Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 185.243.115.84 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	TCP, UDP,ARP	Three most common protocols on the network.
# of Unique IP Addresses	IPv4 808 ipv6 2	Count of observed IP addresses.
Subnets	172.16.4.0/24 185.243.115.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	2	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Watching Youtube
- Browsing medical information
- shopping for toys

Suspicious Activity

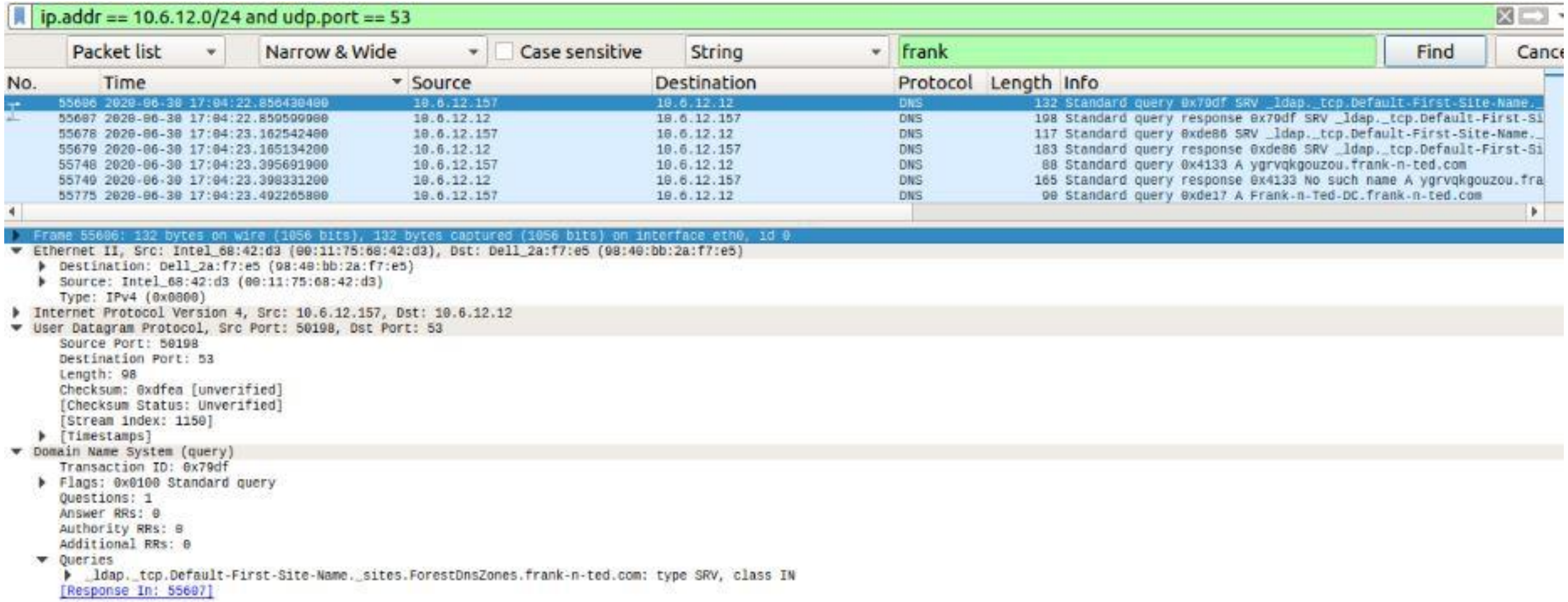
- Creating a server on corporate network
- torrenting
- Malware Transmission

Normal Activity

Streaming Video

Frank-n-ted.com:

- For the streaming I had followed UDP stream allowing me to see all the transactions that occurred.The thing i found odd about this is them accessing port 53.



```
ip.addr == 10.6.12.0/24 and udp.port == 53
```

Packet list | Narrow & Wide | □ Case sensitive | String | frank

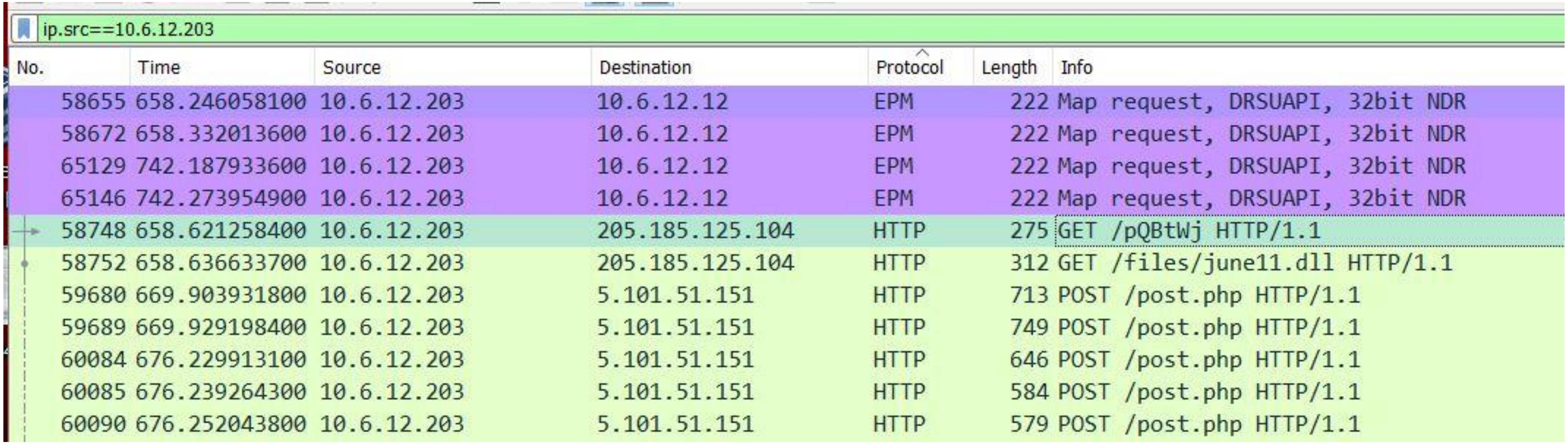
```
No.    Time                           Source         Destination    Protocol Length Info
55686 2020-06-30 17:04:22.856430400  10.6.12.157    10.6.12.12     DNS       132 Standard query 0x79df SRV _ldap._tcp.Default-First-Site-Name._
55687 2020-06-30 17:04:22.859599900  10.6.12.12     10.6.12.157    DNS       198 Standard query response 0x79df SRV _ldap._tcp.Default-First-Si
55678 2020-06-30 17:04:23.162542400  10.6.12.157    10.6.12.12     DNS       117 Standard query 0xde86 SRV _ldap._tcp.Default-First-Site-Name._
55679 2020-06-30 17:04:23.165134200  10.6.12.12     10.6.12.157    DNS       183 Standard query response 0xde86 SRV _ldap._tcp.Default-First-Si
55748 2020-06-30 17:04:23.395691900  10.6.12.157    10.6.12.12     DNS        88 Standard query 0x4133 A ygrvqkgouzou.frank-n-ted.com
55749 2020-06-30 17:04:23.398331200  10.6.12.12     10.6.12.157    DNS       165 Standard query response 0x4133 No such name A ygrvqkgouzou.fra
55775 2020-06-30 17:04:23.492265800  10.6.12.157    10.6.12.12     DNS        90 Standard query 0xde17 A Frank-n-Ted-DC.frank-n-ted.com
```

```
▸ Frame 55686: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface eth0, id 0
▾ Ethernet II, Src: Intel_68:42:d3 (00:11:75:68:42:d3), Dst: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
   ▸ Destination: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
   ▸ Source: Intel_68:42:d3 (00:11:75:68:42:d3)
     Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.6.12.157, Dst: 10.6.12.12
▾ User Datagram Protocol, Src Port: 50198, Dst Port: 53
     Source Port: 50198
     Destination Port: 53
     Length: 98
     Checksum: 0xdfea [unverified]
     [Checksum Status: Unverified]
     [Stream index: 1150]
   ▸ [Timestamps]
▾ Domain Name System (query)
     Transaction ID: 0x79df
   ▸ Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   ▾ Queries
      ▸ _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.frank-n-ted.com: type SRV, class IN
     [Response In: 55687]
```

Record information

What is the get request:

- After viewing the HTMl protocol you can see that there was a successful GET over port 80.



ip.src==10.6.12.203

No.	Time	Source	Destination	Protocol	Length	Info
58655	658.246058100	10.6.12.203	10.6.12.12	EPM	222	Map request, DRSUAPI, 32bit NDR
58672	658.332013600	10.6.12.203	10.6.12.12	EPM	222	Map request, DRSUAPI, 32bit NDR
65129	742.187933600	10.6.12.203	10.6.12.12	EPM	222	Map request, DRSUAPI, 32bit NDR
65146	742.273954900	10.6.12.203	10.6.12.12	EPM	222	Map request, DRSUAPI, 32bit NDR
58748	658.621258400	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
58752	658.636633700	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
59680	669.903931800	10.6.12.203	5.101.51.151	HTTP	713	POST /post.php HTTP/1.1
59689	669.929198400	10.6.12.203	5.101.51.151	HTTP	749	POST /post.php HTTP/1.1
60084	676.229913100	10.6.12.203	5.101.51.151	HTTP	646	POST /post.php HTTP/1.1
60085	676.239264300	10.6.12.203	5.101.51.151	HTTP	584	POST /post.php HTTP/1.1
60090	676.252043800	10.6.12.203	5.101.51.151	HTTP	579	POST /post.php HTTP/1.1

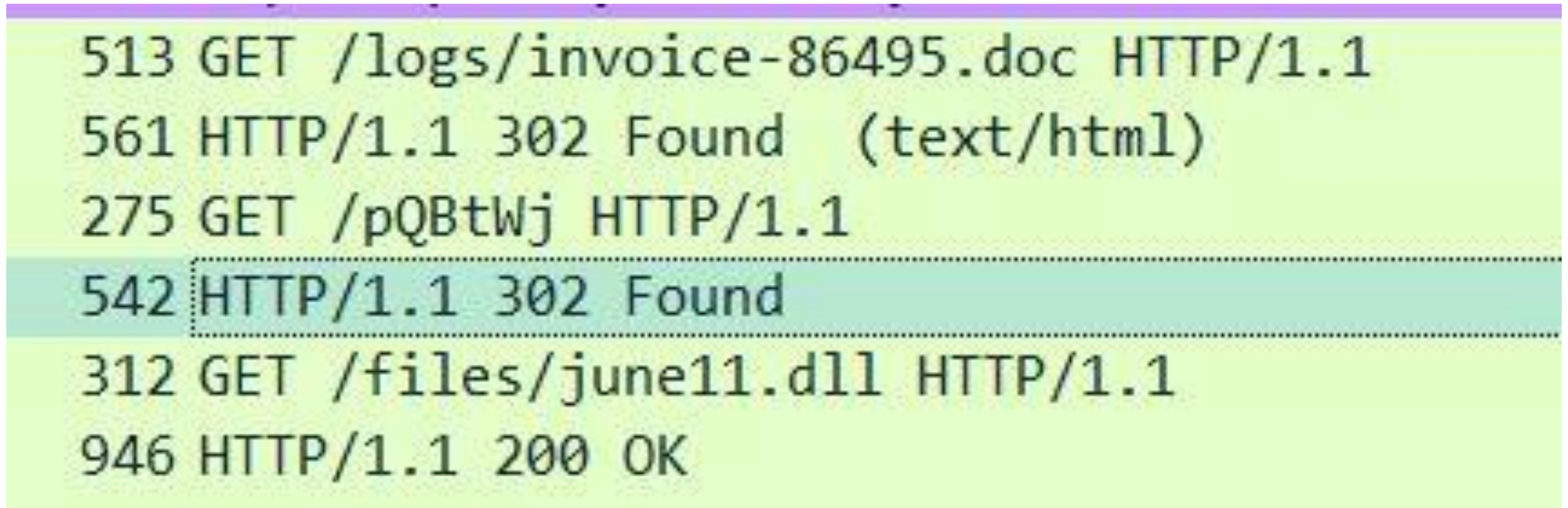
Malicious Activity

ZLoader Rat Download

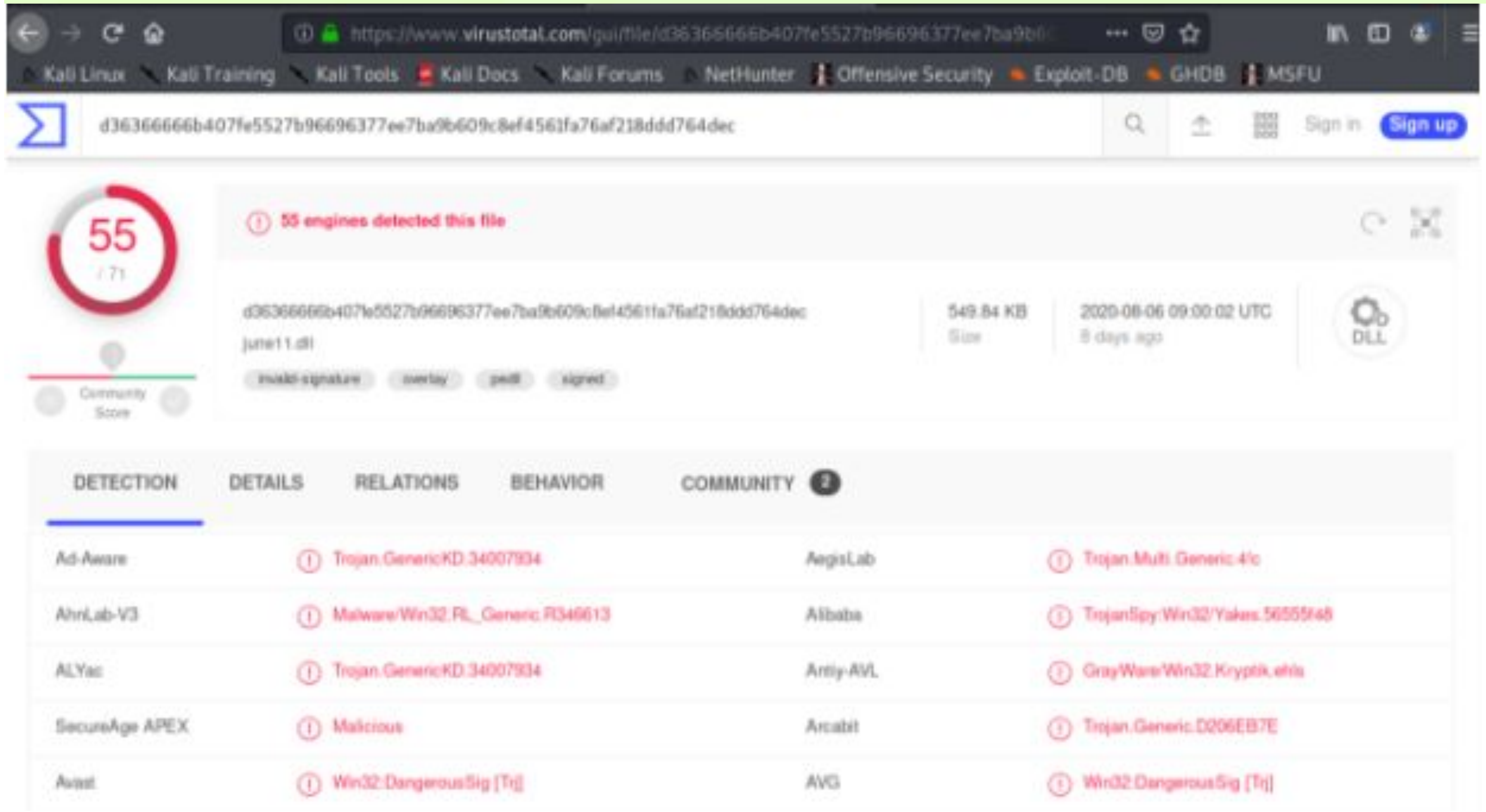
Frank-n-ted have been bad boys:

- frank-n-ted (10.6.12.203) downloaded a file from 205.185.125.104
  - This was the GET request made for : pQBtWj june11.dll

- this is associated with an excel macro
  - june11.dll is identified as a RAT and posted to the host snnmnkxdhflwqthqismb.com(5.101.51.151)
- snnmnkxdhflwqthqismb.com is a C2 site for the ZLoader RAT



```
513 GET /logs/invoice-86495.doc HTTP/1.1
561 HTTP/1.1 302 Found  (text/html)
275 GET /pQBtWj HTTP/1.1
542 HTTP/1.1 302 Found
312 GET /files/june11.dll HTTP/1.1
946 HTTP/1.1 200 OK
```



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

55 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
june11.dll
invalid-signature overlay pedll signed

549.84 KB Size

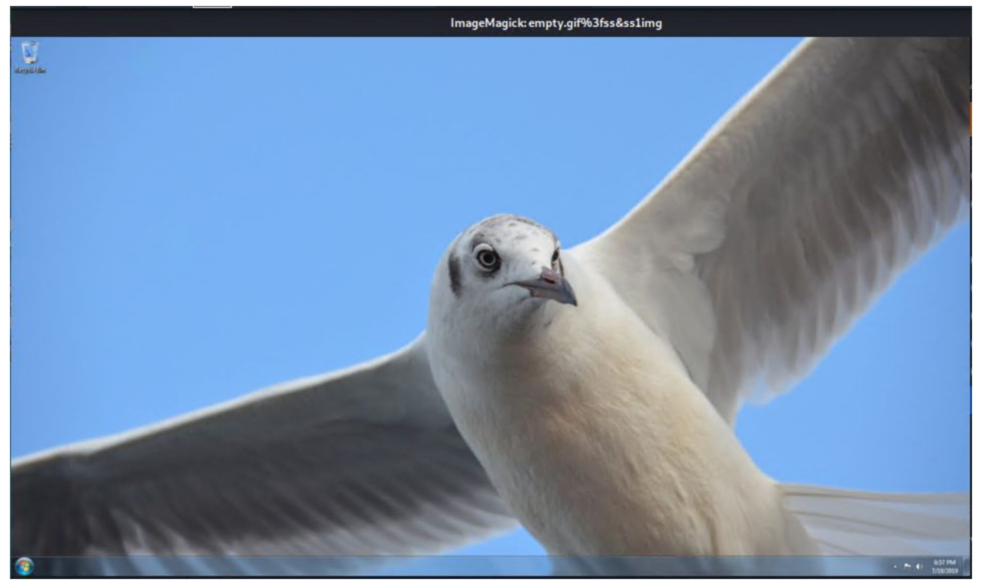
2020-08-06 09:00:02 UTC 8 days ago

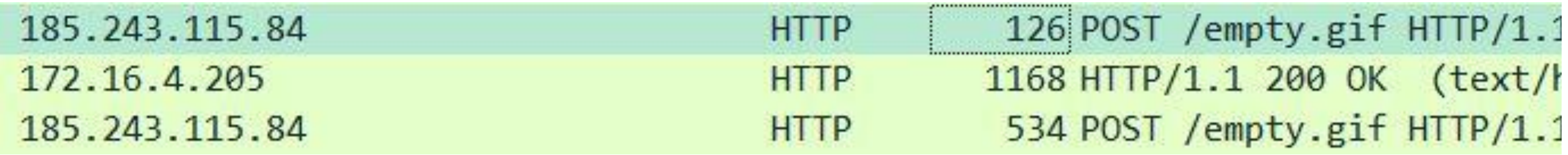
Ad-Aware	Trojan.GenericKD.34007934	AegisLab	Trojan.Multi.Generic.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.GenericKD.34007934	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
SecureAge APEX	Malicious	Arcabit	Trojan.Generic.D206EB7E
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]

Net Support RAT Download

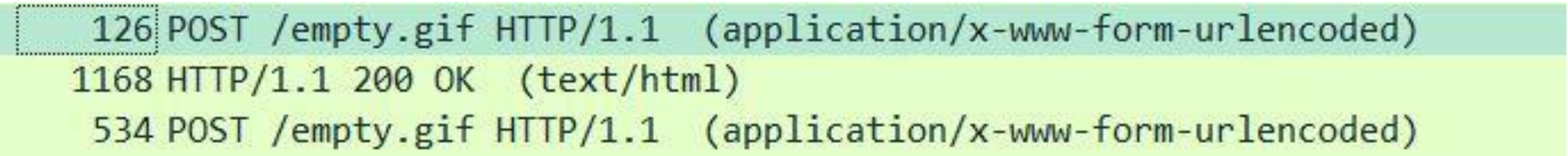
Remote Access Trojan:

- green.nattingsolutions.co 185.243.115.84
  - This is a known infected site
- Post request to 185.243.115.84 included.
  - 501 ASCII hexadecimal data files empty.gif
  - 2 screenshots of the infected users desktop empty.gif?ss&ss1.img | empty.gif?ss&ss2.img
- Post request to 31.7.62.214/fakeurl.htm
  - 114 application/x-www-form-urlencodedfakeurl.html
  - This file name is associated with the NetSupportRat

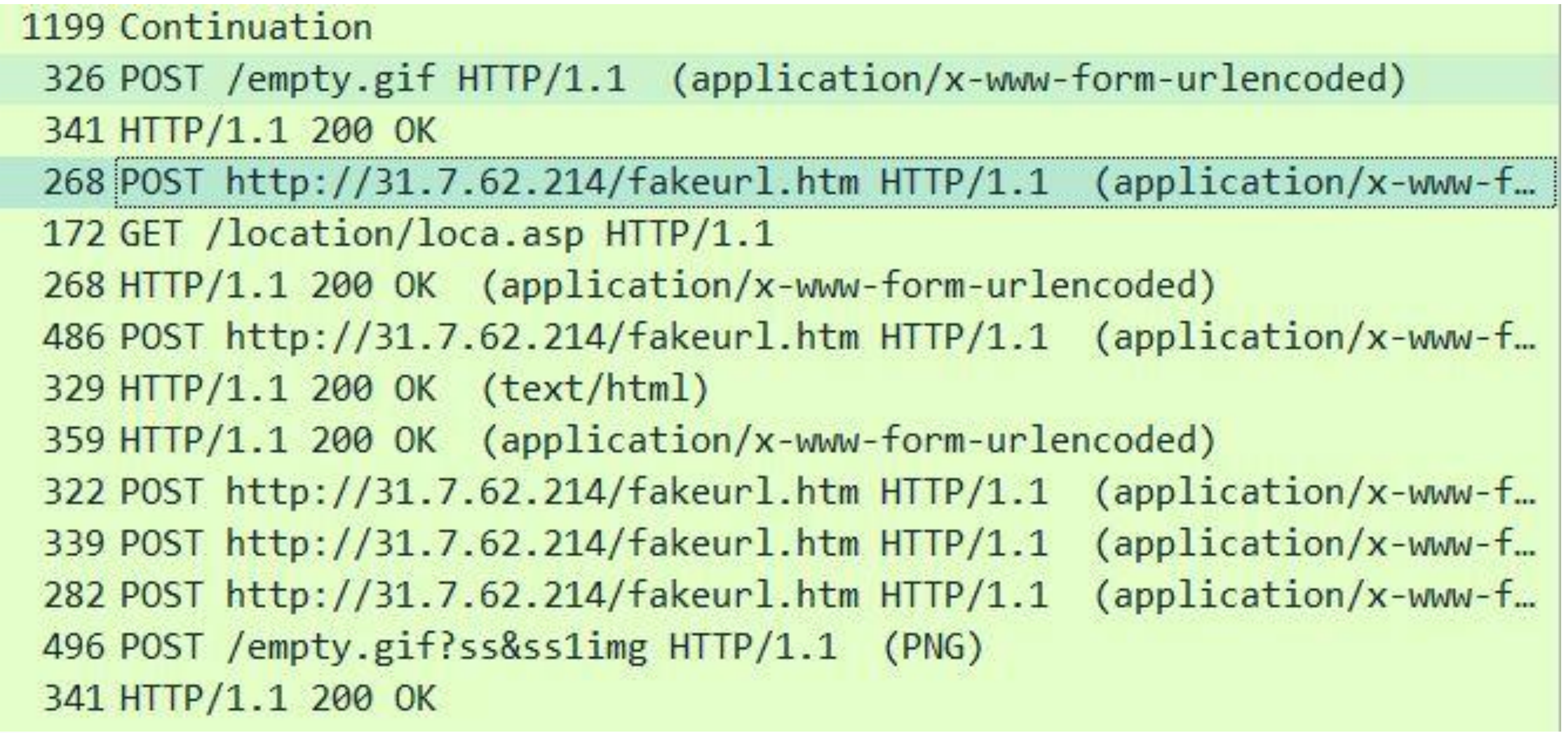




```
185.243.115.84                    HTTP        126 POST /empty.gif HTTP/1.1
172.16.4.205                      HTTP       1168 HTTP/1.1 200 OK  (text/h
185.243.115.84                    HTTP        534 POST /empty.gif HTTP/1.1
```



```
  126 POST /empty.gif HTTP/1.1  (application/x-www-form-urlencoded)
 1168 HTTP/1.1 200 OK  (text/html)
  534 POST /empty.gif HTTP/1.1  (application/x-www-form-urlencoded)
```



```
1199 Continuation
 326 POST /empty.gif HTTP/1.1  (application/x-www-form-urlencoded)
 341 HTTP/1.1 200 OK
 268 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-f…
 172 GET /location/loca.asp HTTP/1.1
 268 HTTP/1.1 200 OK  (application/x-www-form-urlencoded)
 486 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-f…
 329 HTTP/1.1 200 OK  (text/html)
 359 HTTP/1.1 200 OK  (application/x-www-form-urlencoded)
 322 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-f…
 339 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-f…
 282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-f…
 496 POST /empty.gif?ss&ss1img HTTP/1.1  (PNG)
 341 HTTP/1.1 200 OK
```

The End