006C9300   DD 1F F0 C9 DF 0A FF 00  E8 99 FC 3F FF 00 C2 76  Ý ðÉß ÿ è™ü?ÿ Âv
006C9310   D3 FF 00 8D D1 45 00 1F  F0 C9 DF 0A FF 00 E8 99  Óÿ  ÑE  ðÉß ÿ è™
006C9320   FC 3F FF 00 C2 76 D3 FF  00 8D D1 FF 00 0C 9D F0  ü?ÿ ÂvÓÿ  Ñÿ   ð
006C9330   AF FE 89 9F C3 FF 00 FC  27 6D 3F F8 DD 14 50 01  ¯þ‰ŸÃÿ ü'm?øÝ P
006C9340   FF 00 0C 9D F0 AF FE 89  9F C3 FF 00 FC 27 6D 3F  ÿ   ð¯þ‰ŸÃÿ ü'm?
006C9350   F8 DD 1F F0 C9 DF 0A FF  00 E8 99 FC 3F FF 00 C2  øÝ ðÉß ÿ è™ü?ÿ Â
006C9360   76 D3 FF 00 8D D1 45 00  1F F0 C9 DF 0A FF 00 E8  vÓÿ  ÑE  ðÉß ÿ è
006C9370   99 FC 3F FF 00 C2 76 D3  FF 00 8D D1 FF 00 0C 9D  ™ü?ÿ ÂvÓÿ  Ñÿ
006C9380   F0 AF FE 89 9F C3 FF 00  FC 27 6D 3F F8 DD 14 50  ð¯þ‰ŸÃÿ ü'm?øÝ P
006C9390   01 FF 00 0C 9D F0 AF FE  89 9F C3 FF 00 FC 27 6D   ÿ   ð¯þ‰ŸÃÿ ü'm
006C93A0   3F F8 DD 1F F0 C9 DF 0A  FF 00 E8 99 FC 3F FF 00  ?øÝ ðÉß ÿ è™ü?ÿ
006C93B0   C2 76 D3 FF 00 8D D1 45  00 1F F0 C9 DF 0A FF 00  ÂvÓÿ  ÑE  ðÉß ÿ
006C93C0   E8 99 FC 3F FF 00 C2 76  D3 FF 00 8D D1 FF 00 0C  è™ü?ÿ ÂvÓÿ  Ñÿ
006C93D0   9D F0 AF FE 89 9F C3 FF  00 FC 27 6D 3F F8 DD 14   ð¯þ‰ŸÃÿ ü'm?øÝ
006C93E0   50 01 FF 00 0C 9D F0 AF  FE 89 9F C3 FF 00 FC 27  P ÿ   ð¯þ‰ŸÃÿ ü'
006C93F0   6D 3F F8 DD 33 FE 19 43  E1 6F FD 13 5F 00 7F E1  m?øÝ3þ Cáoý _  á
006C9400   3D 69 FF 00 C6 E8 A2 80  25 7F D9 43 E1 6F 95 FF  =iÿ Æè¢€% ÙCáo•ÿ
006C9410   00 24 D7 C0 1F F8 4F 5A  7F F1 BA FB CB FE 09 B9   $×À øOZ ñºûËþ ¹
006C9420   E0 ED 23 E1 6F EC E0 34  FF 00 0C E9 5A 6F 87 74  àí#áoìà4ÿ  éZo‡t
006C9430   F9 75 4B 89 DE DB 4B B6  4B 38 5E 42 11 4B 94 8C  ùuK‰ÞÛK¶K8^B K”Œ
006C9440   00 58 AA A8 CE 33 85 03  B0 A2 8A 00 FF D9         Xª¨Î3… °¢Š ÿÙ
```



打开jpg图片，是一份中国地图。

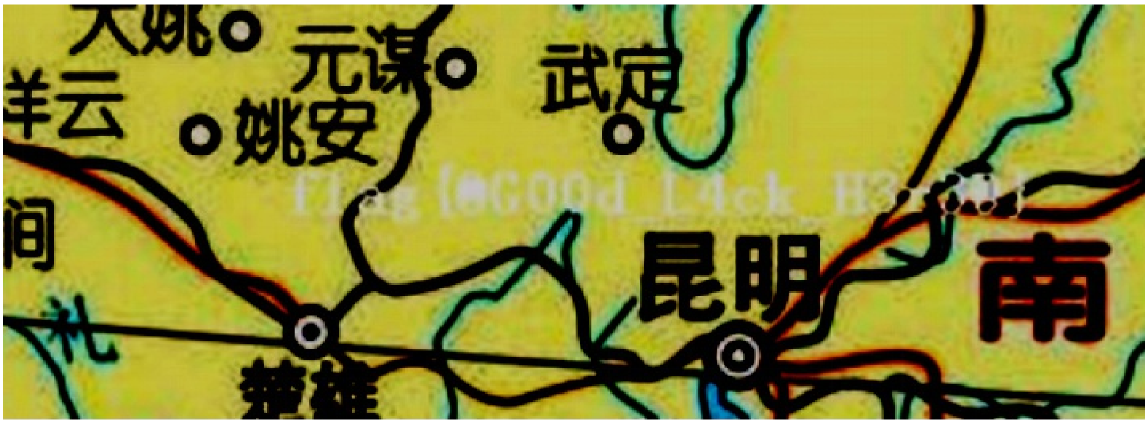
5、**开脑洞：**利用搜索工具

根据对话内容中的

王思聪100以及his family has alot of building —>搜索 万达 100

搜到 万达100店——昆明西山的达广场盛大开业

地点昆明 结合地图 调整对比度和亮度得出 flag



【参考】

1、 [Wireshark系列之7 利用WinHex还原文件 - 一壶浊酒 - 51CTO技术博客]

2、 [WireShark黑客发现之旅–开篇 | WooYun知识库]

3、 [广东省第一届“强网杯” writeup - 程序园]
