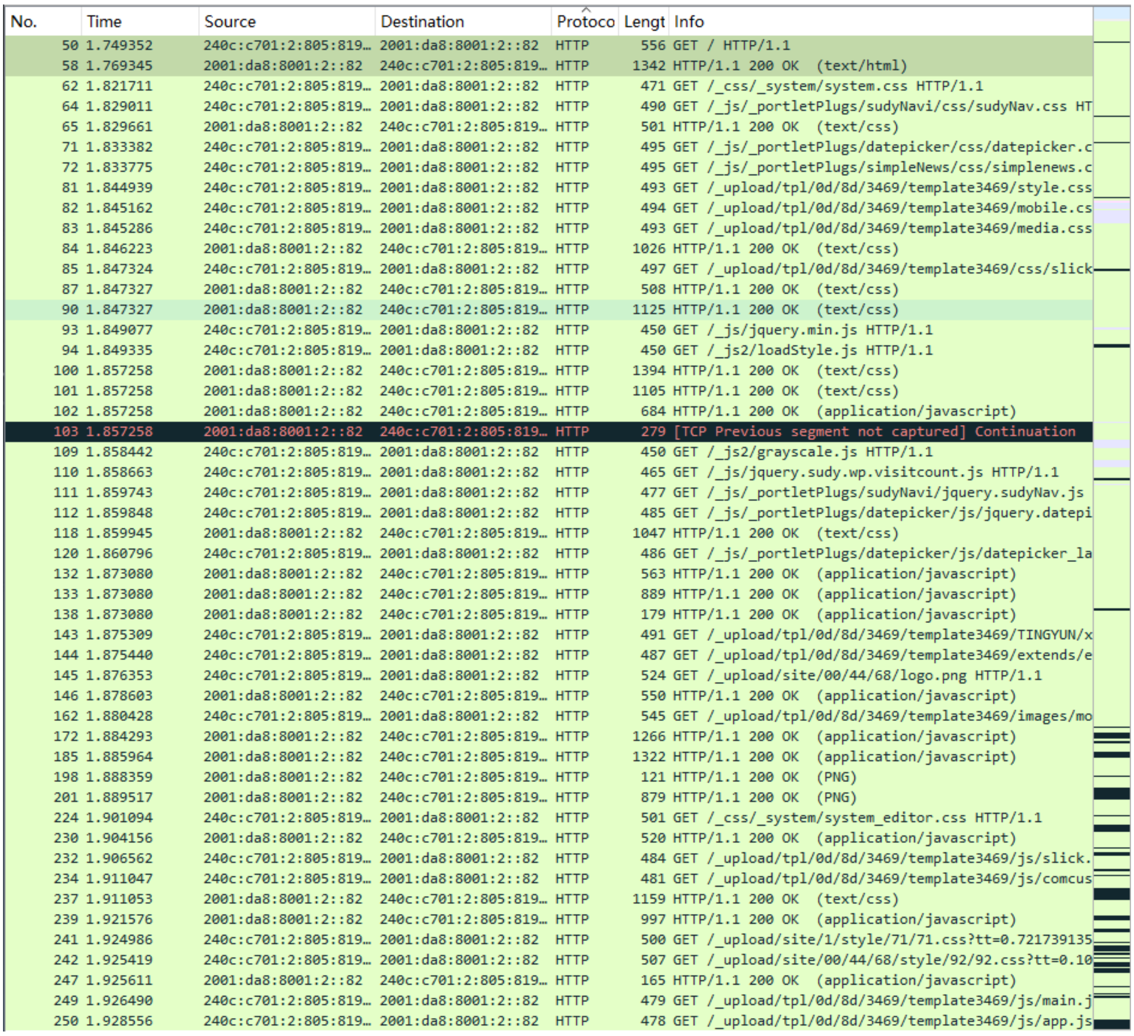
1. ## 请列出捕获到的5种不同类型的协议。

DNS, TLSv1.2, TCP, HTTP, UDP

2. ## 用显示过滤器过滤出所有http消息，从发送第一条 HTTP GET 请求到收到对应的 HTTP OK 回复用了多长时间?

1.769345-1.749352 = 0.019993（秒）



No.	Time	Source	Destination	Protoco	Lengt	Info
50	1.749352	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	556	GET / HTTP/1.1
58	1.769345	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1342	HTTP/1.1 200 OK (text/html)
62	1.821711	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	471	GET /_css/_system/system.css HTTP/1.1
64	1.829011	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	490	GET /_js/_portletPlugs/sudyNavi/css/sudyNav.css HT
65	1.829661	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	501	HTTP/1.1 200 OK (text/css)
71	1.833382	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	495	GET /_js/_portletPlugs/datepicker/css/datepicker.c
72	1.833775	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	495	GET /_js/_portletPlugs/simpleNews/css/simplenews.c
81	1.844939	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	493	GET /_upload/tpl/0d/8d/3469/template3469/style.css
82	1.845162	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	494	GET /_upload/tpl/0d/8d/3469/template3469/mobile.cs
83	1.845286	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	493	GET /_upload/tpl/0d/8d/3469/template3469/media.css
84	1.846223	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1026	HTTP/1.1 200 OK (text/css)
85	1.847324	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	497	GET /_upload/tpl/0d/8d/3469/template3469/css/slick
87	1.847327	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	508	HTTP/1.1 200 OK (text/css)
90	1.847327	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1125	HTTP/1.1 200 OK (text/css)
93	1.849077	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	450	GET /_js/jquery.min.js HTTP/1.1
94	1.849335	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	450	GET /_js2/loadStyle.js HTTP/1.1
100	1.857258	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1394	HTTP/1.1 200 OK (text/css)
101	1.857258	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1105	HTTP/1.1 200 OK (text/css)
102	1.857258	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	684	HTTP/1.1 200 OK (application/javascript)
103	1.857258	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	279	[TCP Previous segment not captured] Continuation
109	1.858442	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	450	GET /_js2/grayscale.js HTTP/1.1
110	1.858663	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	465	GET /_js/jquery.sudy.wp.visitcount.js HTTP/1.1
111	1.859743	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	477	GET /_js/_portletPlugs/sudyNavi/jquery.sudyNav.js
112	1.859848	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	485	GET /_js/_portletPlugs/datepicker/js/jquery.datepi
118	1.859945	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1047	HTTP/1.1 200 OK (text/css)
120	1.860796	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	486	GET /_js/_portletPlugs/datepicker/js/datepicker_la
132	1.873080	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	563	HTTP/1.1 200 OK (application/javascript)
133	1.873080	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	889	HTTP/1.1 200 OK (application/javascript)
138	1.873080	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	179	HTTP/1.1 200 OK (application/javascript)
143	1.875309	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	491	GET /_upload/tpl/0d/8d/3469/template3469/TINGYUN/x
144	1.875440	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	487	GET /_upload/tpl/0d/8d/3469/template3469/extends/e
145	1.876353	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	524	GET /_upload/site/00/44/68/logo.png HTTP/1.1
146	1.878603	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	550	HTTP/1.1 200 OK (application/javascript)
162	1.880428	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	545	GET /_upload/tpl/0d/8d/3469/template3469/images/mo
172	1.884293	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1266	HTTP/1.1 200 OK (application/javascript)
185	1.885964	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1322	HTTP/1.1 200 OK (application/javascript)
198	1.888359	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	121	HTTP/1.1 200 OK (PNG)
201	1.889517	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	879	HTTP/1.1 200 OK (PNG)
224	1.901094	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	501	GET /_css/_system/system_editor.css HTTP/1.1
230	1.904156	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	520	HTTP/1.1 200 OK (application/javascript)
232	1.906562	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	484	GET /_upload/tpl/0d/8d/3469/template3469/js/slick.
234	1.911047	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	481	GET /_upload/tpl/0d/8d/3469/template3469/js/comcus
237	1.911053	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	1159	HTTP/1.1 200 OK (text/css)
239	1.921576	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	997	HTTP/1.1 200 OK (application/javascript)
241	1.924986	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	500	GET /_upload/site/1/style/71/71.css?tt=0.721739135
242	1.925419	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	507	GET /_upload/site/00/44/68/style/92/92.css?tt=0.10
247	1.925611	2001:da8:8001:2::82	240c:c701:2:805:819…	HTTP	165	HTTP/1.1 200 OK (application/javascript)
249	1.926490	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	479	GET /_upload/tpl/0d/8d/3469/template3469/js/main.j
250	1.928556	240c:c701:2:805:819…	2001:da8:8001:2::82	HTTP	478	GET /_upload/tpl/0d/8d/3469/template3469/js/app.js

3. ## 复旦信息办的 IP 地址是什么？你的计算机发送 HTTP GET 请求时的 IP 地址是什么?

复旦信息办是2001:da8:8001:2::82，也可以通过`ping ping ecampus.fudan.edu.cn`得到。本机是240c:c701:2:805:819d:feb1:9031:97c6。

4. ## 找到任意一个 HTTP 包，发出 HTTP 请求的网络浏览器是什么?

找到这一段：
`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36 Edg/128.0.0.0\r\n`
解释：

Mozilla/5.0： 网景公司浏览器的标识，由于互联网初期浏览器市场主要被网景公司占领，很多服务器被设置成仅响应含有标志为Mozilla的浏览器的请求，因此，新款的浏览器为了打入市场，不得不加上这个字段。

Windows NT 10.0 : Windows 10的标识符

Win64; x64： 64位的Windows系统运行在64位的处理器上

AppleWebKit/537.36：苹果公司开发的呈现引擎

KHTML：是Linux平台中Konqueror浏览器的呈现引擎KHTML

Geckeo：呈现引擎

like Gecko：表示其行为与Gecko浏览器引擎类似

Microsoft Edge 浏览器基于Chrome开发，因而也会带上Chrome。

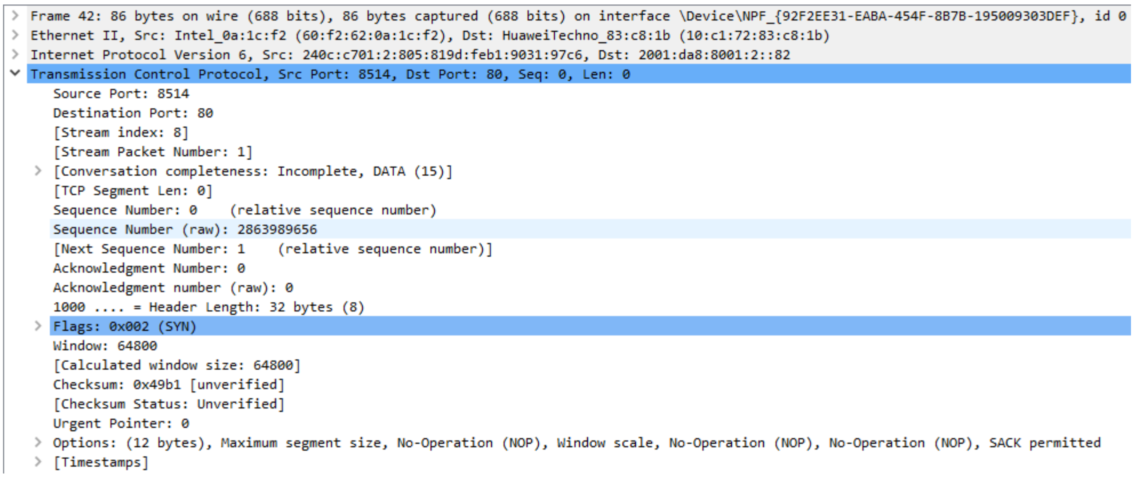
最后一串是Edg，说明使用的是 Microsoft Edge 浏览器。

5. 找到任意一个 TCP 包，源端口号和目的端口号各自是什么？

Transmission Control Protocol, Src Port: 8514, Dst Port: 80, Seq: 0, Len: 0

Source Port: 8514

Destination Port: 80

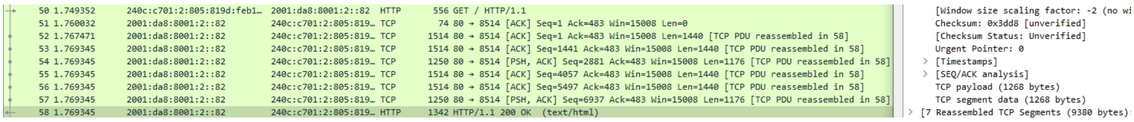


```
> Frame 42: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{92F2EE31-EABA-454F-8B7B-195009303DEF}, id 0
> Ethernet II, Src: Intel_0a:1c:f2 (60:f2:62:0a:1c:f2), Dst: HuaweiTechno_83:c8:1b (10:c1:72:83:c8:1b)
> Internet Protocol Version 6, Src: 240c:c701:2:805:819d:feb1:9031:97c6, Dst: 2001:da8:8001:2::82
v Transmission Control Protocol, Src Port: 8514, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 8514
     Destination Port: 80
     [Stream index: 8]
     [Stream Packet Number: 1]
   > [Conversation completeness: Incomplete, DATA (15)]
     [TCP Segment Len: 0]
     Sequence Number: 0    (relative sequence number)
     Sequence Number (raw): 2863989656
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 0
     Acknowledgment number (raw): 0
     1000 .... = Header Length: 32 bytes (8)
   > Flags: 0x002 (SYN)
     Window: 64800
     [Calculated window size: 64800]
     Checksum: 0x49b1 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
   > [Timestamps]
```

6. 找到一个由多个 TCP 报文段组合而成的 HTTP 响应分组，这个分组是由多少个 TCP 报文段组成的？

7个。

[7 Reassembled TCP Segments (9380 bytes): #52(1440), #53(1440), #54(1176), #55(1440), #56(1440), #57(1176), #58(1268)]

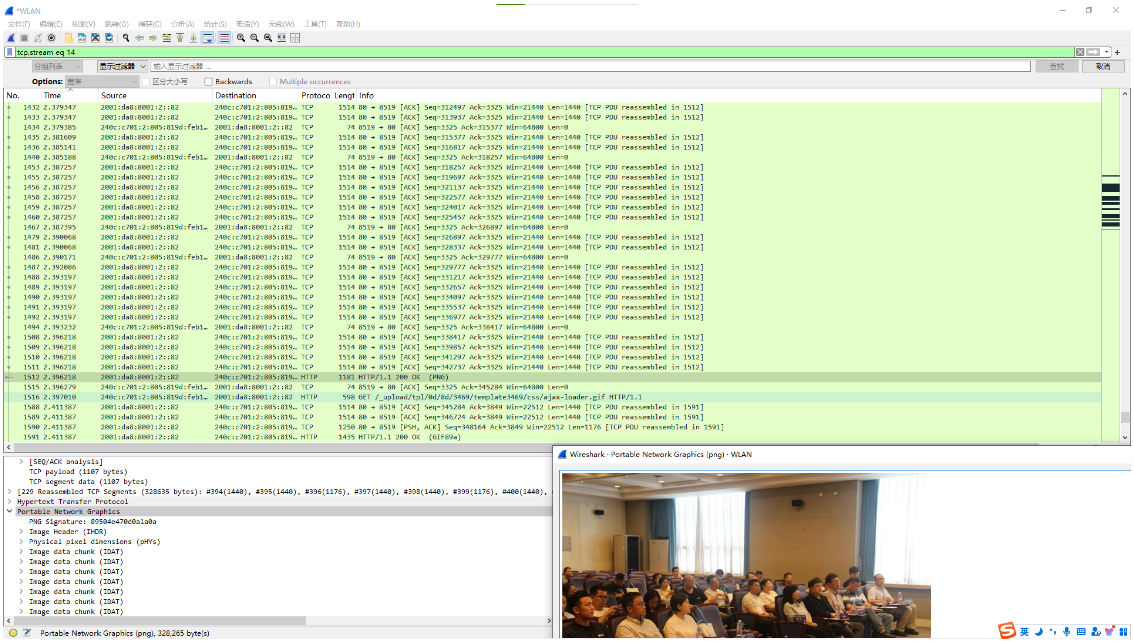


```
50 1.749352   240c:c701:2:805:819d:feb1…  2001:da8:8001:2::82   HTTP    556 GET / HTTP/1.1
51 1.760032   2001:da8:8001:2::82         240c:c701:2:805:819…  TCP      74 80 → 8514 [ACK] Seq=1 Ack=483 Win=15008 Len=0
52 1.767471   2001:da8:8001:2::82         240c:c701:2:805:819…  TCP    1514 80 → 8514 [ACK] Seq=1 Ack=483 Win=15008 Len=1440 [TCP PDU reassembled in 58]
53 1.769345   2001:da8:8001:2::82         240c:c701:2:805:819…  TCP    1514 80 → 8514 [ACK] Seq=1441 Ack=483 Win=15008 Len=1440 [TCP PDU reassembled in 58]
54 1.769345   2001:da8:8001:2::82         240c:c701:2:805:819…  TCP    1250 80 → 8514 [PSH, ACK] Seq=2881 Ack=483 Win=15008 Len=1176 [TCP PDU reassembled in 58]
55 1.769345   2001:da8:8001:2::82         240c:c701:2:805:819…  TCP    1514 80 → 8514 [ACK] Seq=4057 Ack=483 Win=15008 Len=1440 [TCP PDU reassembled in 58]
56 1.769345   2001:da8:8001:2::82         240c:c701:2:805:819…  TCP    1514 80 → 8514 [ACK] Seq=5497 Ack=483 Win=15008 Len=1440 [TCP PDU reassembled in 58]
57 1.769345   2001:da8:8001:2::82         240c:c701:2:805:819…  TCP    1250 80 → 8514 [PSH, ACK] Seq=6937 Ack=483 Win=15008 Len=1176 [TCP PDU reassembled in 58]
58 1.769345   2001:da8:8001:2::82         240c:c701:2:805:819…  HTTP   1342 HTTP/1.1 200 OK  (text/html)
```

```
     [Window size scaling factor: -2 (no wi
     Checksum: 0x3dd8 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > [Timestamps]
   > [SEQ/ACK analysis]
     TCP payload (1268 bytes)
     TCP segment data (1268 bytes)
> [7 Reassembled TCP Segments (9380 bytes):
```

7. 找到一个带有明文图片的分组，通过“显示分组字节”在wireshark中显示图片，并在浏览器中找到对应图片。

图片分组如图：


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
分组列表
显示过滤器
输入显示过滤器 …
查找
取消
Options: 宽窄
区分大小写
Backwards
Multiple occurrences
Wireshark · Portable Network Graphics (png) · WLAN

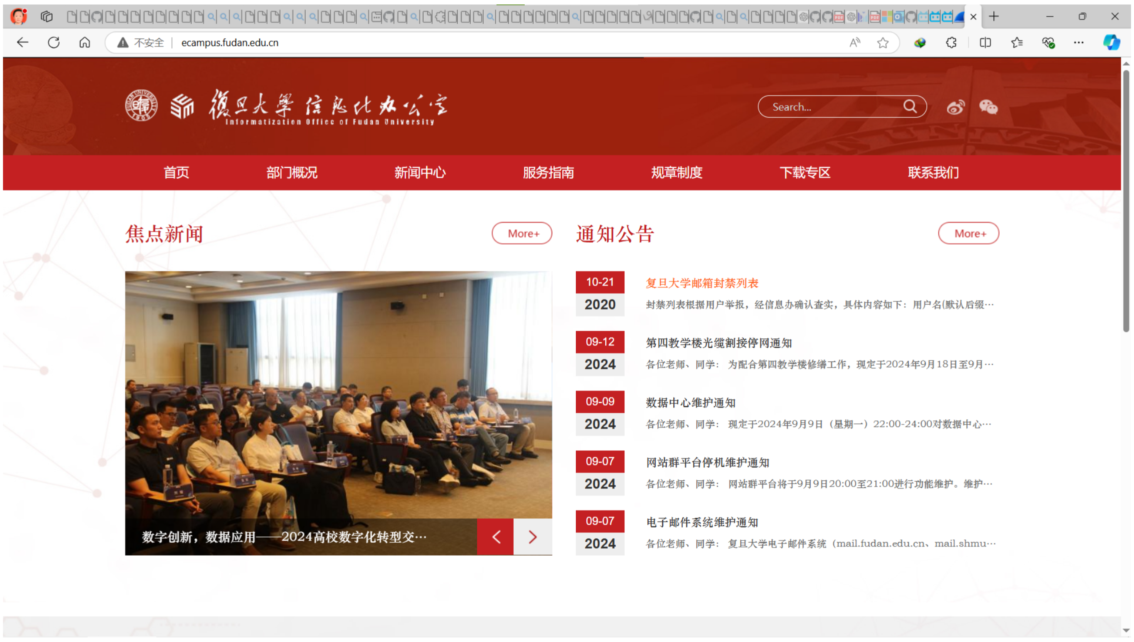
tcp.stream eq 14

```
No.  Time     Source                    Destination              Protoco Lengt Info
1432 2.379347 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=312497 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1433 2.379347 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=313937 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1434 2.379385 240c:c701:2:805:819d:feb1… 2001:da8:8001:2::82  TCP      74 8519 → 80 [ACK] Seq=3325 Ack=315377 Win=64800 Len=0
1435 2.381609 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=315377 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1436 2.385141 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=316817 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1440 2.385188 240c:c701:2:805:819d:feb1… 2001:da8:8001:2::82  TCP      74 8519 → 80 [ACK] Seq=3325 Ack=318257 Win=64800 Len=0
1453 2.387257 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=318257 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1455 2.387257 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=319697 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1456 2.387257 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=321137 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1458 2.387257 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=322577 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1459 2.387257 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=324017 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1460 2.387257 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=325457 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1467 2.387395 240c:c701:2:805:819d:feb1… 2001:da8:8001:2::82  TCP      74 8519 → 80 [ACK] Seq=3325 Ack=326897 Win=64800 Len=0
1479 2.390068 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=326897 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1481 2.390068 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=328337 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1486 2.390171 240c:c701:2:805:819d:feb1… 2001:da8:8001:2::82  TCP      74 8519 → 80 [ACK] Seq=3325 Ack=329777 Win=64800 Len=0
1487 2.392086 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=329777 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1488 2.393197 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=331217 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1489 2.393197 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=332657 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1490 2.393197 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=334097 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1491 2.393197 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=335537 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1492 2.393197 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=336977 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1494 2.393232 240c:c701:2:805:819d:feb1… 2001:da8:8001:2::82  TCP      74 8519 → 80 [ACK] Seq=3325 Ack=338417 Win=64800 Len=0
1508 2.396218 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=338417 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1509 2.396218 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=339857 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1510 2.396218 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=341297 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1511 2.396218 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=342737 Ack=3325 Win=21440 Len=1440 [TCP PDU reassembled in 1512]
1512 2.396218 2001:da8:8001:2::82        240c:c701:2:805:819… HTTP   1181 HTTP/1.1 200 OK  (PNG)
1515 2.396279 240c:c701:2:805:819d:feb1… 2001:da8:8001:2::82  TCP      74 8519 → 80 [ACK] Seq=3325 Ack=345284 Win=64800 Len=0
1516 2.397010 240c:c701:2:805:819d:feb1… 2001:da8:8001:2::82  HTTP    598 GET /_upload/tpl/0d/8d/3469/template3469/css/ajax-loader.gif HTTP/1.1
1588 2.411387 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=345284 Ack=3849 Win=22512 Len=1440 [TCP PDU reassembled in 1591]
1589 2.411387 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1514 80 → 8519 [ACK] Seq=346724 Ack=3849 Win=22512 Len=1440 [TCP PDU reassembled in 1591]
1590 2.411387 2001:da8:8001:2::82        240c:c701:2:805:819… TCP    1250 80 → 8519 [PSH, ACK] Seq=348164 Ack=3849 Win=22512 Len=1176 [TCP PDU reassembled in 1591]
1591 2.411387 2001:da8:8001:2::82        240c:c701:2:805:819… HTTP   1435 HTTP/1.1 200 OK  (GIF89a)
```

```
  > [SEQ/ACK analysis]
    TCP payload (1107 bytes)
    TCP segment data (1107 bytes)
> [229 Reassembled TCP Segments (328635 bytes): #394(1440), #395(1440), #396(1176), #397(1440), #398(1440), #399(1176), #400(1440),
> Hypertext Transfer Protocol
v Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
  > Image Header (IHDR)
  > Physical pixel dimensions (pHYs)
  > Image data chunk (IDAT)
  > Image data chunk (IDAT)
  > Image data chunk (IDAT)
  > Image data chunk (IDAT)
  > Image data chunk (IDAT)
  > Image data chunk (IDAT)
  > Image data chunk (IDAT)
```

Portable Network Graphics (png), 328,265 byte(s)

就是网页左侧的图片。



数字创新，数据应用——2024高校数字化转型交…

10-21 2020 复旦大学邮箱封禁列表
封禁列表根据用户举报，经信息办确认查实，具体内容如下：用户名(默认后缀…

09-12 2024 第四教学楼光缆割接停网通知
各位老师、同学： 为配合第四教学楼修缮工作，现定于2024年9月18日至9月…

09-09 2024 数据中心维护通知
各位老师、同学： 现定于2024年9月9日（星期一）22:00-24:00对数据中心…

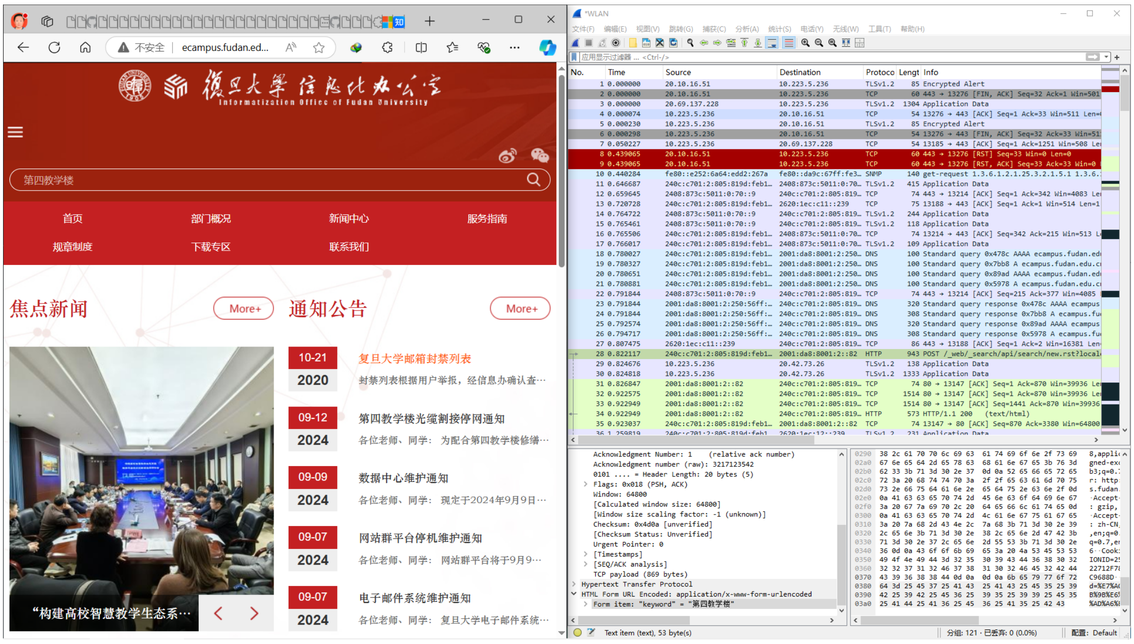
09-07 2024 网站群平台停机维护通知
各位老师、同学： 网站群平台将于9月9日20:00至21:00进行功能维护。维护…

09-07 2024 电子邮件系统维护通知
各位老师、同学： 复旦大学电子邮件系统（mail.fudan.edu.cn、mail.shmu…

8. **重新开启分组捕获，在复旦信息办网站右上角的导航栏搜索任意内容，在捕获到的分组里寻找你输入的内容，观察 HTTP 如何通过 POST 方法发送数据。**

HTTP通过POST方法发送以下包
HTML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "keyword" = "第四教学楼"

在图片右下角。



10-21 2020 复旦大学邮箱封禁列表
封禁列表根据用户举报，经信息办确认查…

09-12 2024 第四教学楼光缆割接停网通知
各位老师、同学： 为配合第四教学楼修缮…

09-09 2024 数据中心维护通知
各位老师、同学： 现定于2024年9月9日…

09-07 2024 网站群平台停机维护通知
各位老师、同学： 网站群平台将于9月9…

09-07 2024 电子邮件系统维护通知
各位老师、同学： 复旦大学电子邮件系统…

```
No.  Time      Source                      Destination                Protoco Lengt Info
   1 0.000000  20.10.16.51                 10.223.5.236               TLSv1.2    85 Encrypted Alert
   2 0.000000  20.10.16.51                 10.223.5.236               TCP        60 443 → 13276 [FIN, ACK] Seq=32 Ack=1 Win=501
   3 0.000000  20.69.137.228               10.223.5.236               TLSv1.2  1304 Application Data
   4 0.000074  10.223.5.236                20.10.16.51                TCP        54 13276 → 443 [ACK] Seq=1 Ack=33 Win=511 Len=
   5 0.000230  10.223.5.236                20.10.16.51                TLSv1.2    85 Encrypted Alert
   6 0.000298  10.223.5.236                20.10.16.51                TCP        54 13276 → 443 [FIN, ACK] Seq=32 Ack=33 Win=51
   7 0.050227  10.223.5.236                20.69.137.228              TCP        54 13185 → 443 [ACK] Seq=1 Ack=1251 Win=508 Le
   8 0.439065  20.10.16.51                 10.223.5.236               TCP        60 443 → 13276 [RST] Seq=33 Win=0 Len=0
   9 0.439065  20.10.16.51                 10.223.5.236               TCP        60 443 → 13276 [RST, ACK] Seq=33 Ack=33 Win=0
  10 0.440284  fe80::e252:6a64:edd2:267a   fe80::da9c:67ff:fe3…       SNMP      140 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.
  11 0.646687  240c:c701:2:805:819d:feb1…  2408:873c:5011:0:70…       TLSv1.2   415 Application Data
  12 0.659645  2408:873c:5011:0:70::9      240c:c701:2:805:819…       TCP        74 443 → 13214 [ACK] Seq=1 Ack=342 Win=4083 Le
  13 0.720728  240c:c701:2:805:819d:feb1…  2620:1ec:c11::239          TCP        75 13188 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1
  14 0.764722  2408:873c:5011:0:70::9      240c:c701:2:805:819…       TLSv1.2   244 Application Data
  15 0.765461  2408:873c:5011:0:70::9      240c:c701:2:805:819…       TLSv1.2   118 Application Data
  16 0.765506  240c:c701:2:805:819d:feb1…  2408:873c:5011:0:70…       TCP        74 13214 → 443 [ACK] Seq=342 Ack=215 Win=513 L
  17 0.766017  240c:c701:2:805:819d:feb1…  2408:873c:5011:0:70…       TLSv1.2   109 Application Data
  18 0.780027  240c:c701:2:805:819d:feb1…  2001:da8:8001:2:250…       DNS       100 Standard query 0x478c AAAA ecampus.fudan.ed
  19 0.780327  240c:c701:2:805:819d:feb1…  2001:da8:8001:2:250…       DNS       100 Standard query 0x7bb8 A ecampus.fudan.edu.c
  20 0.780651  240c:c701:2:805:819d:feb1…  2001:da8:8001:2:250…       DNS       100 Standard query 0x89ad AAAA ecampus.fudan.ed
  21 0.780881  240c:c701:2:805:819d:feb1…  2001:da8:8001:2:250…       DNS       100 Standard query 0x5978 A ecampus.fudan.edu.c
  22 0.791844  2408:873c:5011:0:70::9      240c:c701:2:805:819…       TCP        74 443 → 13214 [ACK] Seq=215 Ack=377 Win=4085
  23 0.791844  2001:da8:8001:2:250:56ff:…  240c:c701:2:805:819…       DNS       320 Standard query response 0x478c AAAA ecampus
  24 0.791844  2001:da8:8001:2:250:56ff:…  240c:c701:2:805:819…       DNS       308 Standard query response 0x7bb8 A ecampus.fu
  25 0.792574  2001:da8:8001:2:250:56ff:…  240c:c701:2:805:819…       DNS       320 Standard query response 0x89ad AAAA ecampus
  26 0.794717  2001:da8:8001:2:250:56ff:…  240c:c701:2:805:819…       DNS       308 Standard query response 0x5978 A ecampus.fu
  27 0.807475  2620:1ec:c11::239           240c:c701:2:805:819…       TCP        86 443 → 13188 [ACK] Seq=1 Ack=2 Win=16381 Len
  28 0.822117  240c:c701:2:805:819d:feb1…  2001:da8:8001:2::82        HTTP      943 POST /_web/_search/api/search/new.rst?local
  29 0.824676  10.223.5.236                20.42.73.26                TLSv1.2   138 Application Data
  30 0.824818  10.223.5.236                20.42.73.26                TLSv1.2  1333 Application Data
  31 0.826847  2001:da8:8001:2::82         240c:c701:2:805:819…       TCP        74 80 → 13147 [ACK] Seq=1 Ack=870 Win=39936 Le
  32 0.922575  2001:da8:8001:2::82         240c:c701:2:805:819…       TCP      1514 80 → 13147 [ACK] Seq=1 Ack=870 Win=39936 Le
  33 0.922949  2001:da8:8001:2::82         240c:c701:2:805:819…       TCP      1514 80 → 13147 [ACK] Seq=1441 Ack=870 Win=39936
  34 0.922949  2001:da8:8001:2::82         240c:c701:2:805:819…       HTTP      573 HTTP/1.1 200   (text/html)
  35 0.923037  240c:c701:2:805:819d:feb1…  2001:da8:8001:2::82        TCP        74 13147 → 80 [ACK] Seq=870 Ack=3380 Win=64800
  36 1.259819  240c:c701:2:805:819d:feb1   2620:1ec:12::239           TLSv1.2   231 Application Data
```

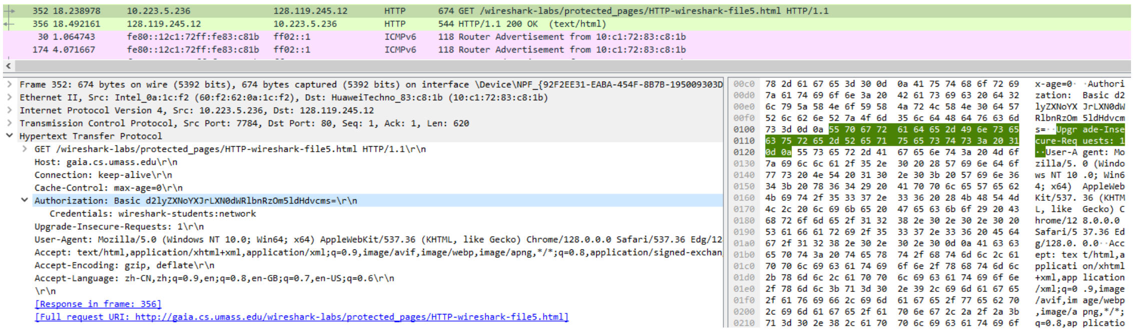
```
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3217123542
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 64800
    [Calculated window size: 64800]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x4d0a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (869 bytes)
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "keyword" = "第四教学楼"
```

```
0290  38 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 73 69   8,applic
02a0  67 6e 65 64 2d 65 78 63  68 61 6e 67 65 3b 76 3d   gned-exc
02b0  62 33 3b 71 3d 30 2e 37  0d 0a 52 65 66 65 72 65   b3;q=0.7
02c0  72 3a 20 68 74 74 70 3a  2f 2f 65 63 61 6d 70 75   r: http:
02d0  73 2e 66 75 64 61 6e 2e  65 64 75 2e 63 6e 2f 0d   s.fudan.
02e0  0a 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67   ·Accept-
02f0  3a 20 67 7a 69 70 2c 20  64 65 66 6c 61 74 65 0d   : gzip,
0300  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept-
0310  3a 20 7a 68 2d 43 4e 2c  7a 68 3b 71 3d 30 2e 39   : zh-CN,
0320  2c 65 6e 3b 71 3d 30 2e  38 2c 65 6e 2d 47 42 3b   ,en;q=0.
0330  71 3d 30 2e 37 2c 65 6e  2d 55 53 3b 71 3d 30 2e   q=0.7,en
0340  36 0d 0a 43 6f 6f 6b 69  65 3a 20 4a 53 45 53 53   6··Cooki
0350  49 4f 4e 49 44 3d 32 35  30 39 43 44 36 38 30 32   IONID=25
0360  32 32 37 31 32 46 37 38  31 30 32 46 45 32 42 44   22712F78
0370  43 39 36 38 38 44 0d 0a  0d 0a 6b 65 79 77 6f 72   C9688D··
0380  64 3d 25 45 37 25 41 43  25 41 43 25 45 35 25 39   d=%E7%AC
0390  42 25 39 42 25 45 36 25  39 35 25 39 39 25 45 35   B%9B%E6%
03a0  25 41 44 25 41 36 25 45  36 25 41 35 25 42 43      %AD%A6%E
```

Text item (text), 53 byte(s)   分组: 121 · 已丢弃: 0 (0.0%)   配置: Default

9. 在抓取的分组中找到输入的用户名和密码（传输使用了base64编码）。将地址中的http改为https，还能否通过捕获分组获得密码?

可以看到密码明文，就在Authorization.Credentials里面。



```
 352 18.238978   10.223.5.236              128.119.245.12   HTTP     674 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 356 18.492161   128.119.245.12            10.223.5.236     HTTP     544 HTTP/1.1 200 OK  (text/html)
  30 1.064743    fe80::12c1:72ff:fe83:c81b ff02::1          ICMPv6   118 Router Advertisement from 10:c1:72:83:c8:1b
 174 4.071667    fe80::12c1:72ff:fe83:c81b ff02::1          ICMPv6   118 Router Advertisement from 10:c1:72:83:c8:1b
```

```
> Frame 352: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on interface \Device\NPF_{92F2EE31-EABA-454F-8B7B-195009303D
> Ethernet II, Src: Intel_0a:1c:f2 (60:f2:62:0a:1c:f2), Dst: HuaweiTechno_83:c8:1b (10:c1:72:83:c8:1b)
> Internet Protocol Version 4, Src: 10.223.5.236, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 7784, Dst Port: 80, Seq: 1, Ack: 1, Len: 620
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36 Edg/12
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
    \r\n
    [Response in frame: 356]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```

```
00c0  78 2d 61 67 65 3d 30 0d  0a 41 75 74 68 6f 72 69   x-age=0· ·Authori
00d0  7a 61 74 69 6f 6e 3a 20  42 61 73 69 63 20 64 32   zation:  Basic d2
00e0  6c 79 5a 58 4e 6f 59 58  4a 72 4c 58 4e 30 64 57   lyZXNoYX JrLXN0dW
00f0  52 6c 62 6e 52 7a 4f 6d  35 6c 64 48 64 76 63 6d   RlbnRzOm 5ldHdvcm
0100  73 3d 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   s=··Upgr ade-Inse
0110  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
0120  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0130  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Windo
0140  77 73 20 4e 54 20 31 30  2e 30 3b 20 57 69 6e 36   ws NT 10 .0; Win6
0150  34 3b 20 78 36 34 29 20  41 70 70 6c 65 57 65 62   4; x64)  AppleWeb
0160  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
0170  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
0180  68 72 6f 6d 65 2f 31 32  38 2e 30 2e 30 2e 30 20   hrome/12 8.0.0.0
0190  53 61 66 61 72 69 2f 35  33 37 2e 33 36 20 45 64   Safari/5 37.36 Ed
01a0  67 2f 31 32 38 2e 30 2e  30 2e 30 0d 0a 41 63 63   g/128.0. 0.0··Acc
01b0  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
01c0  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml
01d0  2b 78 6d 6c 2c 61 70 70  6c 69 63 61 74 69 6f 6e   +xml,app lication
01e0  2f 78 6d 6c 3b 71 3d 30  2e 39 2c 69 6d 61 67 65   /xml;q=0 .9,image
01f0  2f 61 76 69 66 2c 69 6d  61 67 65 2f 77 65 62 70   /avif,im age/webp
0200  2c 69 6d 61 67 65 2f 61  70 6e 67 2c 2a 2f 2a 3b   ,image/a png,*/*;
0210  71 3d 30 2e 38 2c 61 70  70 6c 69 63 61 74 69 6f   q=0.8,ap plicatio
```

改为HTTPS直接抓取不到分组。