Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

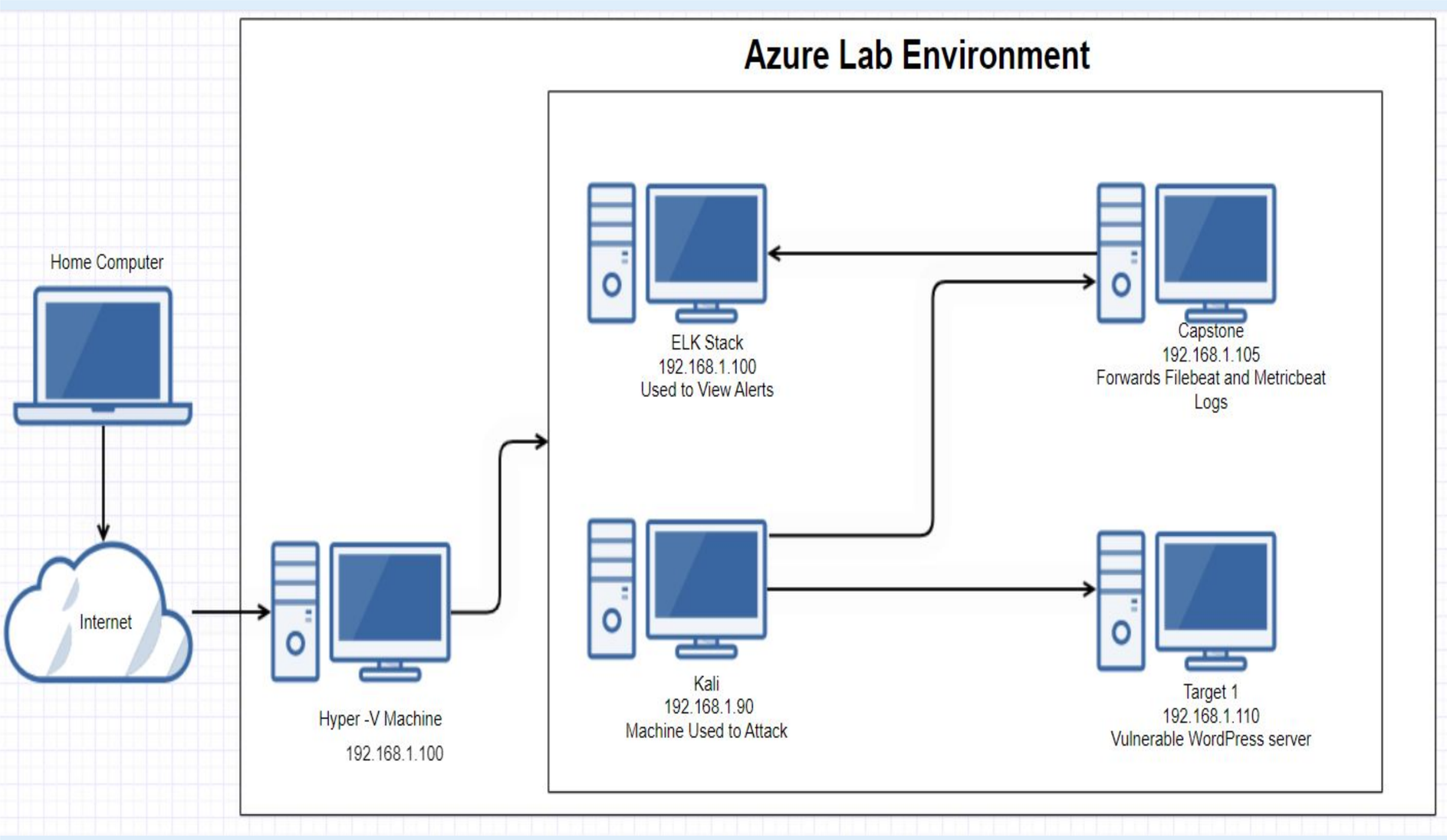
By: Jesus Martinez, Traxus Broadnax, Ardavan Moghaddam, Monica Garcia, Arick Johnson

Table of Contents

This document contains the following resources:

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
Hostname: Kali

IPv4:192.168.1.100
OS: Linux
Hostname: ELK

IPv4:192.168.1.110
OS: Linux
Hostname: Target 1

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Wordpress User Enumeration	By using wpscan, we were able to obtain Michael & Steven's user names	Access into Target 1 via SSH, as well as MySQL, which reveals passwords
MySQL Database Breach	Access to credentials by using wp-config.php, as well as hashes	User's credentials are easily accessible to attackers
Weak Passwords	Passwords were easily accessible by using dictionary brute force attack	Passwords are accessed with minimal efforts

Cont. Critical Vulnerabilities: Target 1

Wordpress User Enumeration

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u
_______________________________________________________________
```

```
[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Weak Passwords

```
root@Kali:~# cd Desktop/
root@Kali:~/Desktop# ls
wp_hashes.txt
root@Kali:~/Desktop# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 43 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 37 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 33 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 32 candidates buffered for the current salt, minimum 48 neede
d for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 23 candidates buffered for the current salt, minimum 48 neede
d for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (user2)
```

My SQL Database Breach

```
michael@target1:/var/www/html/wordpress$ cat wp-config.php
```

```
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----
------+---------------------+---------------------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | use
r_url | user_registered     | user_activation_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----
------+---------------------+---------------------+-------------+---------------+
|  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 |
+----+------------+------------------------------------+---------------+-------------------+----
------+---------------------+---------------------+-------------+---------------+
2 rows in set (0.00 sec)

mysql>
```

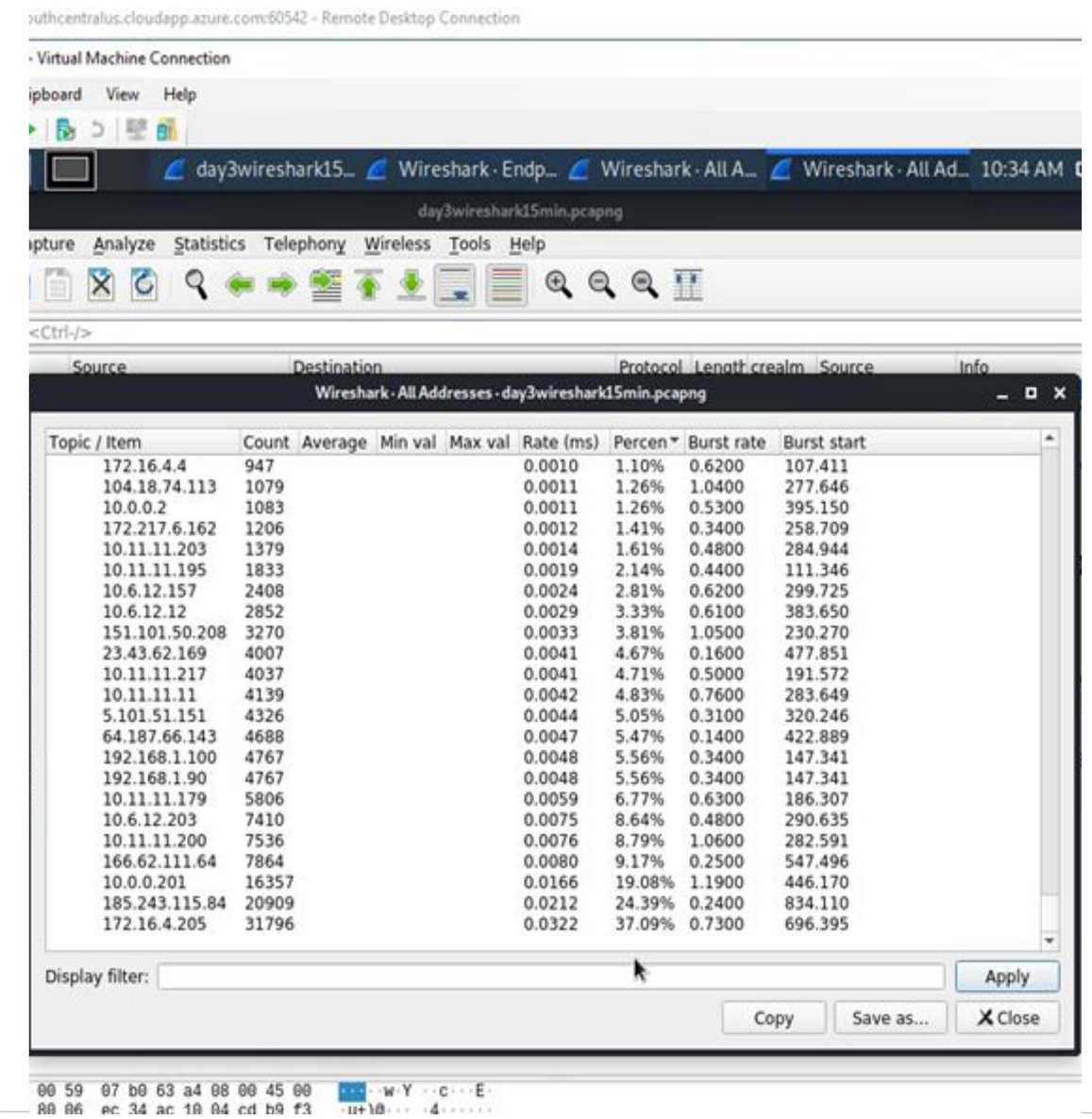
Traffic Profile

Traffic Profile

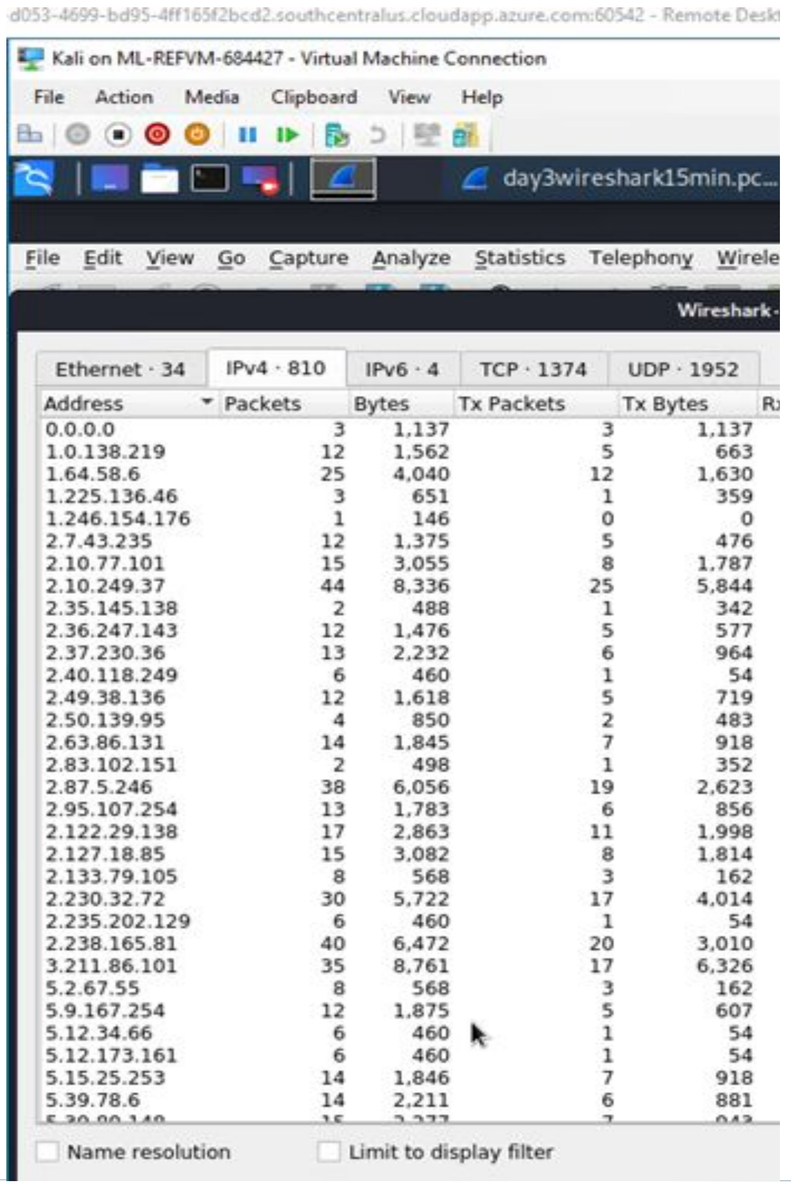
Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205(37.09%) 185.243.115.84(24.39%) 10.0.0.201(19.08%)	Machines that sent the most traffic.
Most Common Protocols	TCP, UDP	Three most common protocols on the network.
# of Unique IP Addresses	810	On that 15 minutes that we start the traffic we found around 810 different and unique IPs.
Subnets	172.16.4.0/24 185.243.115.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	june11.dll	Upload the file on virustotal.com most of the security vendors such as Mcafee, Alibaba etc. are distinguished as malicious.

In first Screenshot we can see top 3 IP addresses 172.16.4.205 and 185.243.115.84, 10.0.0.201 they created around 80 percents of all traffics. and in the second screenshot we can see 810 Unique IP Addresses.

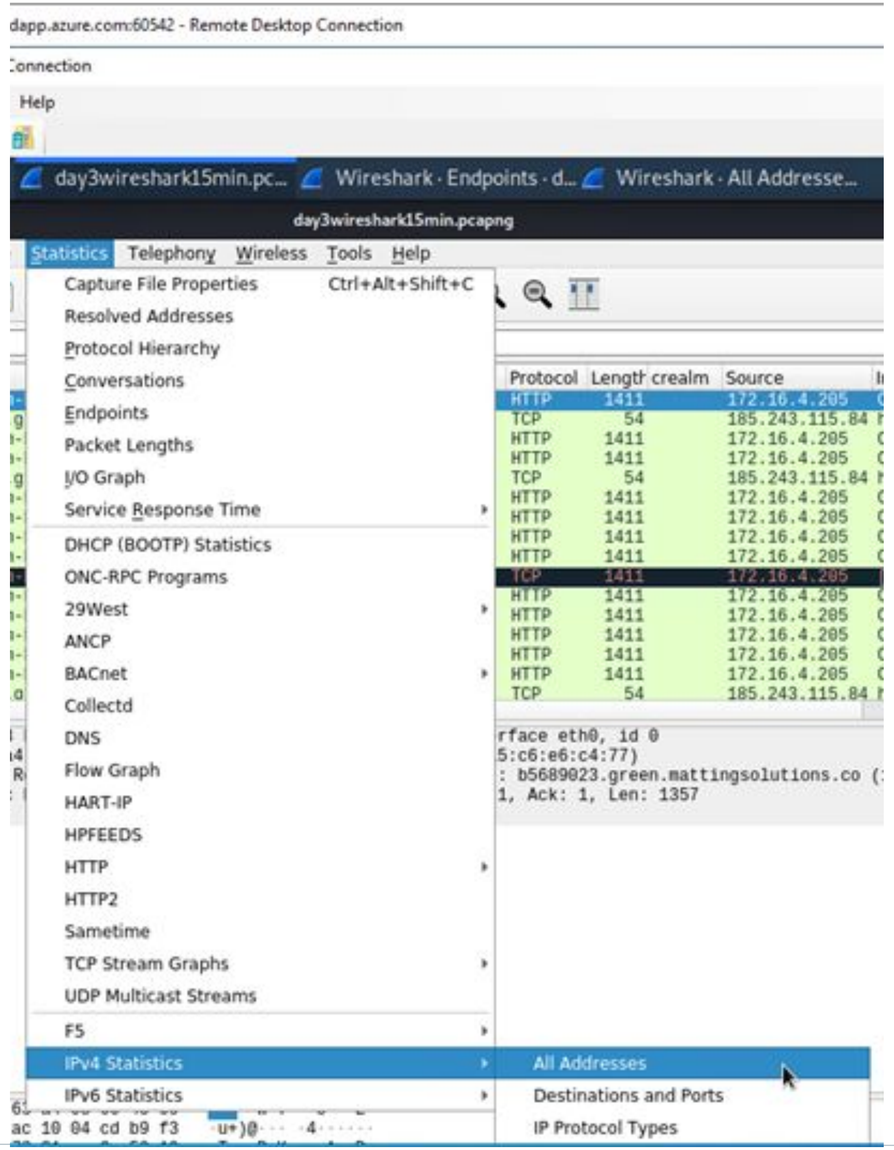


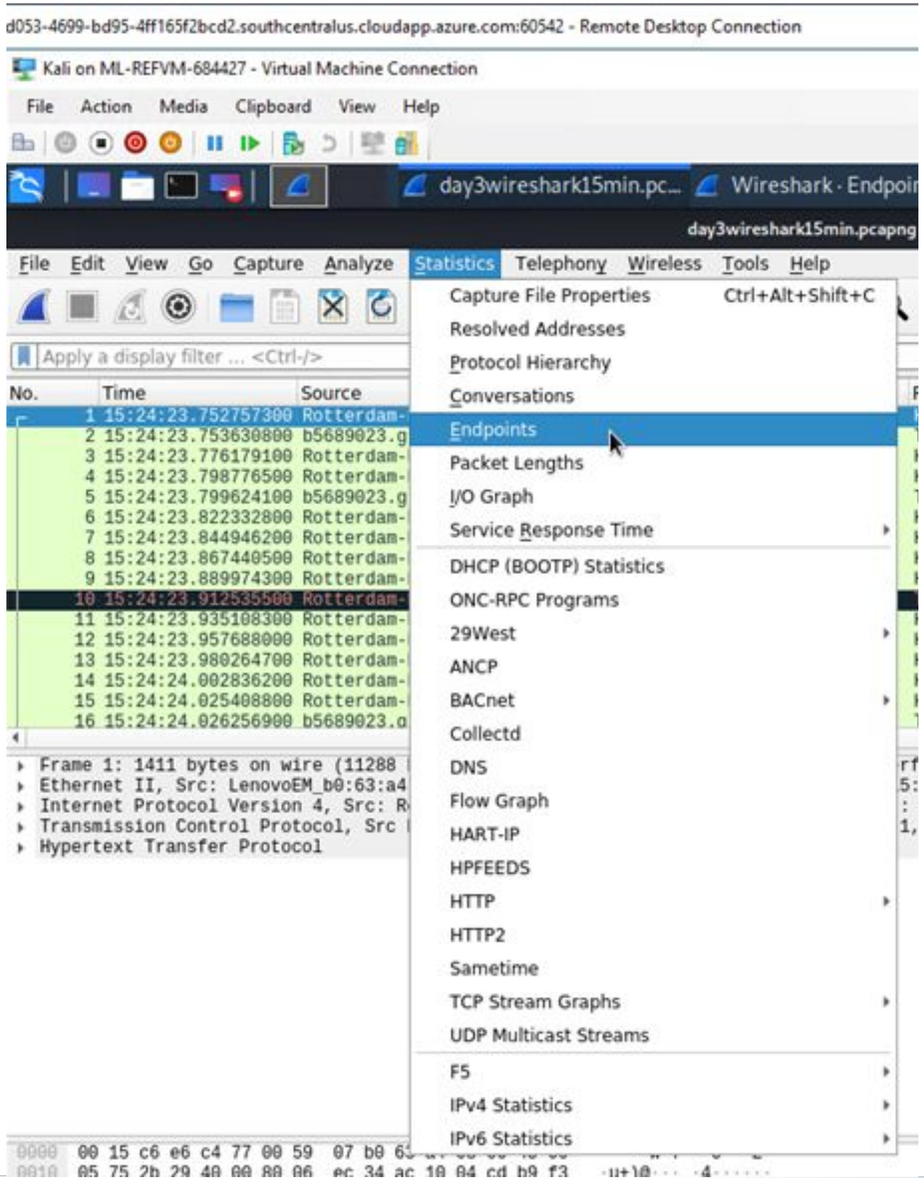
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percen	Burst rate	Burst start
172.16.4.4	947				0.0010	1.10%	0.6200	107.411
104.18.74.113	1079				0.0011	1.26%	1.0400	277.646
10.0.0.2	1083				0.0011	1.26%	0.5300	395.150
172.217.6.162	1206				0.0012	1.41%	0.3400	258.709
10.11.11.203	1379				0.0014	1.61%	0.4800	284.944
10.11.11.195	1833				0.0019	2.14%	0.4400	111.346
10.6.12.157	2408				0.0024	2.81%	0.6200	299.725
10.6.12.12	2852				0.0029	3.33%	0.6100	383.650
151.101.50.208	3270				0.0033	3.81%	1.0500	230.270
23.43.62.169	4007				0.0041	4.67%	0.1600	477.851
10.11.11.217	4037				0.0041	4.71%	0.5000	191.572
10.11.11.11	4139				0.0042	4.83%	0.7600	283.649
5.101.51.151	4326				0.0044	5.05%	0.3100	320.246
64.187.66.143	4688				0.0047	5.47%	0.1400	422.889
192.168.1.100	4767				0.0048	5.56%	0.3400	147.341
192.168.1.90	4767				0.0048	5.56%	0.3400	147.341
10.11.11.179	5806				0.0059	6.77%	0.6300	186.307
10.6.12.203	7410				0.0075	8.64%	0.4800	290.635
10.11.11.200	7536				0.0076	8.79%	1.0600	282.591
166.62.111.64	7864				0.0080	9.17%	0.2500	547.496
10.0.0.201	16357				0.0166	19.08%	1.1900	446.170
185.243.115.84	20909				0.0212	24.39%	0.2400	834.110
172.16.4.205	31796				0.0322	37.09%	0.7300	696.395



Address	Packets	Bytes	Tx Packets	Tx Bytes
0.0.0.0	3	1,137	3	1,137
1.0.138.219	12	1,562	5	663
1.64.58.6	25	4,040	12	1,630
1.225.136.46	3	651	1	359
1.246.154.176	1	146	0	0
2.7.43.235	12	1,375	5	476
2.10.77.101	15	3,055	8	1,787
2.10.249.37	44	8,336	25	5,844
2.35.145.138	2	488	1	342
2.36.247.143	12	1,476	5	577
2.37.230.36	13	2,232	6	964
2.40.118.249	6	460	1	54
2.49.38.136	12	1,618	5	719
2.50.139.95	4	850	2	483
2.63.86.131	14	1,845	7	918
2.83.102.151	2	498	1	352
2.87.5.246	38	6,056	19	2,623
2.95.107.254	13	1,783	6	856
2.122.29.138	17	2,863	11	1,998
2.127.18.85	15	3,082	8	1,814
2.133.79.105	8	568	3	162
2.230.32.72	30	5,722	17	4,014
2.235.202.129	6	460	1	54
2.238.165.81	40	6,472	20	3,010
3.211.86.101	35	8,761	17	6,326
5.2.67.55	8	568	3	162
5.9.167.254	12	1,875	5	607
5.12.34.66	6	460	1	54
5.12.173.161	6	460	1	54
5.15.25.253	14	1,846	7	918
5.39.78.6	14	2,211	6	881

To find Top Talkers IP Addresses, we can go to statistics menu then click on IPv4 statistics then click on all Addresses. (First Screenshot)
To find how many Unique IP Addresses we have, we can go to statistics menu then click on Endpoints.(Second screenshot)

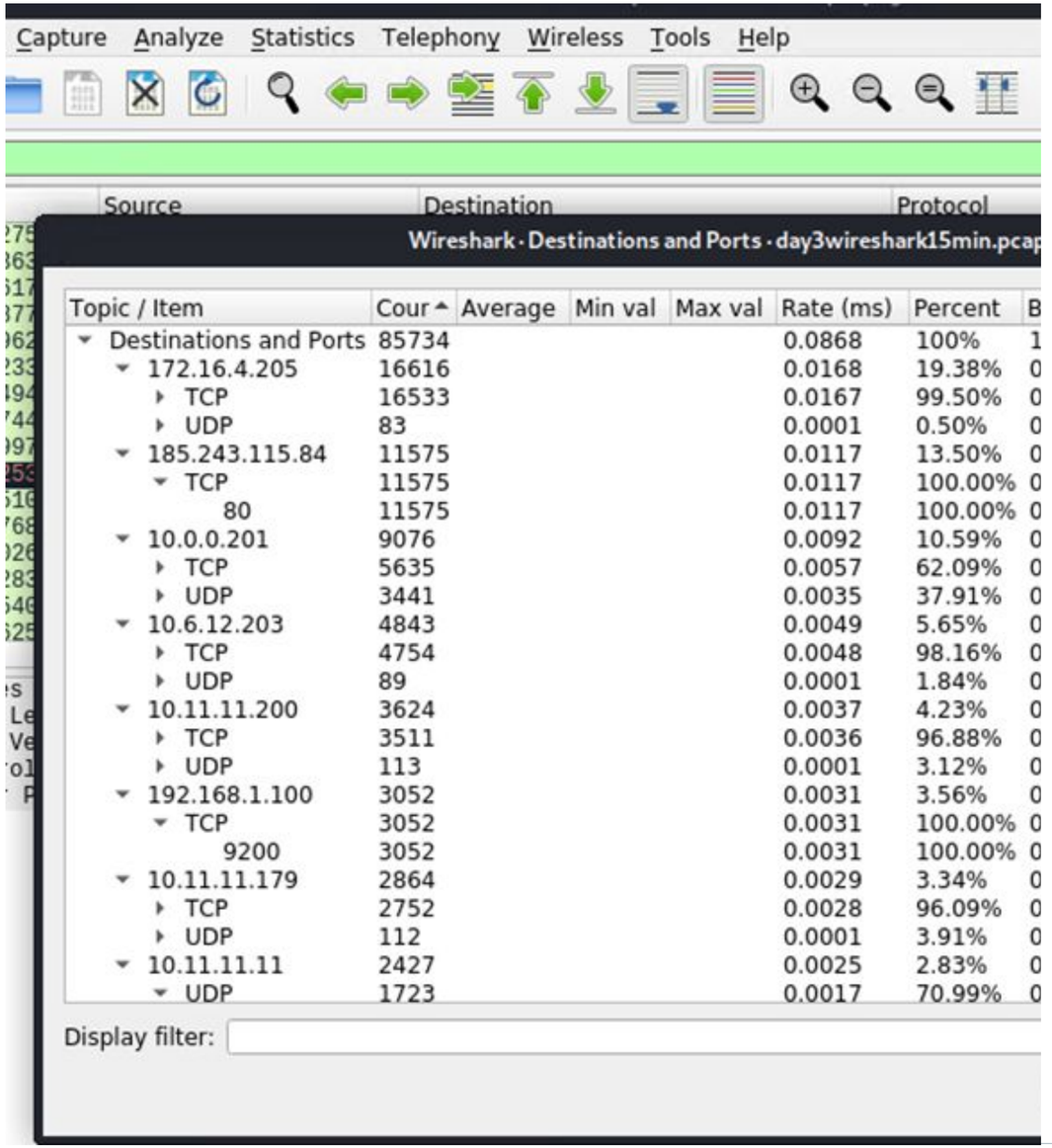




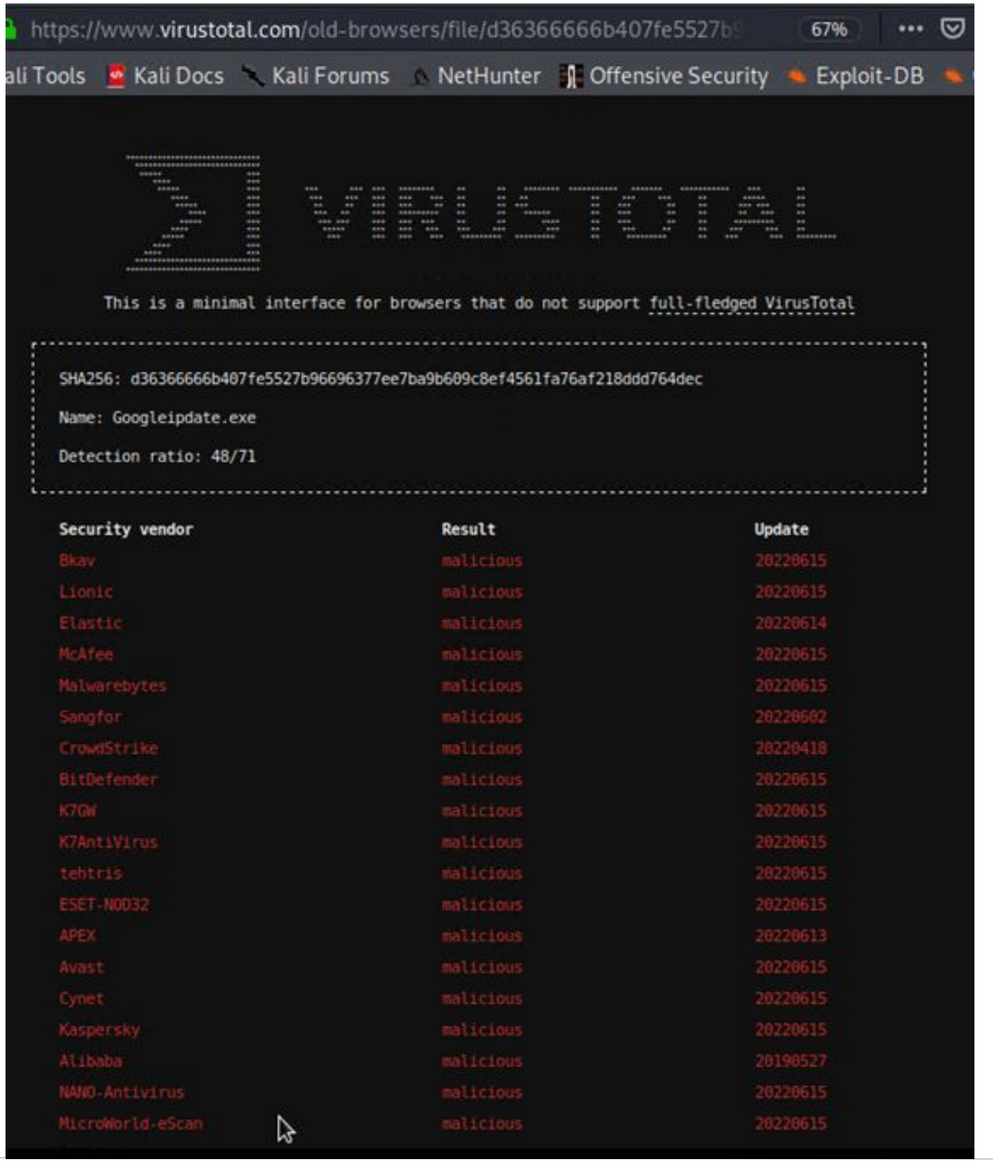
To find Most Common Protocols, we can go to statistics menu then open IPv4 then click on Destinations and Ports.(first screenshot).
Upload the file on virustotal.com most of the security vendors such as Mcafee, AVG etc. are distinguished as malicious. (second Screenshot)

TCP: The Transmission Control Protocol is one of the main protocols of the Internet protocol suite.

UDP: User Datagram Protocol (UDP) refers to a protocol used for communication throughout the internet.



Topic / Item	Cour	Average	Min val	Max val	Rate (ms)	Percent	B
Destinations and Ports	85734				0.0868	100%	1
172.16.4.205	16616				0.0168	19.38%	0
TCP	16533				0.0167	99.50%	0
UDP	83				0.0001	0.50%	0
185.243.115.84	11575				0.0117	13.50%	0
TCP	11575				0.0117	100.00%	0
80	11575				0.0117	100.00%	0
10.0.0.201	9076				0.0092	10.59%	0
TCP	5635				0.0057	62.09%	0
UDP	3441				0.0035	37.91%	0
10.6.12.203	4843				0.0049	5.65%	0
TCP	4754				0.0048	98.16%	0
UDP	89				0.0001	1.84%	0
10.11.11.200	3624				0.0037	4.23%	0
TCP	3511				0.0036	96.88%	0
UDP	113				0.0001	3.12%	0
192.168.1.100	3052				0.0031	3.56%	0
TCP	3052				0.0031	100.00%	0
9200	3052				0.0031	100.00%	0
10.11.11.179	2864				0.0029	3.34%	0
TCP	2752				0.0028	96.09%	0
UDP	112				0.0001	3.91%	0
10.11.11.11	2427				0.0025	2.83%	0
UDP	1723				0.0017	70.99%	0



Security vendor	Result	Update
Bkav	malicious	20220615
Lionic	malicious	20220615
Elastic	malicious	20220614
McAfee	malicious	20220615
Malwarebytes	malicious	20220615
Sangfor	malicious	20220602
CrowdStrike	malicious	20220418
BitDefender	malicious	20220615
K7GW	malicious	20220615
K7AntiVirus	malicious	20220615
tehtris	malicious	20220615
ESET-NOD32	malicious	20220615
APEX	malicious	20220613
Avast	malicious	20220615
Cynet	malicious	20220615
Kaspersky	malicious	20220615
Alibaba	malicious	20190527
NANO-Antivirus	malicious	20220615
MicroWorld-eScan	malicious	20220615

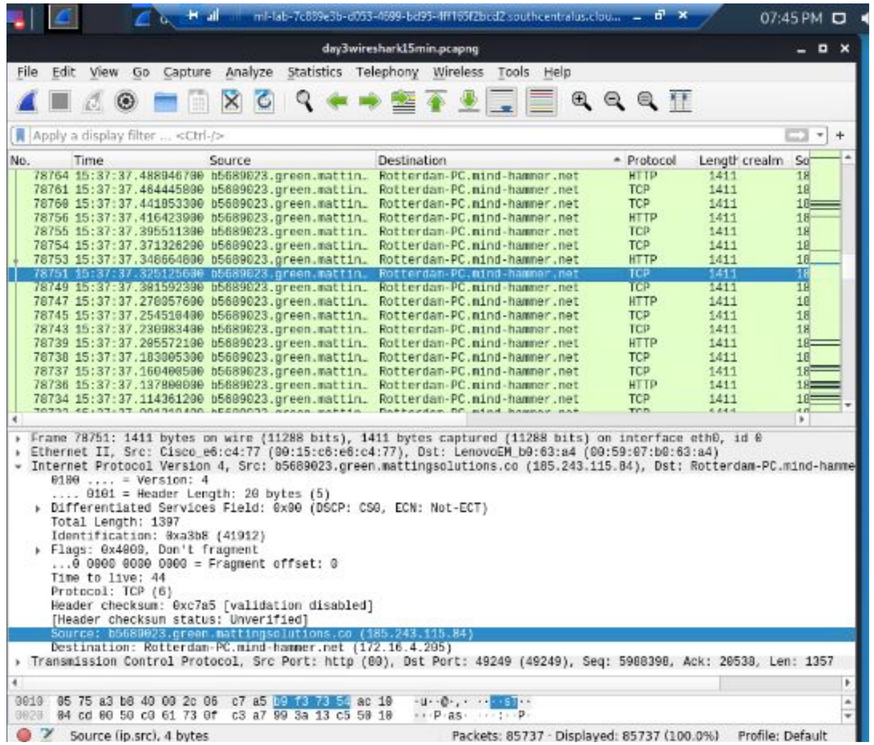
Behavioral Analysis

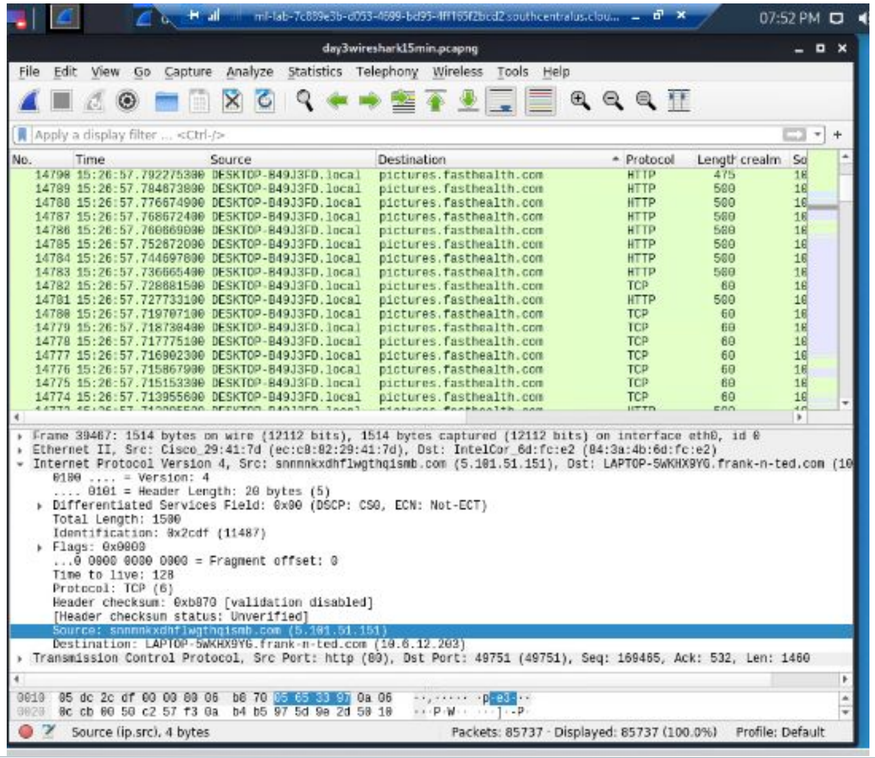
Purpose of Traffic on the Network

Users has two kinds of activity:

“Normal” Activity

- Normal use of the websites like, rotterdam-pc.mind-hammer.net, pictures.fasthealth.com

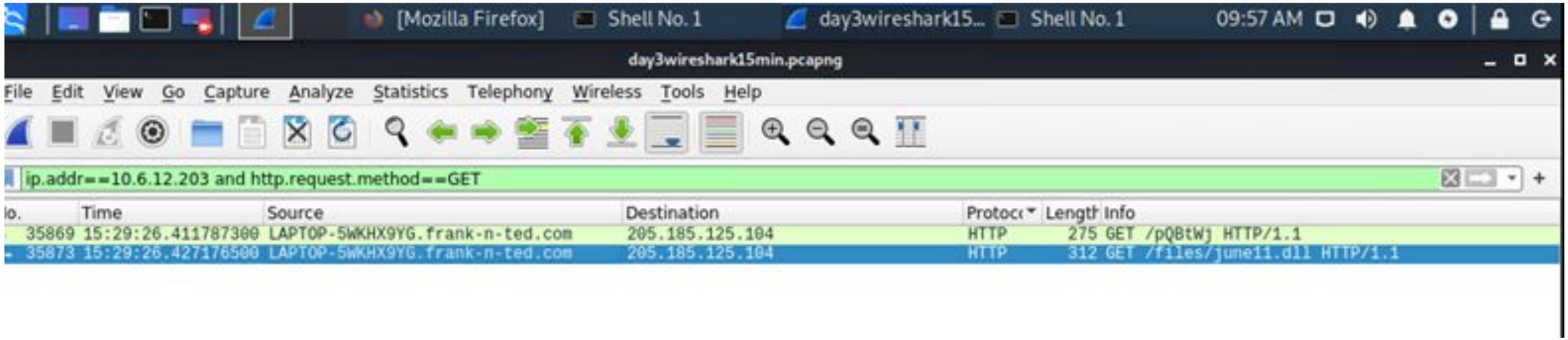




Suspicious Activity

users opened the below link to download:

LAPTOP-5WKHX9YG.frank-n-ted.com used to download : http://205.185.125.104/files/june11.dll

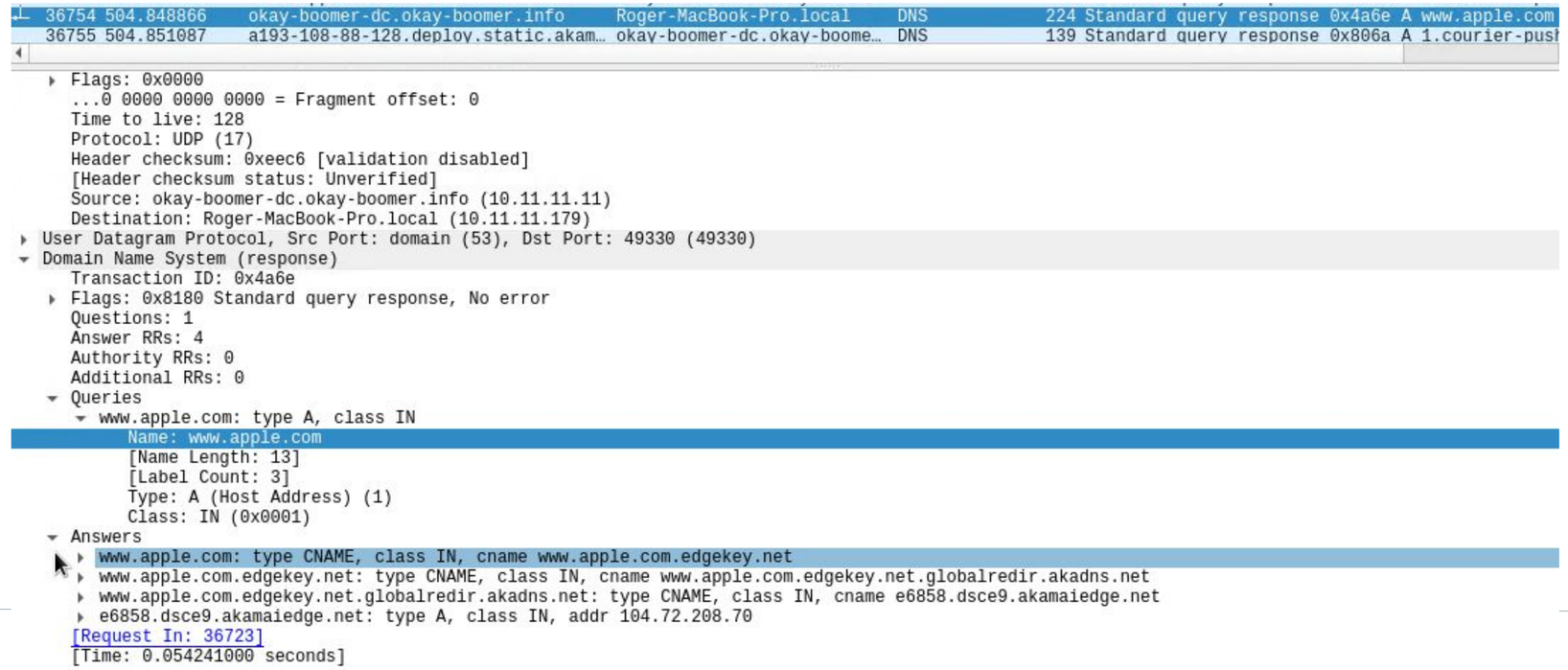


Normal Activity

Browsing Apple.com

Summarize the following:

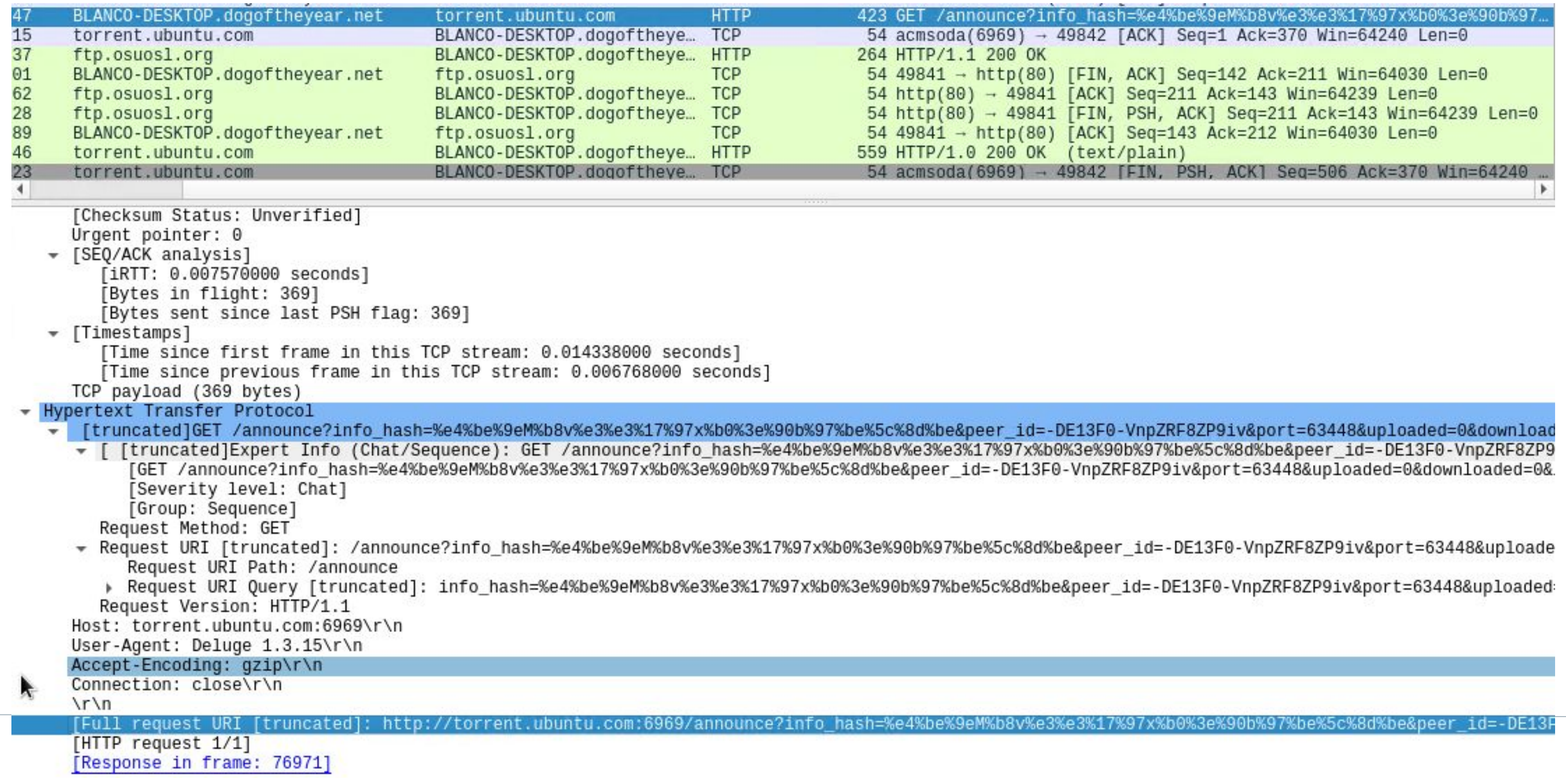
- What kind of traffic did you observe? Which protocol(s)?
  - Standard Query Response using the DNS protocol.
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - They were browsing Apple.com
- Include screenshots of packets justifying your conclusions.



Ubuntu? I hardly know you!

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - Download a file. Using the GET method of the HTTP protocol
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - They are downloading a torrent of the OS Ubuntu from the website torrent.ubuntu.com



Malicious Activity

ITube? No, YouTube!

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?

  LDAP

- What, specifically, was the user doing?

  Connecting to an AD (Active Directory) to steal time from the company by watching YouTube and browsing the web. This careless behaviour led to the downloading of malware (june11.dll).

- Include a description of any interesting findings:

  Screenshots of websites browsed by the users and the discovery of the june11.dll.

Final Lab - ml-lab-7c889e3b-d053-4699-bd95-4ff165f2bcd2.southcentralus.cloudapp.azure.com:54177 - Remote Desktop Connection

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

[Shell No. 1] Day2WSsniff.pcapng 09:37

Day2WSsniff.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.6.12.0/24

No.	Time	Source	Destination	Protoc	Length	Info
53156	15:30:39.974170700	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	129	SASL GSS-API Integ
53189	15:30:40.128644900	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	541	bindRequest(4) "<R
53191	15:30:40.133718500	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	LDAP	264	bindResponse(4) su
53192	15:30:40.135279000	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	97	SASL GSS-API Integ
53223	15:30:40.256061400	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	404	searchRequest(1) "
53225	15:30:40.302504300	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	LDAP	1386	searchResEntry(1) "
53228	15:30:40.336025700	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	529	bindRequest(3) "<R
53230	15:30:40.341094300	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	LDAP	264	bindResponse(3) su
53244	15:30:40.409303000	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	219	SASL GSS-API Integ
53245	15:30:40.417882000	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	LDAP	536	SASL GSS-API Integ
53250	15:30:40.453572400	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	529	bindRequest(7) "<R
53252	15:30:40.458632200	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	LDAP	264	bindResponse(7) su
53260	15:30:40.462383400	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	230	SASL GSS-API Integ

```
▸ Flags: 0x4000, Don't fragment
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x2953 [validation disabled]
  [Header checksum status: Unverified]
  Source: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
  Destination: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
▾ Transmission Control Protocol, Src Port: 49693 (49693), Dst Port: ldap (389), Seq: 1, Ack: 1, Len: 350
  Source Port: 49693 (49693)
  Destination Port: ldap (389)
  [Stream index: 611]
  [TCP Segment Len: 350]
  Sequence number: 1    (relative sequence number)
  Sequence number (raw): 3986943879
  [Next sequence number: 351    (relative sequence number)]
0020  0c 0c c2 1d 01 85 ed a3  ef 87 19 6c 8a e6 50 18   ······· ··· ··l··P·
0030  20 14 18 8e 00 00 30 84  00 00 01 58 02 01 01 63   ·····0· ···X···c
0040  84 00 00 01 4f 04 00 0a  01 00 0a 01 00 02 01 00   ····O··· ........
0050  02 01 78 01 01 00 87 0b  6f 62 6a 65 63 74 63 6c   ··x····· objectcl
0060  61 73 73 30 84 00 00 01  2b 04 11 73 75 62 73 63   ass0···· +··subsc
0070  68 65 6d 61 53 75 62 65  6e 74 72 79 04 0d 64 73   hemaSube ntry··ds
0080  53 65 72 76 69 63 65 4e  61 6d 65 04 0e 6e 61 6d   ServiceN ame··nam
0090  69 6e 67 43 6f 6e 74 65  78 74 73 04 14 64 65 66   ingConte xts··def
00a0  61 75 6c 74 4e 61 6d 69  6e 67 43 6f 6e 74 65 78   aultNami ngContex
00b0  74 04 13 73 63 68 65 6d  61 4e 61 6d 69 6e 67 43   t··schem aNamingC
00c0  6f 6e 74 65 78 74 04 1a  63 6f 6e 66 69 67 75 72   ontext·· configur
00d0  61 74 69 6f 6e 4e 61 6d  69 6e 67 43 6f 6e 74 65   ationNam ingConte
00e0  78 74 04 17 72 6f 6f 74  44 6f 6d 61 69 6e 4e 61   xt··root DomainNa
00f0  6d 69 6e 67 43 6f 6e 74  65 78 74 04 10 73 75 70   mingCont ext··sup
0100  70 6f 72 74 65 64 43 6f  6e 74 72 6f 6c 04 14 73   portedCo ntrol··s
0110  75 70 70 6f 72 74 65 64  4c 44 41 50 56 65 72 73   upported LDAPVers
0120  69 6f 6e 04 15 73 75 70  70 6f 72 74 65 64 4c 44   ion··sup portedLD
```

This shows the raw value of the sequence number (tcp.seq_raw), 4 bytes Packets: 92816 · Displayed: 996

Status: Running

Dashboa | Post Atte | My virtua | unit_24/ | Network | LDAP vs.

n-able.com/blog/difference-between-ldap-ad#:~:text=What%20Is%20the%20Role%20of,and%2...

Bootcamp | Coding Resources | Cybersecurity Reso... | Games | IT Resources | Occult Resources | Shopping | Skills

N-ABLE EN

What Howes ultimately produced was an open and cross-platform application protocol used over an IP network to manage and access directory information. This protocol allows users to access the kind of important, internal information that might be stored in an AD. Unlike a phone book, this information is not limited to name, address, and phone number alone. It often includes email address, title, department, length of time with the company, and much more. LDAP also enables permission for users to access resources like printers that share the same network.

What Is the Role of LDAP in Active Directory?

LDAP is the core protocol behind AD. Directory access is performed via LDAP—whenever a client performs a search for a specific object in AD (say for a user or a printer), LDAP is being utilized to query relevant objects and return the correct results.

Users obtain access to information and resources through a process of LDAP authentication, which usually involves multiple levels of permission. Anonymous users have the least access to information—if they have access at all—because there is no information that identifies these users and allows them to be authenticated. They might, for instance, see only employee names without access to contact information.

A majority of users—typically company employees—are granted access to the kind of information that may be especially relevant or useful to them on a day-to-day basis. Administrators essentially function as the LDAP administrators, and have access to the greatest amount of information. They can also add or remove data from the server as needed. In addition to these conventional roles, it's also possible to create subadminster or manager roles with some of the privileges of an administrator, which can be helpful to IT teams in large companies and organizations in particular.

LDAP and Data Breaches

Due to the importance of AD to the makeup of the IT structure of most companies and organizations, it tends to be a prized target for hackers and other malicious actors. By accessing a single user account, these actors can put sensitive data such as passwords and files at risk. If that account belongs to an administrator, the level of vulnerability is potentially even greater. In the worst-case scenario, the integrity of the entire IT infrastructure could be in jeopardy if AD accounts are compromised.

This is where LDAP becomes especially important. Through its authentic defense against malicious attacks on an AD. But how does this authenticatic of

LDAP offers two main methods of authentication to keep your data safe. The first, called simple

Hey there Welcome to N-able! What led you to stop by today?

Talking: Arick Johnson

You are screen sharing Stop Share

Type here to search 90°F Sunny 10:37 AM 6/11/2022

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
56504	15:31:02.699107200	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	586		http(80) → 49739 [PSH, AC
56505	15:31:02.723287800	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	1514		http(80) → 49739 [ACK] Se
56506	15:31:02.740077400	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	1050		http(80) → 49739 [PSH, AC
56507	15:31:02.740923100	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	TCP	54		49739 → http(80) [ACK] Se
56508	15:31:02.741782800	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	TCP	54		49739 → http(80) [ACK] Se
56509	15:31:02.756927200	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	946		HTTP/1.1 200 OK
56510	15:31:02.757821500	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	TCP	54		49739 → http(80) [ACK] Se
56511	15:31:02.758666500	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	55		[TCP Keep-Alive] 49680 →
56512	15:31:02.759714600	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	66		[TCP Keep-Alive ACK] micr
56513	15:31:02.760575700	DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolcus00.cloudapp.net	TCP	54		49709 → https(443) [FIN,
56514	15:31:02.761444200	skypedataprdcolcus00.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	54		https(443) → 49709 [ACK]
56515	15:31:02.762361000	skypedataprdcolcus00.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	54		https(443) → 49709 [FIN,
56516	15:31:02.763175100	DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolcus00.cloudapp.net	TCP	54		49709 → https(443) [ACK]

```
Frame 56509: 946 bytes on wire (7568 bits), 946 bytes captured (7568 bits) on interface eth0, id 0
Ethernet II, Src: Cisco_29:41:7d (ec:c8:82:29:41:7d), Dst: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
Internet Protocol Version 4, Src: 205.185.125.104 (205.185.125.104), Dst: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49739 (49739), Seq: 562913, Ack: 480, Len: 892
[456 Reassembled TCP Segments (563316 bytes): #55751(1460), #55752(996), #55753(1460), #55754(996), #55755(1228), #55757(1460), #55758(996), #55760(1460), #
Hypertext Transfer Protocol
Data (563032 bytes)
```

Wireshark · Packet 56509 · Day2WSsniff.pcapng

```
Frame 56509: 946 bytes on wire (7568 bits), 946 bytes captured (7568 bits) on interface eth0, id 0
Ethernet II, Src: Cisco_29:41:7d (ec:c8:82:29:41:7d), Dst: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
Internet Protocol Version 4, Src: 205.185.125.104 (205.185.125.104), Dst: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49739 (49739), Seq: 562913, Ack: 480, Len: 892
[456 Reassembled TCP Segments (563316 bytes): #55751(1460), #55752(996), #55753(1460), #55754(996), #55755(1228), #55757(
Hypertext Transfer Protocol
Data (563032 bytes)
```

```
0000  84 3a 4b 6d fc e2
0010  03 a4 25 fa 00 00
0020  0c cb 00 50 c2 4b
0030  fa f0 b1 e6 00 00
0040  bb 39 cc e6 1d da
0050  d9 fa fb ff 8b 0d
0060  a1 82 03 4b 30 82
```

Frame (946 bytes) | Rea

No.: 56509 · Time: 15:31:02.75692

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
56509	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: june11.dll

Save | Save All | Close | Help

Too pooped to boop

- What kind of traffic did you observe? Which protocol(s)?

  HTTP

- What, specifically, was the user doing?

  Downloading a Betty Boop avi movie torrent file from publicdomaintorrents.com

- Include a description of any interesting files:

  Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

Day2WSsniff.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
67039	15:32:40.397411000	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	465		GET /divxi.jpg HTTP/1.1
67192	15:32:41.418497100	BLANCO-DESKTOP.dogoftheyear.net	www.assoc-amazon.com	HTTP	415		GET /s/ads.js HTTP/1.1
67241	15:32:42.144952200	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	531		GET /usercomments.html?mo
67329	15:32:43.184691500	BLANCO-DESKTOP.dogoftheyear.net	www.assoc-amazon.com	HTTP	427		GET /s/ads-common.js HTTP
67365	15:32:43.478960800	BLANCO-DESKTOP.dogoftheyear.net	rcm-na.assoc-amazon.com	HTTP	885		GET /e/cm?t=publicdomai0f
67437	15:32:44.119973600	BLANCO-DESKTOP.dogoftheyear.net	fls-na.amazon-adsystem.com	HTTP	1067		GET /1/associates-ads/1/O
67611	15:32:44.927002100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	589		GET /bt/btdownload.php?ty
67655	15:32:45.122748900	BLANCO-DESKTOP.dogoftheyear.net	ftp.osuosl.org	HTTP	195		GET /version-1.0 HTTP/1.1
67659	15:32:45.132146700	BLANCO-DESKTOP.dogoftheyear.net	torrent.ubuntu.com	HTTP	423		GET /announce?info_hash=%
67895	15:32:45.790638000	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	434		GET /bt/announce.php?info
67925	15:32:45.867480400	BLANCO-DESKTOP.dogoftheyear.net	moonstar.publicdomaintorrents.com	HTTP	434		GET /announce?info_hash=%
68019	15:32:46.152011100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	253		GET /bt/scrape.php?info_h
68039	15:32:46.197046600	BLANCO-DESKTOP.dogoftheyear.net	moonstar.publicdomaintorrents.com	HTTP	253		GET /scrape?info_hash=%1d

```
▸ Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (80), Seq: 1, Ack: 1, Len: 535
▾ 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 Version: HTTP/1.1
    Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: www.publicdomaintorrents.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

```
0030  ff ff 31 06 00 00 47 45  54 20 2f 62 74 2f 62 74   ··1···GE T /bt/bt
0040  64 6f 77 6e 6c 6f 61 64  2e 70 68 70 3f 74 79 70   download .php?typ
0050  65 3d 74 6f 72 72 65 6e  74 26 66 69 6c 65 3d 42   e=torren t&file=B
0060  65 74 74 79 5f 42 6f 6f  70 5f 52 68 79 74 68 6d   etty_Boo p_Rhythm
0070  5f 6f 6e 5f 74 68 65 5f  52 65 73 65 72 76 61 74   _on_the_ Reservat
0080  69 6f 6e 2e 61 76 69 2e  74 6f 72 72 65 6e 74 20   ion.avi. torrent
0090  48 54 54 50 2f 31 2e 31  0d 0a 52 65 66 65 72 65   HTTP/1.1 ··Refere
00a0  72 3a 20 68 74 74 70 3a  2f 2f 70 75 62 6c 69 63   r: http: //public
00b0  64 6f 6d 61 69 6e 74 6f  72 72 65 6e 74 73 2e 69   domainto rrents.i
00c0  6e 66 6f 2f 6e 73 68 6f  77 6d 6f 76 69 65 2e 68   nfo/nsho wmovie.h
00d0  74 6d 6c 3f 6d 6f 76 69  65 69 64 3d 35 31 33 0d   tml?movi eid=513·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00f0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0100  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0110  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0120  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0130  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
```

HTTP Request-URI (http.request.uri), 85 bytes Packets: 92816 · Displayed: 46 (0.0%) Profile: Default

Status: Running

That's all folks!

Sources:

Malicious Chihuahua:
https://www.reddit.com/r/hmmm/comments/g72uwz/hmmm/

Betty Boop GIF:
https://imgur.com/t/betty_boop/eSDqkYs