Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Team: Patricia Bottari, Mike Wong, Pio Castro, Sheldon Bryan

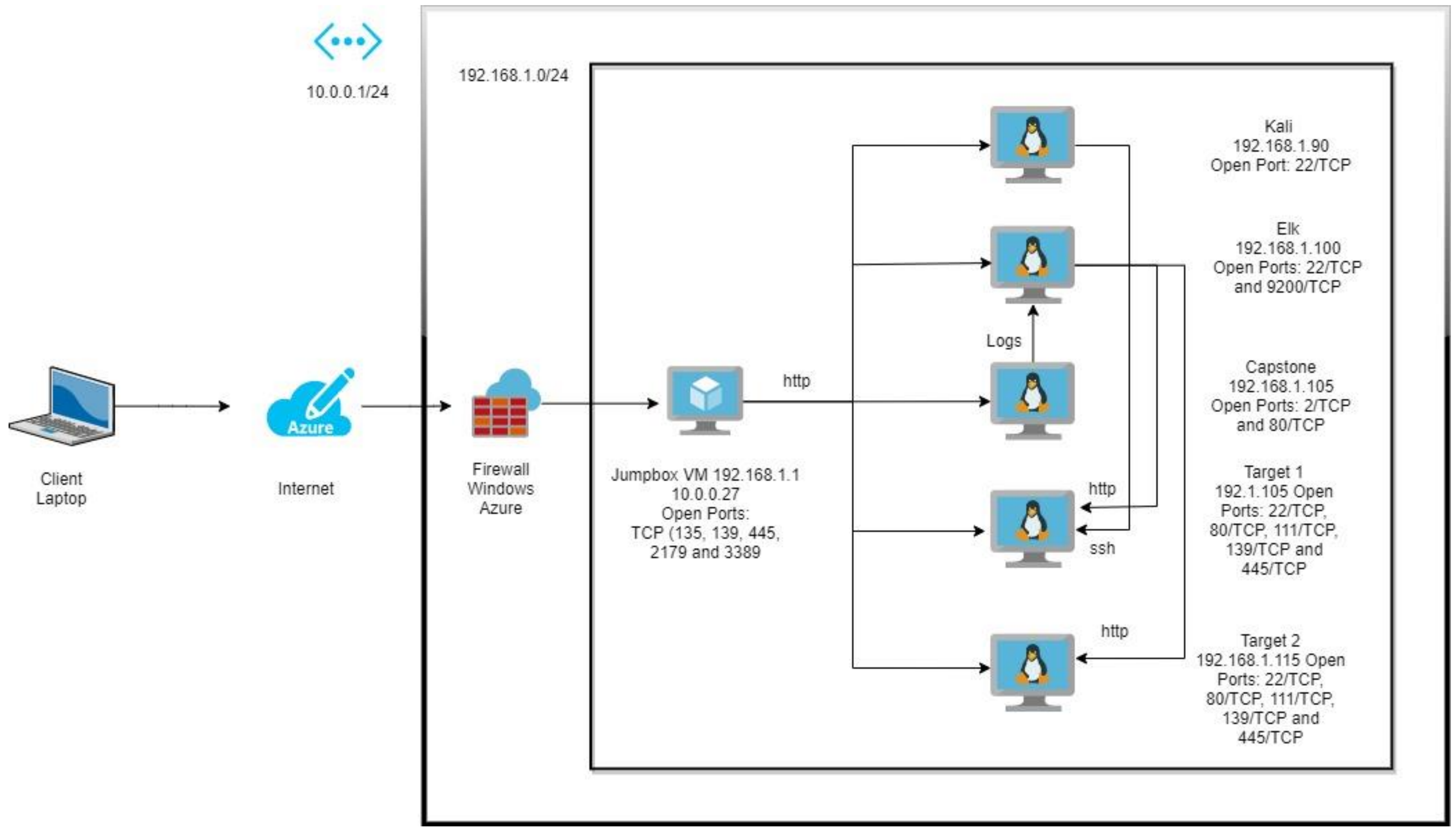
Table of Contents

This document contains the following resources:

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

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: Linux 2.6.32
Hostname: Kali

IPv4:192.168.1.100
OS: Linux
Hostname: Elk

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux 3.2 - 4.9
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux 3.2 - 4.9
Hostname: Target 2

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Exposed Network Information	Machine responds to nmap and wpscan.	Information on open ports, services, and usernames.
Weak Password Policy	Password policy that failed to establish rules for password creation such as length and complexity.	Increases the probability of an attacker having success using brute force and dictionary attacks against user accounts or guessing a password.
Open SSH port	Allow remote connection with server.	Give attackers unauthorized remote access.
Sensitive Information Leak	Username and password included in config file.	Attacker can gain access to login information.
SQL Database Access	Allow access to SQL database.	Attackers can get access to important databases.
Root privilege escalation with Python	Available information about user permission levels and server login/password.	Increases the probability of an attacker to gain root access by running python script.

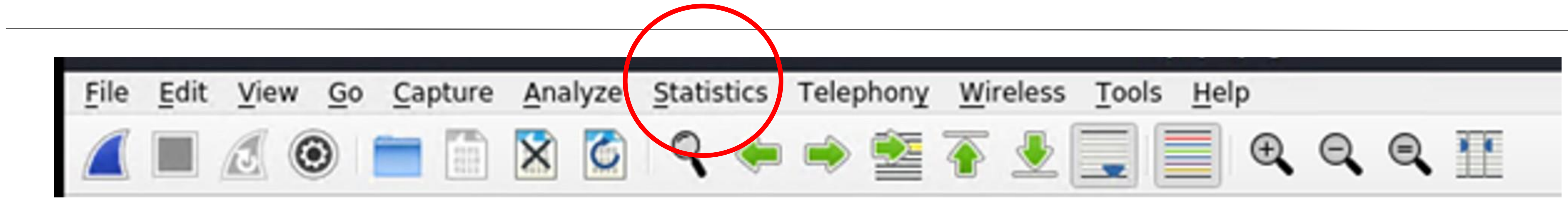
Traffic Profile

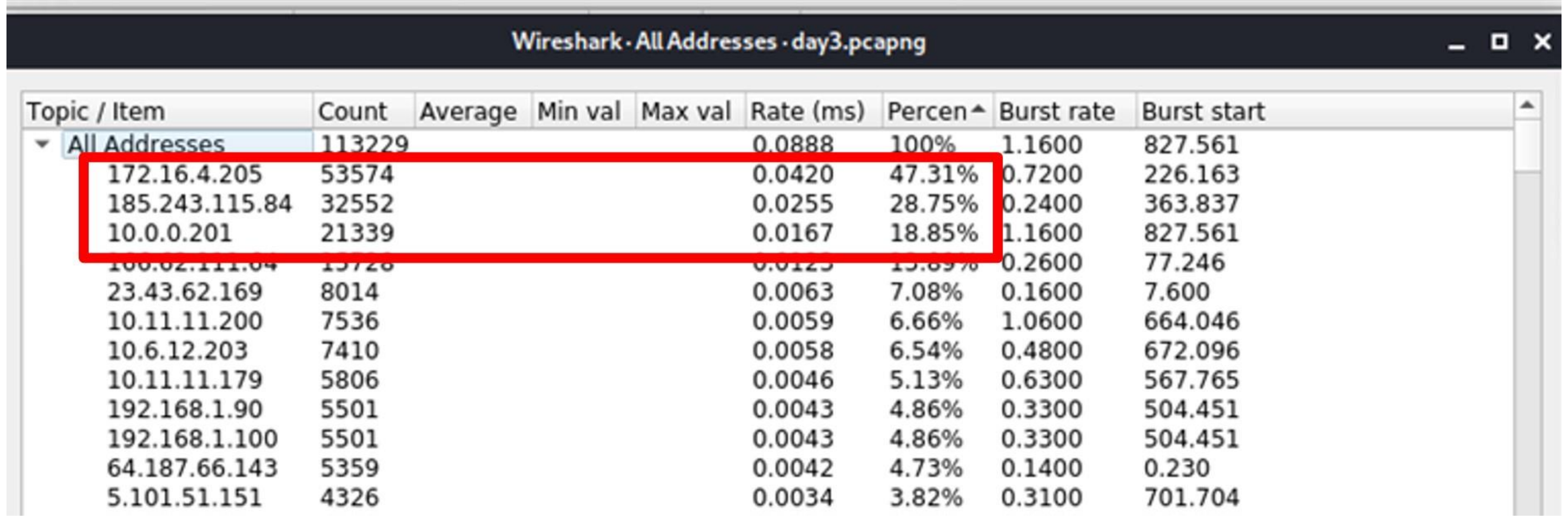
Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 - 47.31% 185.243.115.84 - 28.75% 10.0.0.201 - 18.85%	Machines that sent the most traffic.
Most Common Protocols	TCP - 89.49% UDP - 10.43% None - 0.08%	Three most common protocols on the network.
# of Unique IP Addresses	IPv4 - 113229 IPv6 - 2	Count of observed IP addresses.
Subnets	10.0.0.0/24 10.6.12.0/24 172.16.4.0/24 192.168.1.0/24	Observed subnet ranges.
# of Malware Species	One (1): june11.ddl	Number of malware binaries identified in traffic.

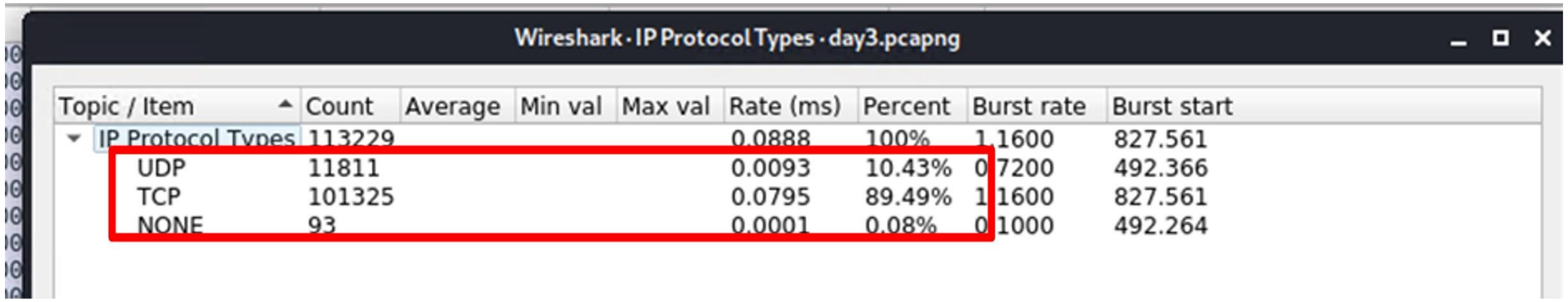
Traffic Profile





Wireshark · All Addresses · day3.pcapng

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
All Addresses	113229				0.0888	100%	1.1600	827.561
172.16.4.205	53574				0.0420	47.31%	0.7200	226.163
185.243.115.84	32552				0.0255	28.75%	0.2400	363.837
10.0.0.201	21339				0.0167	18.85%	1.1600	827.561
166.62.111.64	15728				0.0123	13.89%	0.2600	77.246
23.43.62.169	8014				0.0063	7.08%	0.1600	7.600
10.11.11.200	7536				0.0059	6.66%	1.0600	664.046
10.6.12.203	7410				0.0058	6.54%	0.4800	672.096
10.11.11.179	5806				0.0046	5.13%	0.6300	567.765
192.168.1.90	5501				0.0043	4.86%	0.3300	504.451
192.168.1.100	5501				0.0043	4.86%	0.3300	504.451
64.187.66.143	5359				0.0042	4.73%	0.1400	0.230
5.101.51.151	4326				0.0034	3.82%	0.3100	701.704



Wireshark · IP Protocol Types · day3.pcapng

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
IP Protocol Types	113229				0.0888	100%	1.1600	827.561
UDP	11811				0.0093	10.43%	0.7200	492.366
TCP	101325				0.0795	89.49%	1.1600	827.561
NONE	93				0.0001	0.08%	0.1000	492.264

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity:

“Normal” Activity

- Watching YouTube
- Searching websites such as: sabethahospitals.com; mysocalledchaos.com and iphonehacks.com

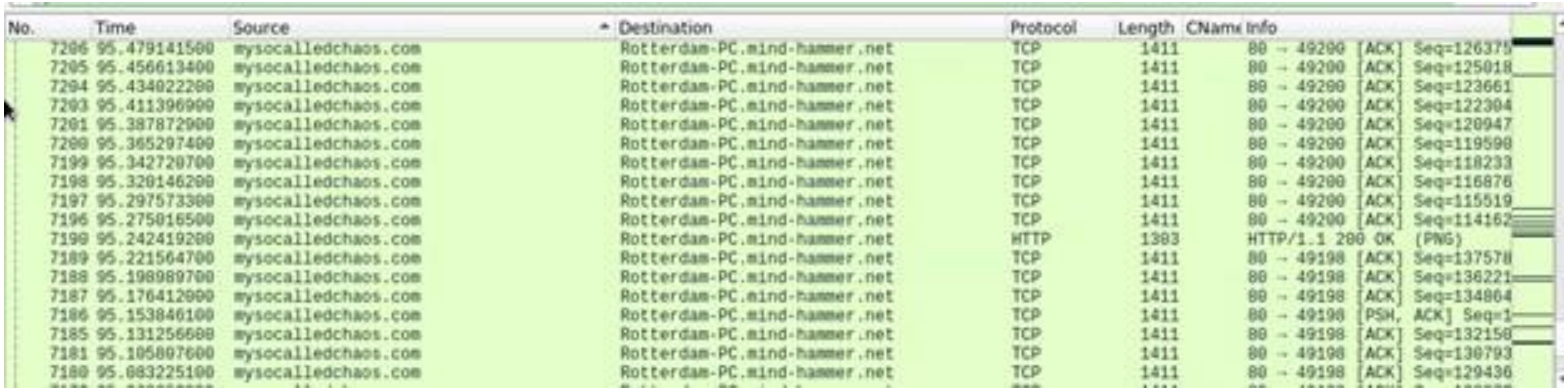
Suspicious Activity

- Malware download
- Illegal video download

Normal Activity

Internet Browsing Normal Behavior 1

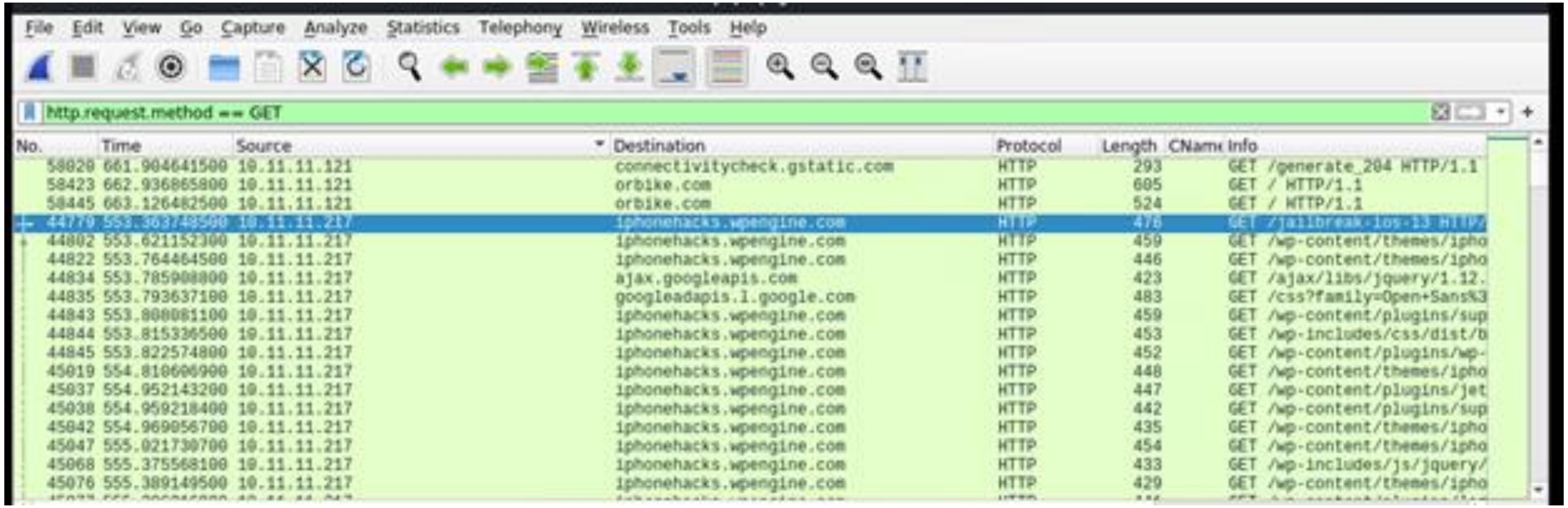
- Observed traffic for standard query, GET requests and TCP re-transmissions.
- The packets captured were for HTTP and TCP protocols.
- Browsing the site mysocalledchaos.com



No.	Time	Source	Destination	Protocol	Length	CName	Info
7206	95.479141500	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=126375
7205	95.456613400	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=125018
7204	95.434022200	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=123661
7203	95.411396900	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=122304
7201	95.387872900	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=120947
7200	95.365297400	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=119590
7199	95.342720700	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=118233
7198	95.320146200	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=116876
7197	95.297573300	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=115519
7196	95.275016500	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49200 [ACK] Seq=114162
7190	95.242419200	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	HTTP	1303		HTTP/1.1 200 OK (PNG)
7189	95.221564700	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49198 [ACK] Seq=137578
7188	95.198989700	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49198 [ACK] Seq=136221
7187	95.176412000	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49198 [ACK] Seq=134864
7186	95.153846100	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49198 [PSH, ACK] Seq=1
7185	95.131256600	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49198 [ACK] Seq=132150
7181	95.105807600	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49198 [ACK] Seq=130793
7180	95.083225100	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	1411		80 → 49198 [ACK] Seq=129436

Browsing Normal Behavior 2

- Observed traffic for standard query, GET requests and TCP re-transmissions.
- The packets captured were for HTTP and TCP protocols.
- Browsing the site iphonehacks.com: jailbreak articles

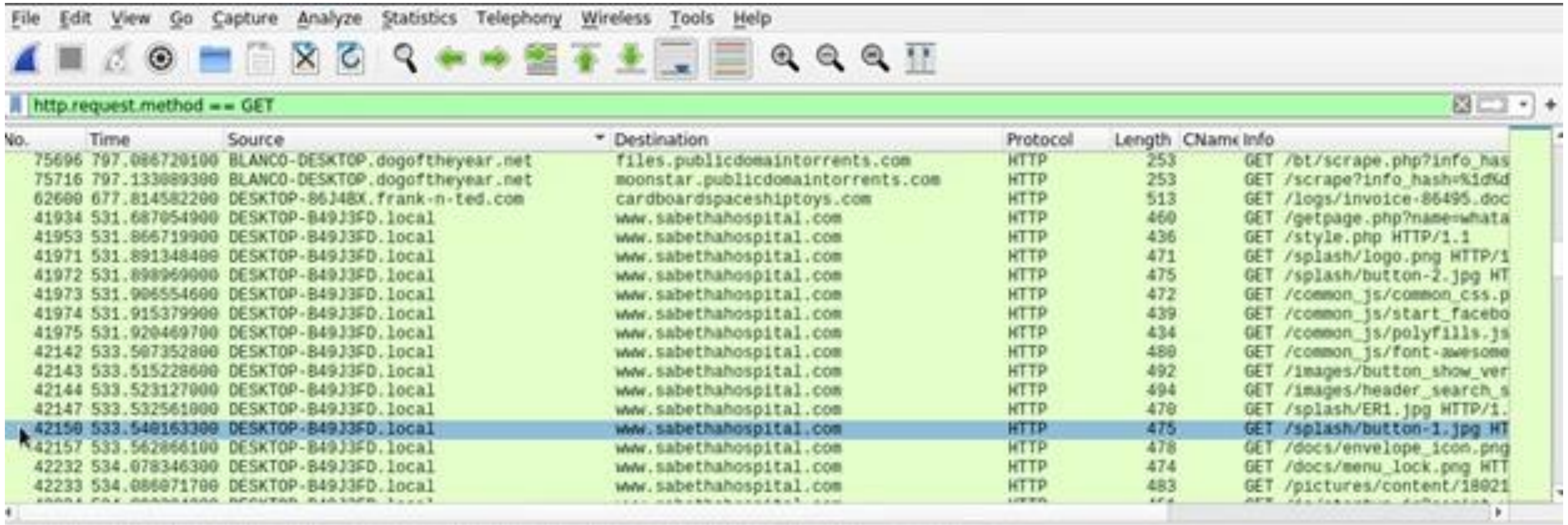


http.request.method == GET

No.	Time	Source	Destination	Protocol	Length	CName	Info
58020	661.904641500	10.11.11.121	connectivitycheck.gstatic.com	HTTP	293		GET /generate_204 HTTP/1.1
58423	662.936865800	10.11.11.121	orbike.com	HTTP	605		GET / HTTP/1.1
58445	663.126482500	10.11.11.121	orbike.com	HTTP	524		GET / HTTP/1.1
44779	553.363748500	10.11.11.217	iphonehacks.wpengine.com	HTTP	476		GET /jailbreak-ios-13 HTTP/
44802	553.621152300	10.11.11.217	iphonehacks.wpengine.com	HTTP	459		GET /wp-content/themes/ipho
44822	553.764464500	10.11.11.217	iphonehacks.wpengine.com	HTTP	446		GET /wp-content/themes/ipho
44834	553.785908800	10.11.11.217	ajax.googleapis.com	HTTP	423		GET /ajax/libs/jquery/1.12.
44835	553.793637100	10.11.11.217	googleadapis.l.google.com	HTTP	483		GET /css?family=Open+Sans%3
44843	553.808081100	10.11.11.217	iphonehacks.wpengine.com	HTTP	459		GET /wp-content/plugins/sup
44844	553.815336500	10.11.11.217	iphonehacks.wpengine.com	HTTP	453		GET /wp-includes/css/dist/b
44845	553.822574800	10.11.11.217	iphonehacks.wpengine.com	HTTP	452		GET /wp-content/plugins/wp-
45019	554.810606900	10.11.11.217	iphonehacks.wpengine.com	HTTP	448		GET /wp-content/themes/ipho
45037	554.952143200	10.11.11.217	iphonehacks.wpengine.com	HTTP	447		GET /wp-content/plugins/jet
45038	554.959218400	10.11.11.217	iphonehacks.wpengine.com	HTTP	442		GET /wp-content/plugins/sup
45042	554.969056700	10.11.11.217	iphonehacks.wpengine.com	HTTP	435		GET /wp-content/themes/ipho
45047	555.021730700	10.11.11.217	iphonehacks.wpengine.com	HTTP	454		GET /wp-content/themes/ipho
45068	555.375568100	10.11.11.217	iphonehacks.wpengine.com	HTTP	433		GET /wp-includes/js/jquery/
45076	555.389149500	10.11.11.217	iphonehacks.wpengine.com	HTTP	429		GET /wp-content/themes/ipho

Browsing Normal Behavior 3

- Observed traffic for standard query, GET requests.
- The packets captured were for HTTP and TCP protocols.
- Browsing the site sabethahospitals.com



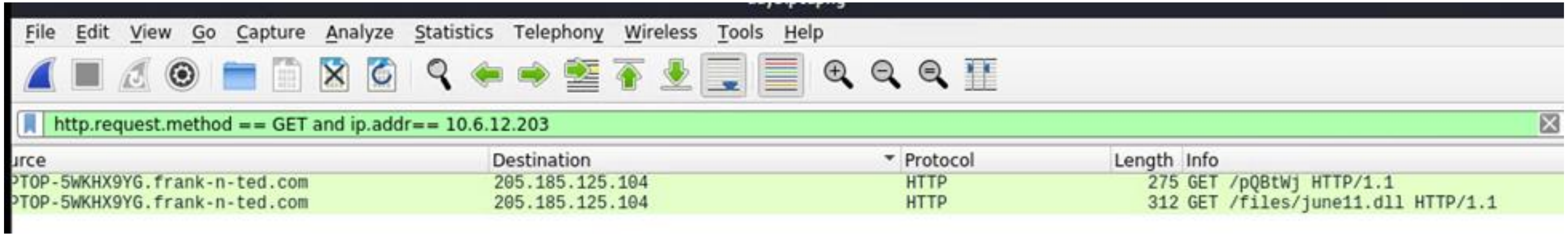
http.request.method == GET

No.	Time	Source	Destination	Protocol	Length	CName	Info
75696	797.086720100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	253		GET /bt/scrape.php?info_has
75716	797.133089300	BLANCO-DESKTOP.dogoftheyear.net	moonstar.publicdomaintorrents.com	HTTP	253		GET /scrape?info_hash=%1d%d
62600	677.814582200	DESKTOP-86J4BX.frank-n-ted.com	cardboardspaceshiptoys.com	HTTP	513		GET /logs/invoice-86495.doc
41934	531.687054900	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	460		GET /getpage.php?name=whata
41953	531.866719900	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	436		GET /style.php HTTP/1.1
41971	531.891348400	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	471		GET /splash/logo.png HTTP/1
41972	531.898969000	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	475		GET /splash/button-2.jpg HT
41973	531.906554600	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	472		GET /common_js/common_css.p
41974	531.915379900	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	439		GET /common_js/start_facebo
41975	531.920469700	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	434		GET /common_js/polyfills.js
42142	533.507352800	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	480		GET /common_js/font-awesome
42143	533.515228600	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	492		GET /images/button_show_ver
42144	533.523127000	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	494		GET /images/header_search_s
42147	533.532561000	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	470		GET /splash/ER1.jpg HTTP/1.
42150	533.540163300	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	475		GET /splash/button-1.jpg HT
42157	533.562866100	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	478		GET /docs/envelope_icon.png
42232	534.078346300	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	474		GET /docs/menu_lock.png HTT
42233	534.086071700	DESKTOP-B49J3FD.local	www.sabethahospital.com	HTTP	483		GET /pictures/content/18021

Malicious Activity

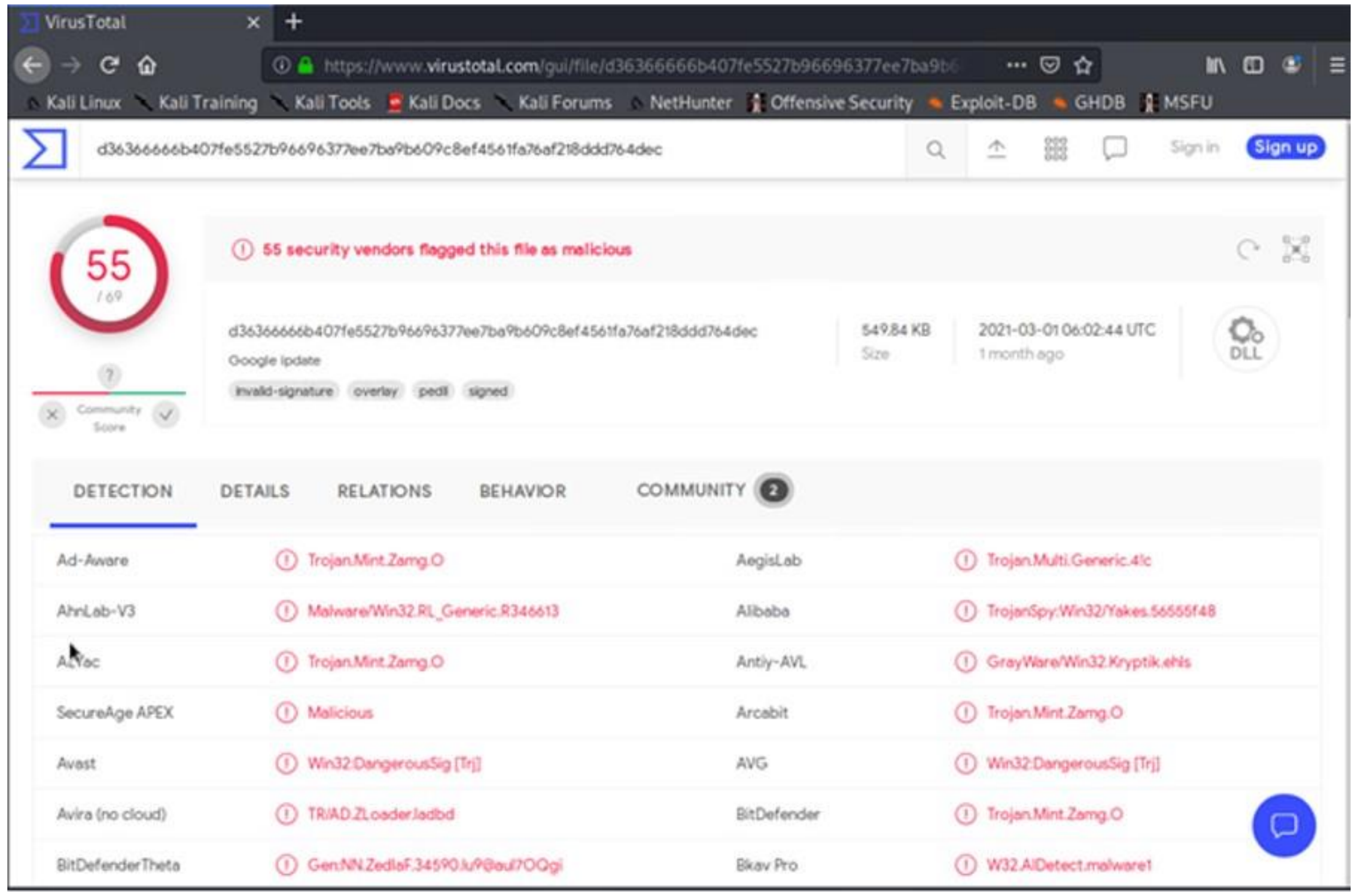
HTTP Malicious Behavior 1

- User views a malicious file containing dos.exe malware: 205.185.125.104/files/june11.dll
- Traffic was over HTTP.



```
http.request.method == GET and ip.addr== 10.6.12.203
```

```
urce                              Destination              Protocol   Length Info
PTOP-5WKHX9YG.frank-n-ted.com     205.185.125.104          HTTP          275 GET /pQBtWj HTTP/1.1
PTOP-5WKHX9YG.frank-n-ted.com     205.185.125.104          HTTP          312 GET /files/june11.dll HTTP/1.1
```



https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

55 / 69

55 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Google Ipdate

invalid-signature overlay pedll signed

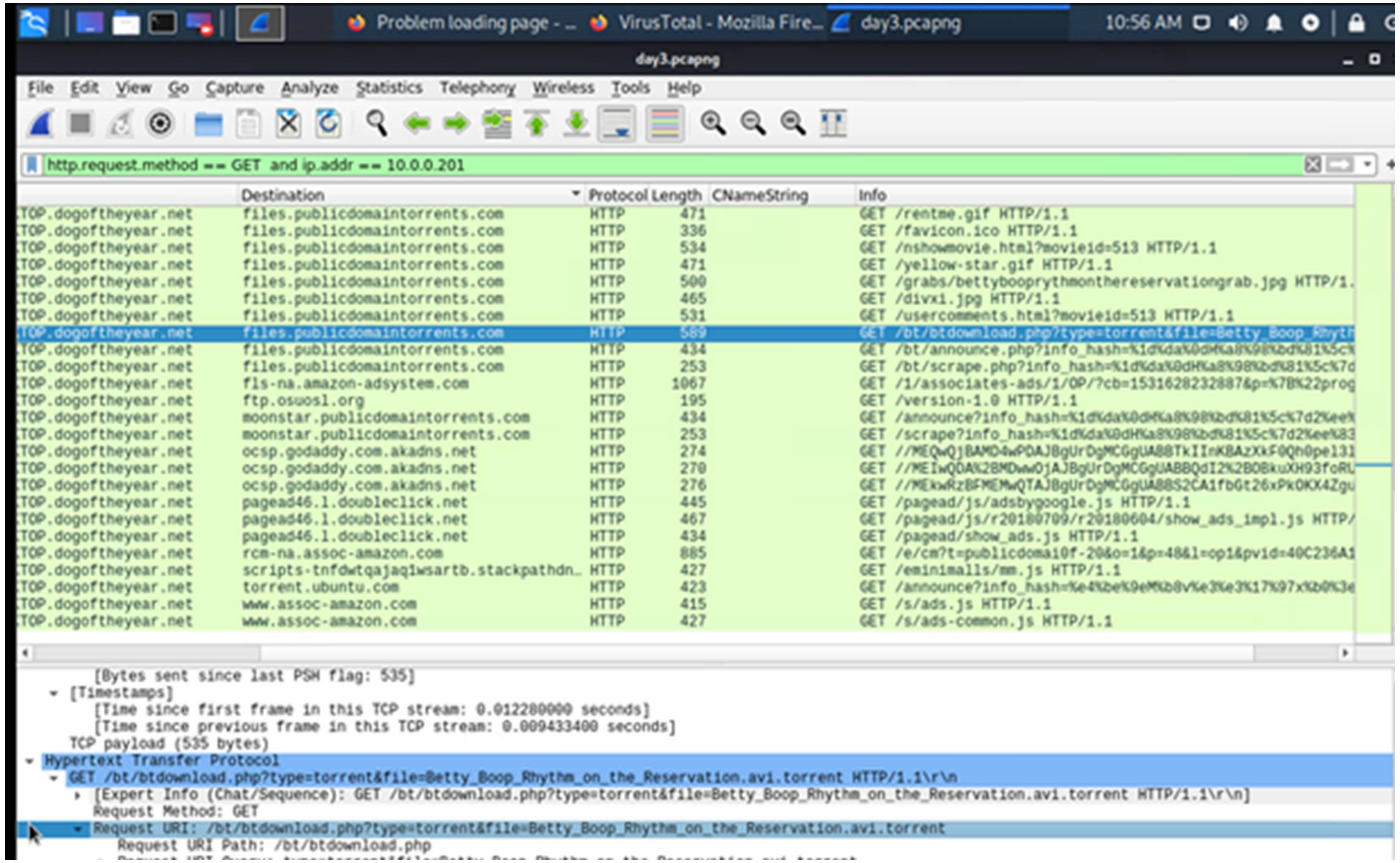
549.84 KB Size

2021-03-01 06:02:44 UTC 1 month ago

Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	Trojan.Multi.Generic.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
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.34590.lu9@aul7OQgi	Bkav Pro	W32.AIDetect.malware1

Illegal Download Malicious Behavior 2

- MAC address destination was 00:16:17:18:66:c8.
- OS version: Windows NT 10 use
- Username: elmer.blanco.
- Malicious file Betty_Boop_Rythym_on_the_Reservation.avi.torrent was downloaded.


Problem loading page - ...
VirusTotal - Mozilla Fire...
day3.pcapng
10:56 AM
day3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method == GET and ip.addr == 10.0.0.201

```
                     Destination                             Protocol Length CNameString   Info
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     471                GET /rentme.gif HTTP/1.1
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     336                GET /favicon.ico HTTP/1.1
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     534                GET /nshowmovie.html?movieid=513 HTTP/1.1
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     471                GET /yellow-star.gif HTTP/1.1
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     500                GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     465                GET /divx1.jpg HTTP/1.1
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     531                GET /usercomments.html?movieid=513 HTTP/1.1
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     589                GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhyth
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     434                GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%
.TOP.dogoftheyear.net   files.publicdomaintorrents.com         HTTP     253                GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d
.TOP.dogoftheyear.net   fls-na.amazon-adsystem.com             HTTP    1067                GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22prog
.TOP.dogoftheyear.net   ftp.osuosl.org                         HTTP     195                GET /version-1.0 HTTP/1.1
.TOP.dogoftheyear.net   moonstar.publicdomaintorrents.com      HTTP     434                GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%
.TOP.dogoftheyear.net   moonstar.publicdomaintorrents.com      HTTP     253                GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%83
.TOP.dogoftheyear.net   ocsp.godaddy.com.akadns.net            HTTP     274                GET //MEQwQjBAMD4wPDAJBgUrDgMCGgUABBTkIInKBAzXkF0Qh0pel31
.TOP.dogoftheyear.net   ocsp.godaddy.com.akadns.net            HTTP     270                GET //MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBQdI2%2BOBkuXH93foRU
.TOP.dogoftheyear.net   ocsp.godaddy.com.akadns.net            HTTP     276                GET //MEkwRzBFMEMwQTAJBgUrDgMCGgUABBS2CA1fbGt26xPkOKX4Zgu
.TOP.dogoftheyear.net   pagead46.l.doubleclick.net             HTTP     445                GET /pagead/js/adsbygoogle.js HTTP/1.1
.TOP.dogoftheyear.net   pagead46.l.doubleclick.net             HTTP     467                GET /pagead/js/r20180709/r20180604/show_ads_impl.js HTTP/
.TOP.dogoftheyear.net   pagead46.l.doubleclick.net             HTTP     434                GET /pagead/show_ads.js HTTP/1.1
.TOP.dogoftheyear.net   rcm-na.assoc-amazon.com                HTTP     885                GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A1
.TOP.dogoftheyear.net   scripts-tnfdwtqajaq1wsartb.stackpathdn… HTTP     427                GET /eminimalls/mm.js HTTP/1.1
.TOP.dogoftheyear.net   torrent.ubuntu.com                     HTTP     423                GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e
.TOP.dogoftheyear.net   www.assoc-amazon.com                   HTTP     415                GET /s/ads.js HTTP/1.1
.TOP.dogoftheyear.net   www.assoc-amazon.com                   HTTP     427                GET /s/ads-common.js HTTP/1.1
```

```
      [Bytes sent since last PSH flag: 535]
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.012280000 seconds]
      [Time since previous frame in this TCP stream: 0.009433400 seconds]
    TCP payload (535 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      Request Method: GET
    ▾ Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
        Request URI Path: /bt/btdownload.php
```

The End