Final Engagement

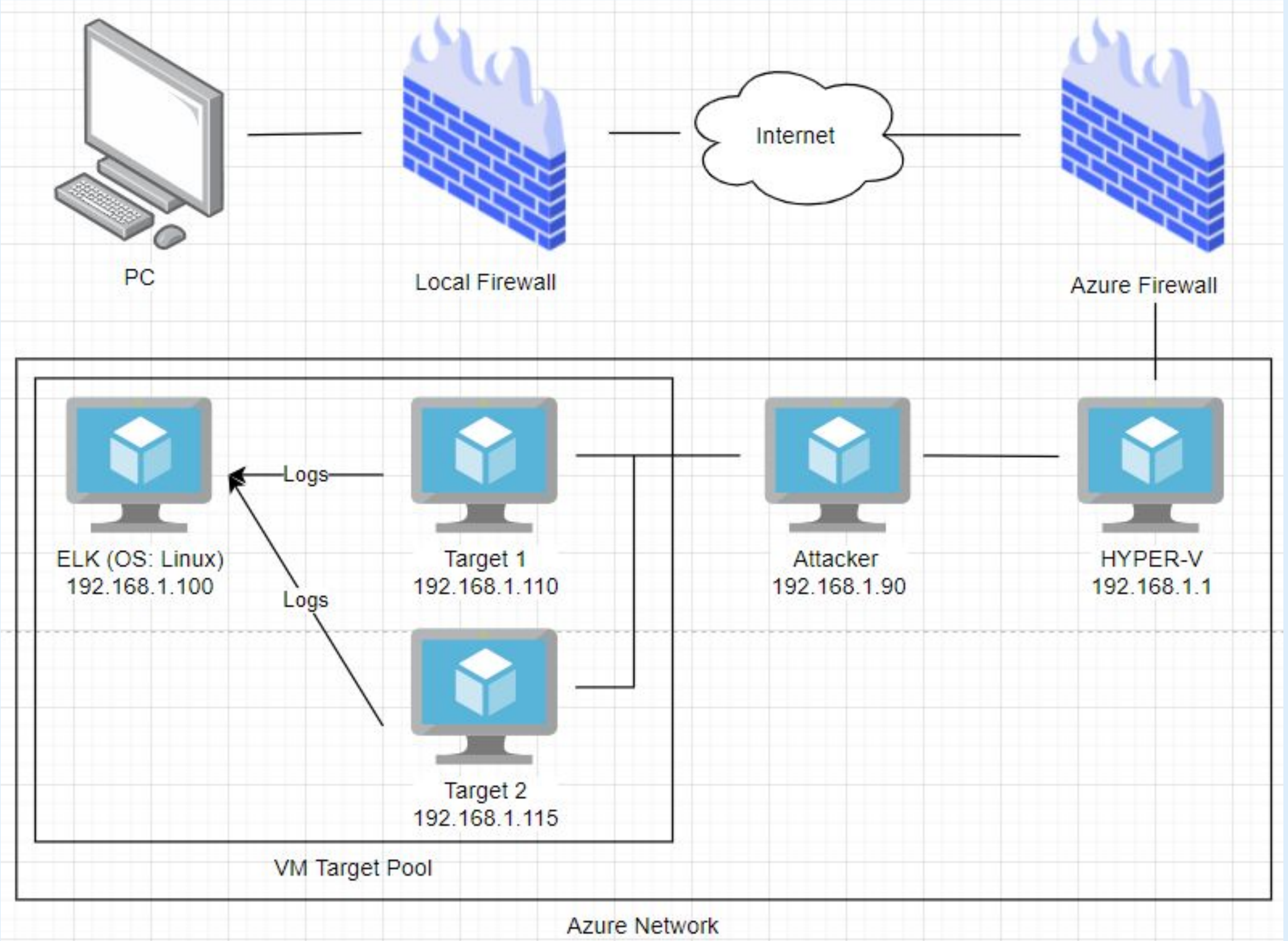
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
22/TCP SSH	CVE-2018-6082 CVSS= **4.3**	System is vulnerable to brute force and dictionary attacks.
80/TCP HTTP	CVE-2019-6579 CVSS= **9.8**	An attacker can execute system commands with administrative privileges.
111/TCP rpcbind	CVE-2017-8779 CVSS= **7.8**	Vulnerability disrupts memory allocation which can allow a remote attacker to cause a denial of service, aka. rpcbomb.
139/TCP netbios-sn	CVE-2017-0143 NIST= **8.1**	Windows remote code execution vulnerability. Allows a remote attacker to execute code.

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
445/TCP microsoft-ds	CVE-2020-0796 NIST= **10.0**	An attacker who successfully exploits the SMBv3 protocol can gain access to a system to execute code.
Simple passwords	Lack of complexity in passwords. No 2-Factor Authentication at login.	Simple passwords like first and last names can be easily guessed or cracked using a tool like john by a hacker. In addition, 2-Factor Authentication was missing at login for the user's Michael and Steven.
Root accessibility	Sudoer privileges for non-administrative users.	Steven had sudoer privileges that allows an attacker to gain root access by exploiting the binary program python.

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 10.0.0.201 166.62.111.64 185.243.115.84	Machines that sent the most traffic.
Most Common Protocols	TLS DNS HTTP	Three most common protocols on the network.
# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	10.0.0.0/24, 10.6.12.0/24, 10.11.11.0/24, 172.16.4.0/24 172.217.0.0/16, 192.168.1.0/24	Observed subnet ranges.
# of Malware Species	1, june11.dll was discovered as a trojan.	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

- Hobbie Research
- Youtube

Suspicious Activity

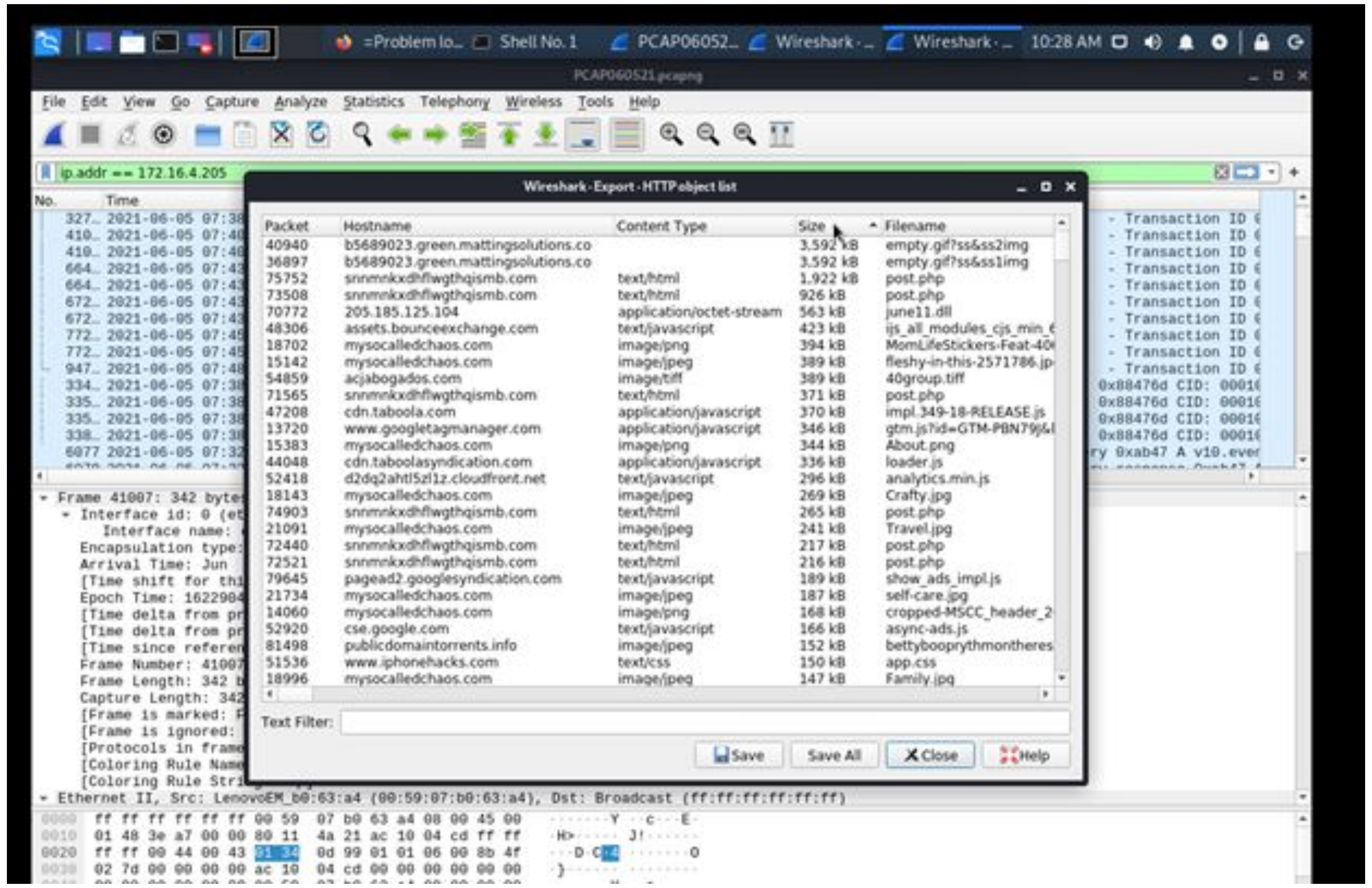
- Illegal Downloads and Torrents
- Custom Domain Installation

Normal Activity

General Usage

Summarize the following:

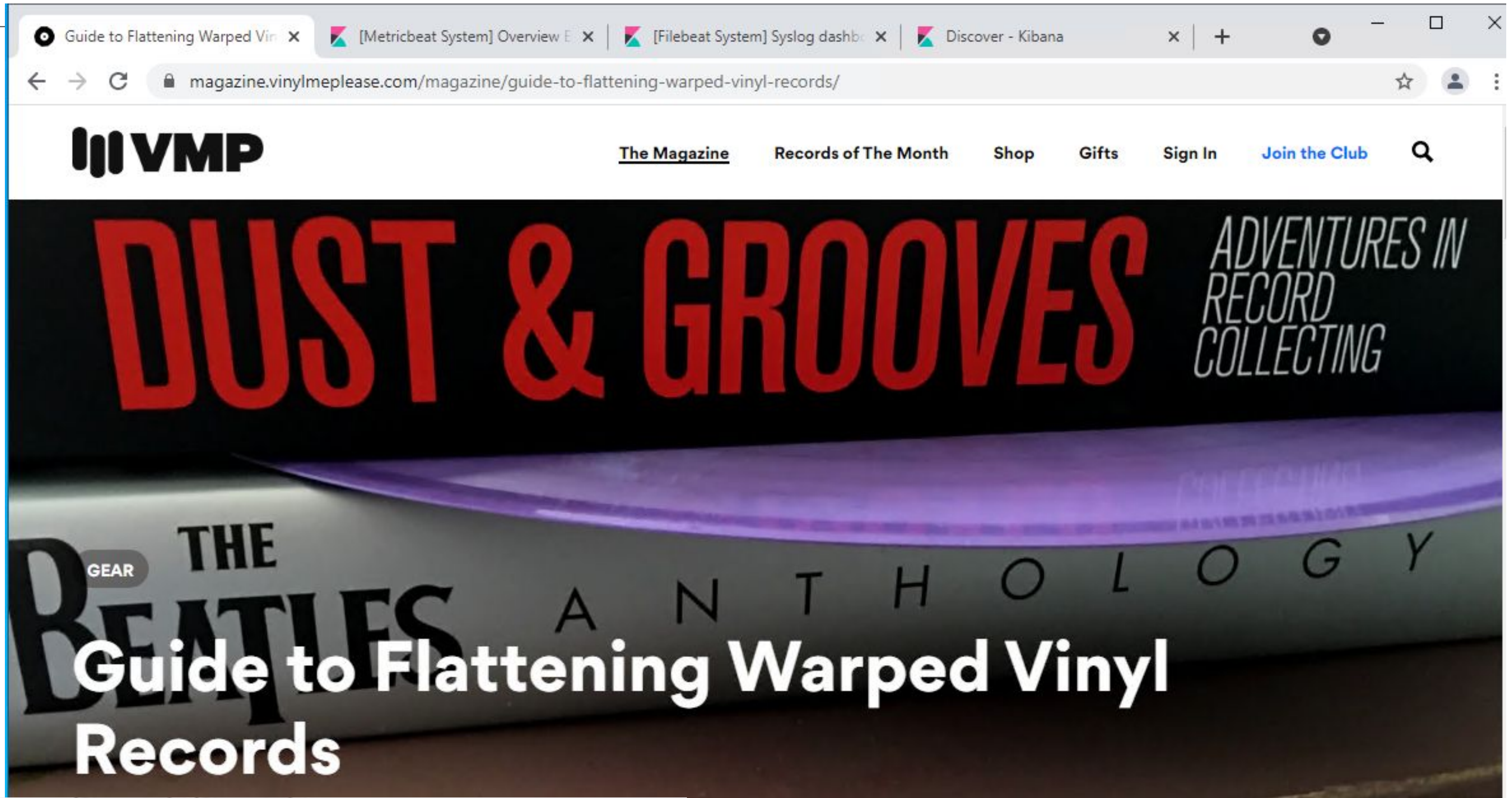
- What kind of traffic did you observe? Which protocol(s)? HTTP
- What, specifically, was the user doing? Which site were they browsing? Etc.
    - Viewing images, reading text documents, accessing websites such as mysocalledchaos.com
- Include screenshots of packets justifying your conclusions.



Packet	Hostname	Content Type	Size	Filename
40940	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2img
36897	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
75752	snnmnkxdhflwgthqismb.com	text/html	1,922 kB	post.php
73508	snnmnkxdhflwgthqismb.com	text/html	926 kB	post.php
70772	205.185.125.104	application/octet-stream	563 kB	june11.dll
48306	assets.bounceexchange.com	text/javascript	423 kB	ijs_all_modules_cjs_min_
18702	mysocalledchaos.com	image/png	394 kB	MomLifeStickers-Feat-40
15142	mysocalledchaos.com	image/jpeg	389 kB	fleshy-in-this-2571786.jp
54859	acjabogados.com	image/tiff	389 kB	40group.tiff
71565	snnmnkxdhflwgthqismb.com	text/html	371 kB	post.php
47208	cdn.taboola.com	application/javascript	370 kB	impl.349-18-RELEASE.js
13720	www.googletagmanager.com	application/javascript	346 kB	gtm.js?id=GTM-PBN79J&
15383	mysocalledchaos.com	image/png	344 kB	About.png
44048	cdn.taboolasyndication.com	application/javascript	336 kB	loader.js
52418	d2dq2ahtl5zl1z.cloudfront.net	text/javascript	296 kB	analytics.min.js
18143	mysocalledchaos.com	image/jpeg	269 kB	Crafty.jpg
74903	snnmnkxdhflwgthqismb.com	text/html	265 kB	post.php
21091	mysocalledchaos.com	image/jpeg	241 kB	Travel.jpg
72440	snnmnkxdhflwgthqismb.com	text/html	217 kB	post.php
72521	snnmnkxdhflwgthqismb.com	text/html	216 kB	post.php
79645	pagead2.googlesyndication.com	text/javascript	189 kB	show_ads_impl.js
21734	mysocalledchaos.com	image/jpeg	187 kB	self-care.jpg
14060	mysocalledchaos.com	image/png	168 kB	cropped-MSCC_header_2
52920	cse.google.com	text/javascript	166 kB	async-ads.js
81498	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmontheres
51536	www.iphonehacks.com	text/css	150 kB	app.css
18996	mysocalledchaos.com	image/jpeg	147 kB	Family.jpg

Web Browsing - Users indulging hobbies

- User viewed instructions on flattening warped records from www.vinylmeplease.com

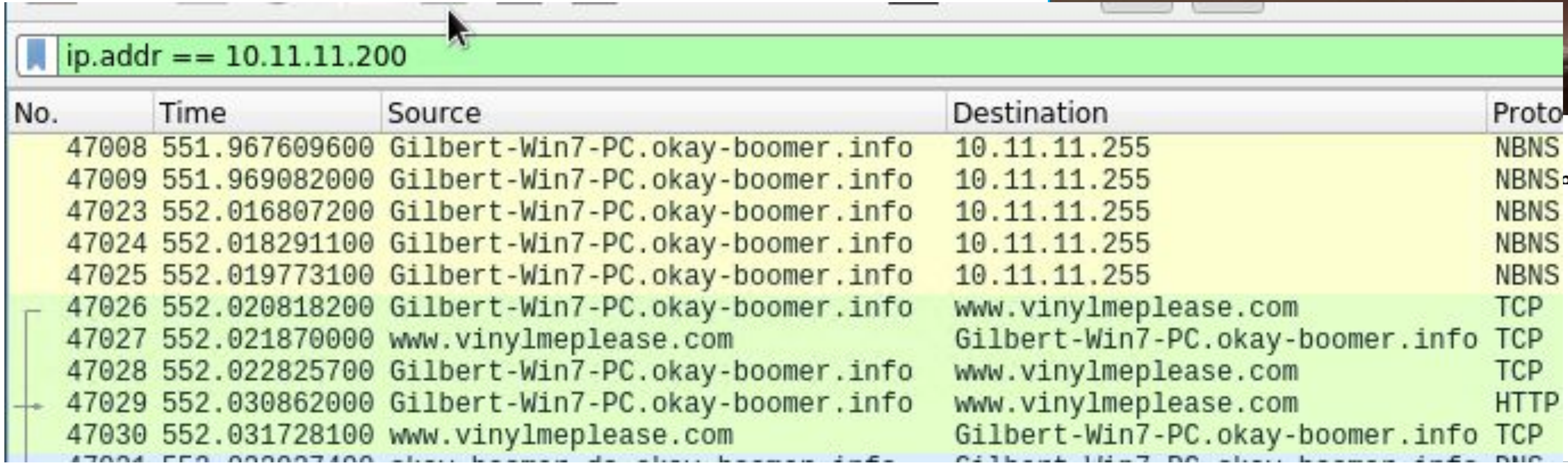


Guide to Flattening Warped Vi × | [Metricbeat System] Overview × | [Filebeat System] Syslog dashb × | Discover - Kibana ×

magazine.vinylmeplease.com/magazine/guide-to-flattening-warped-vinyl-records/

Guide to Flattening Warped Vinyl Records

...orized records. there



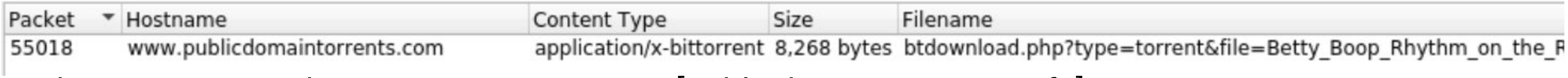
```
ip.addr == 10.11.11.200

No.    Time          Source                           Destination                       Proto
 47008 551.967609600 Gilbert-Win7-PC.okay-boomer.info 10.11.11.255                      NBNS
 47009 551.969082000 Gilbert-Win7-PC.okay-boomer.info 10.11.11.255                      NBNS
 47023 552.016807200 Gilbert-Win7-PC.okay-boomer.info 10.11.11.255                      NBNS
 47024 552.018291100 Gilbert-Win7-PC.okay-boomer.info 10.11.11.255                      NBNS
 47025 552.019773100 Gilbert-Win7-PC.okay-boomer.info 10.11.11.255                      NBNS
 47026 552.020818200 Gilbert-Win7-PC.okay-boomer.info www.vinylmeplease.com             TCP
 47027 552.021870000 www.vinylmeplease.com            Gilbert-Win7-PC.okay-boomer.info  TCP
 47028 552.022825700 Gilbert-Win7-PC.okay-boomer.info www.vinylmeplease.com             TCP
 47029 552.030862000 Gilbert-Win7-PC.okay-boomer.info www.vinylmeplease.com             HTTP
 47030 552.031728100 www.vinylmeplease.com            Gilbert-Win7-PC.okay-boomer.info  TCP
```

Malicious Activity

Illegal Downloads and Torrents

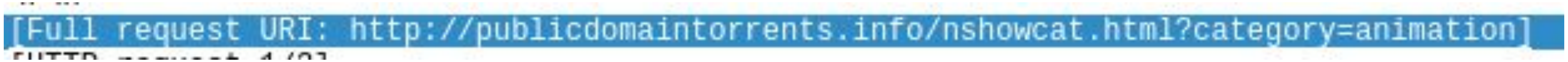
Malicious online activity within the network

- User 10.0.0.201 was detected downloading a torrent file.



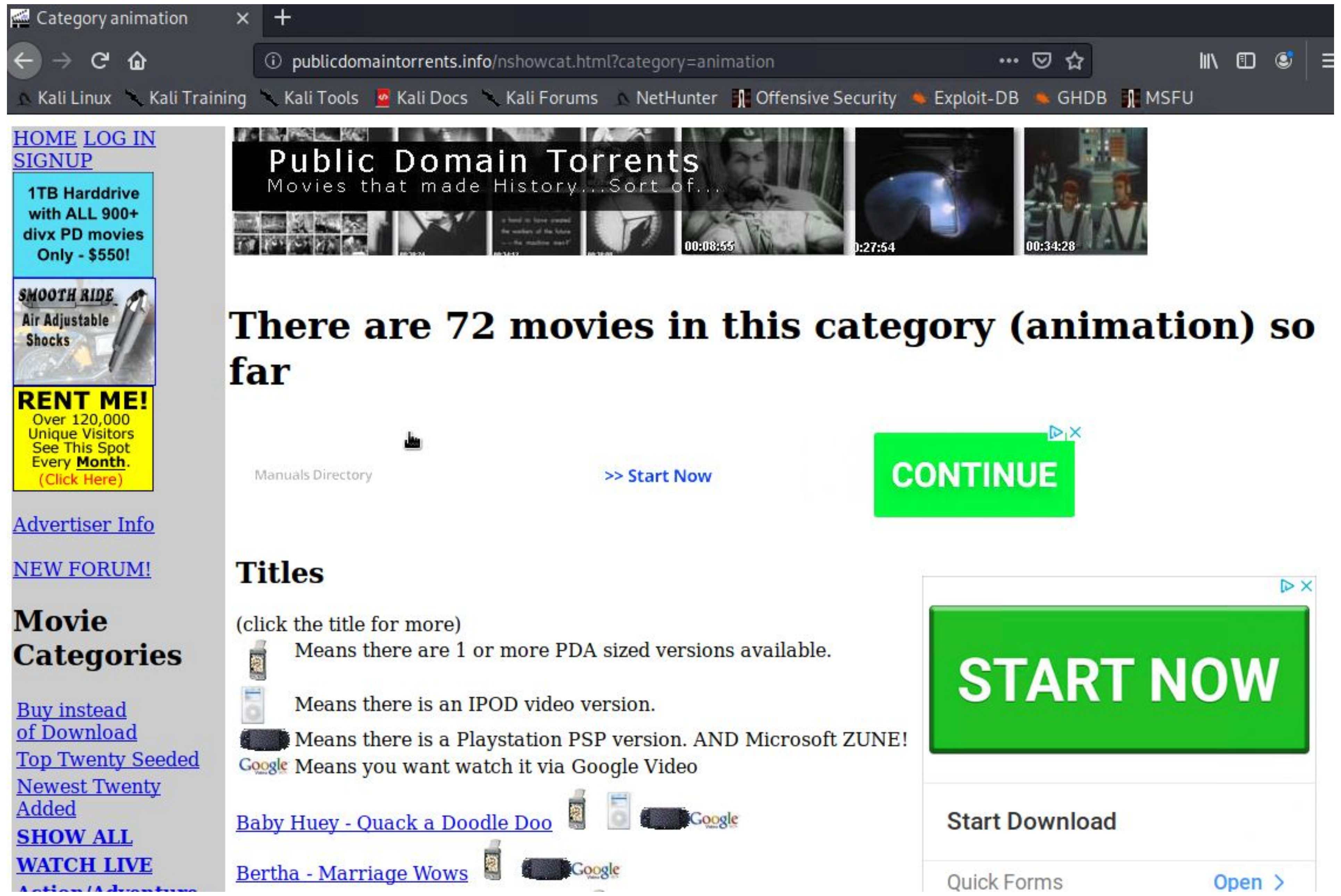
Packet	Hostname	Content Type	Size	Filename
55018	www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_R

- The user executed a HTTP GET request to [publicdomaintorrents.info]



```
[Full request URI: http://publicdomaintorrents.info/nshowcat.html?category=animation]
```

- The user was browsing through a potentially malicious website
- The user was downloading a potentially malicious file
- The website in question on the right



There are 72 movies in this category (animation) so far

Titles

(click the title for more)

Means there are 1 or more PDA sized versions available.

Means there is an IPOD video version.

Means there is a Playstation PSP version. AND Microsoft ZUNE!

Google Means you want watch it via Google Video

Baby Huey - Quack a Doodle Doo

Bertha - Marriage Wows

Movie Categories

Buy instead of Download

Top Twenty Seeded

Newest Twenty Added

SHOW ALL

WATCH LIVE

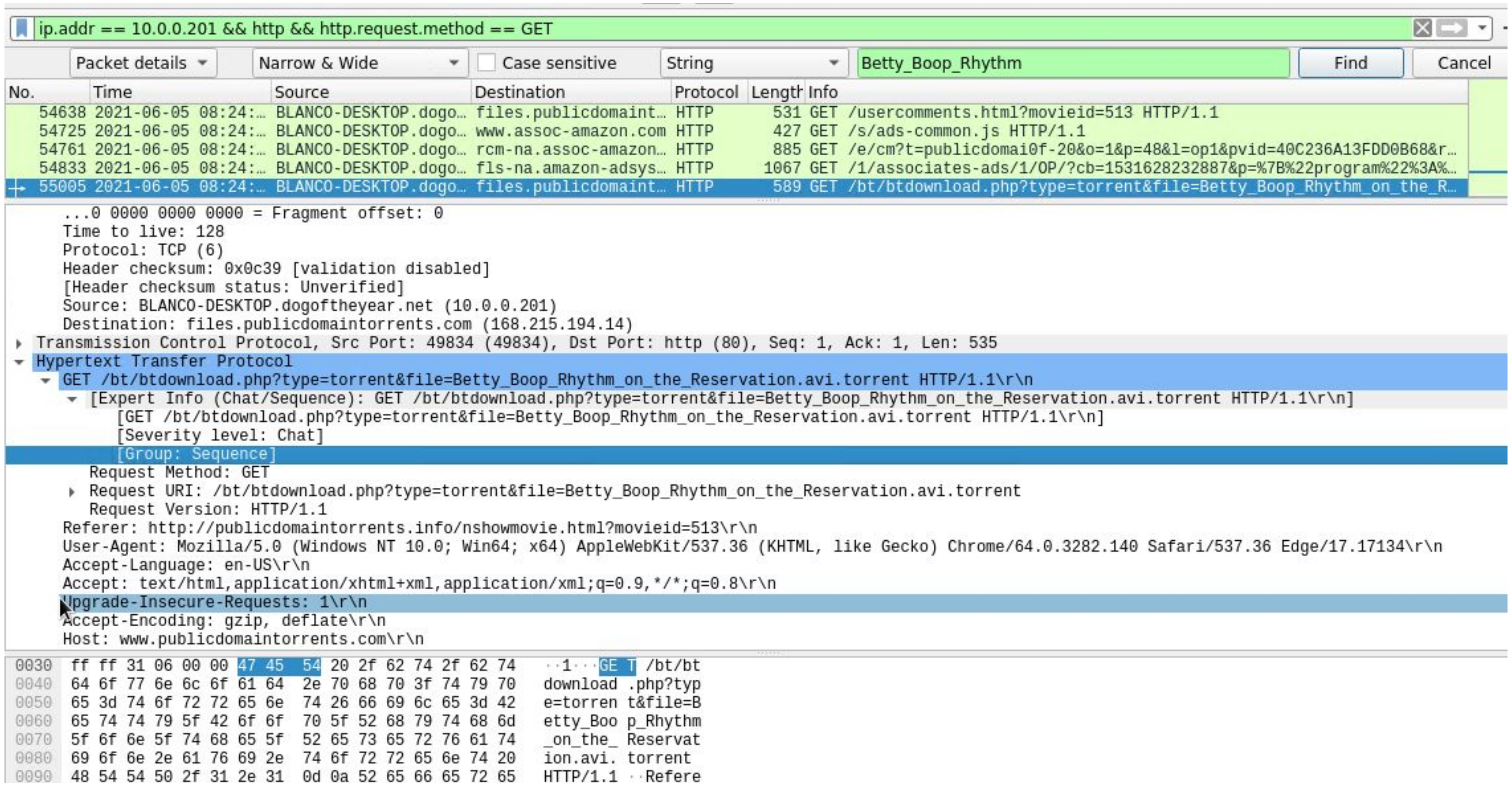
Illegal Downloads and Torrents (Cont.)

Wireshark evidence

The IP address user 10.0.0.201 constantly sent requests to the domain [publicdomaintorrents.info].

In one of the requests, the user downloaded a torrent file which can download a file using the torrent system.

This download was risky since the file could have been a malicious file.



```
ip.addr == 10.0.0.201 && http && http.request.method == GET
```

```
No.    Time                   Source                   Destination               Protocol Length Info
 54638 2021-06-05 08:24:…  BLANCO-DESKTOP.dogo…  files.publicdomaint…   HTTP      531 GET /usercomments.html?movieid=513 HTTP/1.1
 54725 2021-06-05 08:24:…  BLANCO-DESKTOP.dogo…  www.assoc-amazon.com  HTTP      427 GET /s/ads-common.js HTTP/1.1
 54761 2021-06-05 08:24:…  BLANCO-DESKTOP.dogo…  rcm-na.assoc-amazon…  HTTP      885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&r…
 54833 2021-06-05 08:24:…  BLANCO-DESKTOP.dogo…  fls-na.amazon-adsys…  HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%…
 55005 2021-06-05 08:24:…  BLANCO-DESKTOP.dogo…  files.publicdomaint…   HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_R…
```

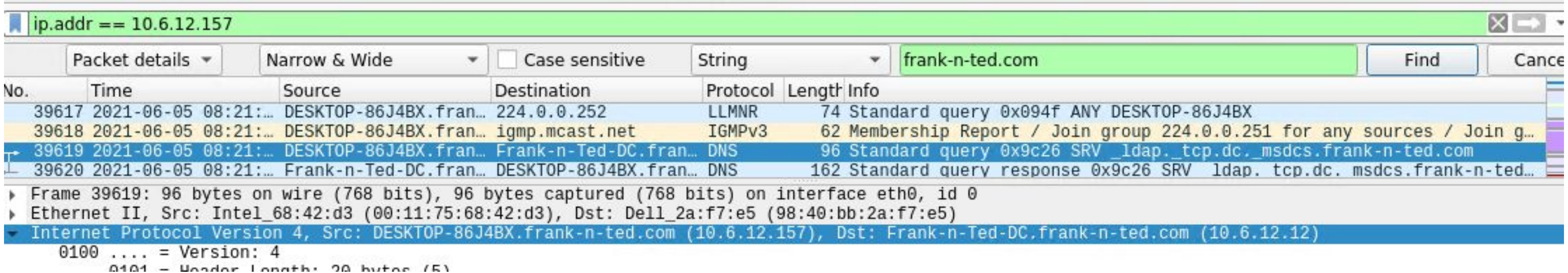
```
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0c39 [validation disabled]
    [Header checksum status: Unverified]
    Source: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
    Destination: files.publicdomaintorrents.com (168.215.194.14)
▸ 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]
        [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      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
```

```
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
```

Custom Domain Installation

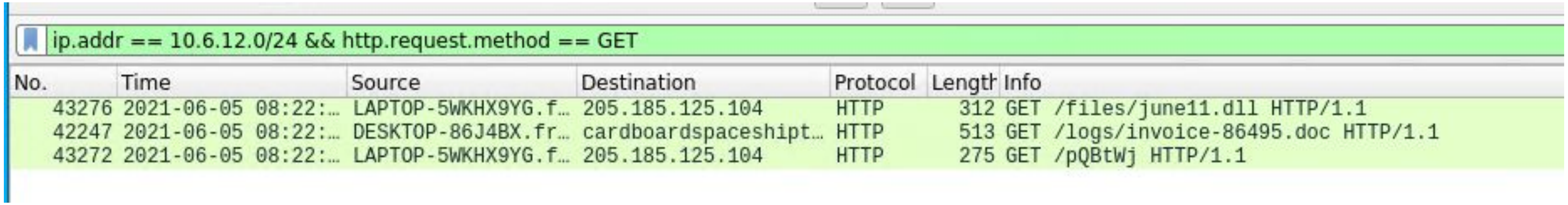
Unknown DNS activities within the network

- While monitoring DNS protocols, an unknown domain [frank-n-ted.com] was detected



```
ip.addr == 10.6.12.157
Packet details    Narrow & Wide    □ Case sensitive    String    frank-n-ted.com    Find    Cance
No.   Time               Source              Destination         Protocol Length Info
39617 2021-06-05 08:21:… DESKTOP-86J4BX.fran… 224.0.0.252        LLMNR     74 Standard query 0x094f ANY DESKTOP-86J4BX
39618 2021-06-05 08:21:… DESKTOP-86J4BX.fran… igmp.mcast.net     IGMPv3    62 Membership Report / Join group 224.0.0.251 for any sources / Join g…
39619 2021-06-05 08:21:… DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… DNS      96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
39620 2021-06-05 08:21:… Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS     162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted…
▸ Frame 39619: 96 bytes on wire (768 bits), 96 bytes captured (768 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)
▾ Internet Protocol Version 4, Src: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
    0100 .... = Version: 4
    0101 .... = Header Length: 20 bytes (5)
```

- The user within the 10.6.12.0/24 network set up an Active Directory (AD) network on 10.6.12.157
- The IP 10.6.12.157 requested HTTP GET requests to an unverified address

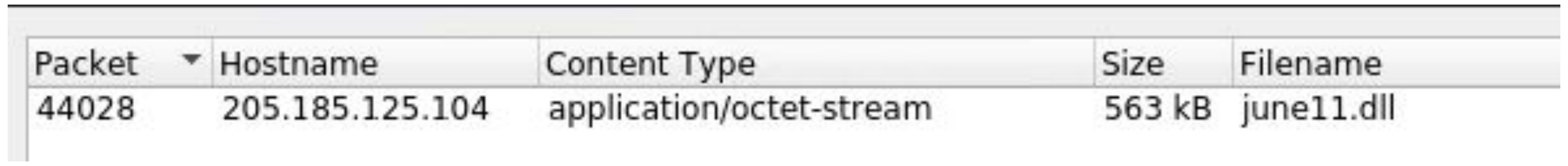


```
ip.addr == 10.6.12.0/24 && http.request.method == GET
No.   Time               Source             Destination          Protocol Length Info
43276 2021-06-05 08:22:… LAPTOP-5WKHX9YG.f… 205.185.125.104      HTTP     312 GET /files/june11.dll HTTP/1.1
42247 2021-06-05 08:22:… DESKTOP-86J4BX.fr… cardboardspaceshipt… HTTP     513 GET /logs/invoice-86495.doc HTTP/1.1
43272 2021-06-05 08:22:… LAPTOP-5WKHX9YG.f… 205.185.125.104      HTTP     275 GET /pQBtWj HTTP/1.1
```

Custom Domain Installation (Cont.)

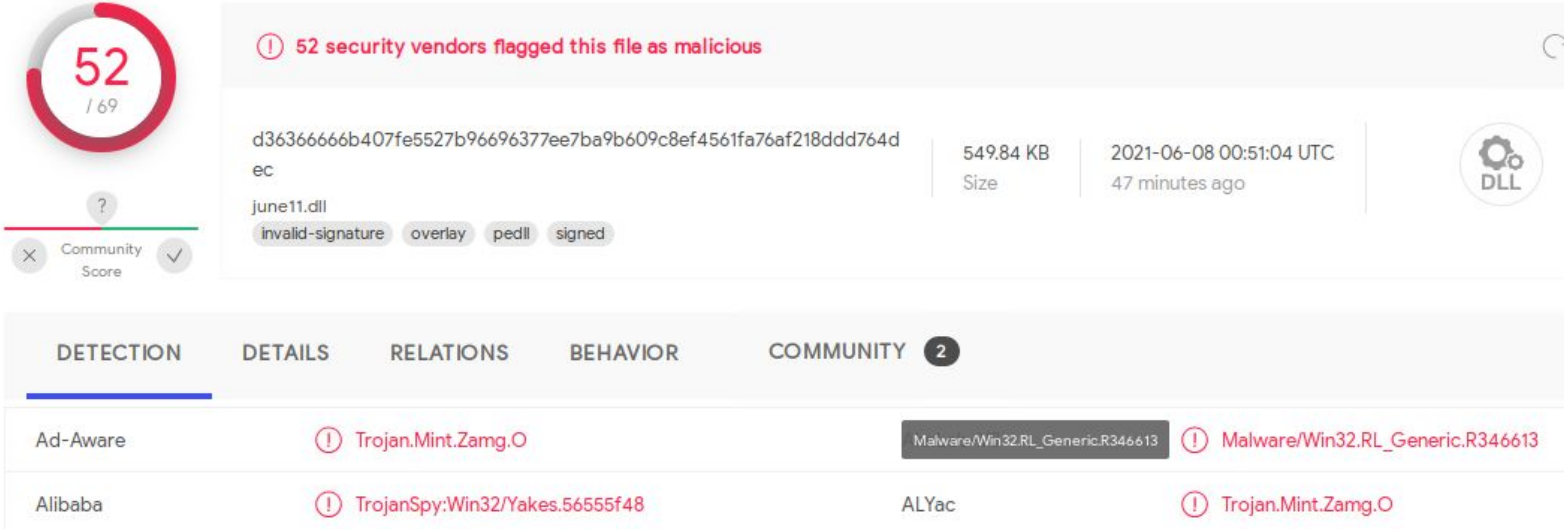
Suspicious Download

- Although the destination website could not be reached, a file named “june11.dll” was downloaded



Packet	Hostname	Content Type	Size	Filename
44028	205.185.125.104	application/octet-stream	563 kB	june11.dll

- After running the file through VirusTotal.com, the downloaded file is most likely a malicious Trojan Horse



52
/ 69

52 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764d
ec

june11.dll

invalid-signature overlay pedll signed

549.84 KB
Size

2021-06-08 00:51:04 UTC
47 minutes ago

Ad-Aware	Trojan.Mint.Zamg.O	Malware/Win32.RL_Generic.R346613	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O

The End