

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



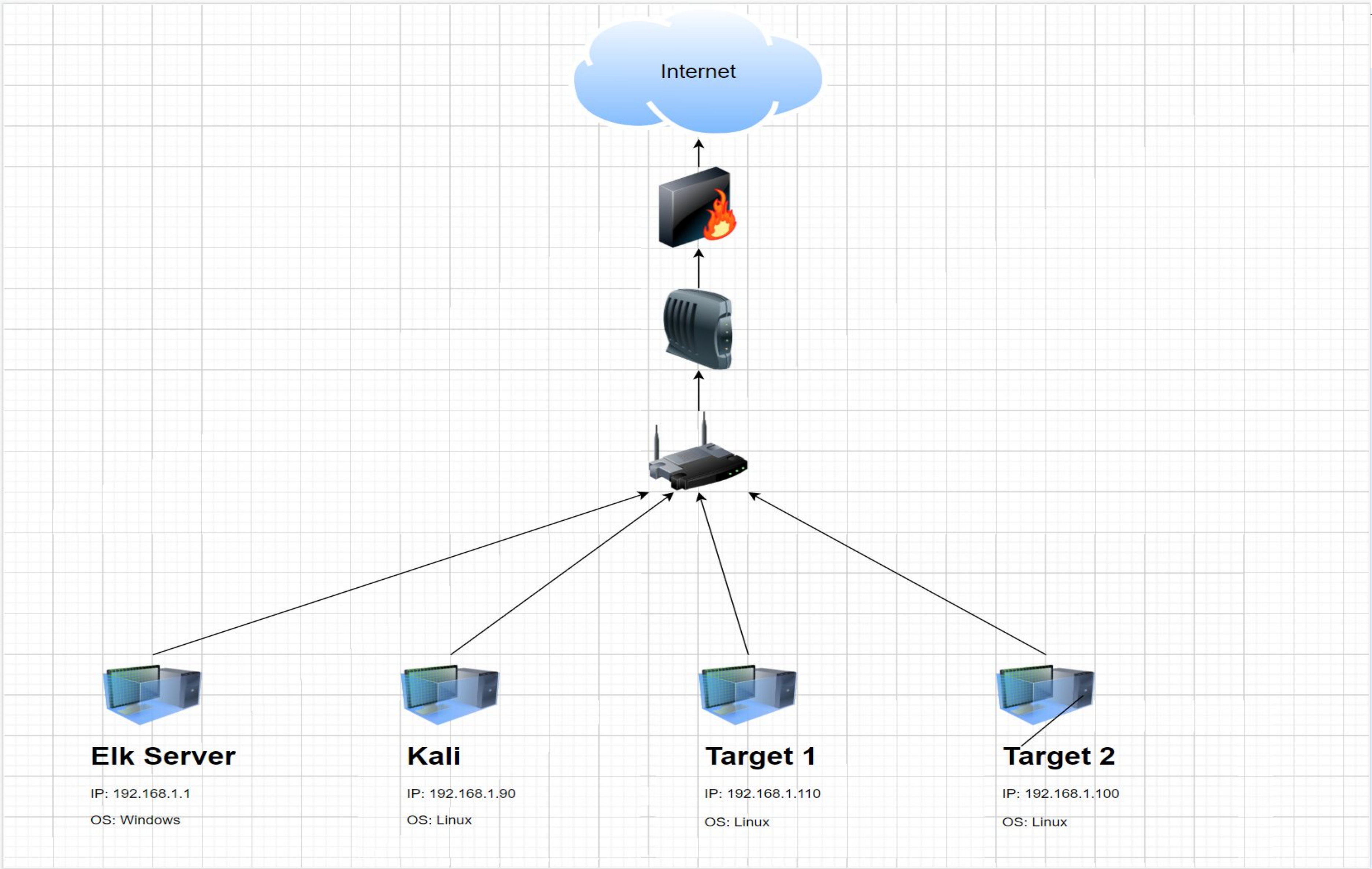
Normal Activity



Malicious Activity

Network Topology & Critical Vulnerabilities

Network Topology



Network

Address
Range:192.168.1.1/225
Netmask:255.255.255.0
Gateway:10.0.0.1

Machines

IPv4:192.168.1.1
OS:Windows
Hostname:Elk Server

IPv4:192.168.1.90
OS:Linux
Hostname:Kali

IPv4:192.168.1.110
OS:Linux
Hostname:Target 1

IPv4:192.168.1.100
OS:Linux
Hostname:Target 2

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
SSH	22/top	OpenSSH
HTTP	80/tcp	Apache http 2.4.10
rpcbind	111/tcp	2-4
netbios-ssn	139/tcp	Samba smdb 3.X - 4.X
netbios-ssn	445/tcp	samba smbd 3.X - 4.X

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
ssh	22/tcp	openSSH
http	80/tcp	apache http 2.4.10
rpcbind	111/tcp	2.4 (rpc)
netbios-ssn	139/tcp	samba smbd 3.X - 4.X
netbios-ssn	445/tcp	samba smbd 3.X - 4.X

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 - 40m bytes 185.243.115.84 - 30m bytes 166.62.111.64 - 8082k bytes	Machines that sent the most traffic.
Most Common Protocols	TCP- 90, 496 packets UDP- 11, 838 packets TLS- 10,657 packets	Three most common protocols on the network.
# of Unique IP Addresses	810 ipv4, 7 ipv6	Count of observed IP addresses.
Subnets	172.16.4.0/24 10.6.12.0/24 10.11.110/24	Observed subnet ranges.
# of Malware Species	51	Number of malware binaries identified in traffic.

Statistics

Measurement	Captured	Displayed	Marked
Packets	102464	102464 (100.0%)	—
Time span, s	1093.372	1093.372	—
Average pps	93.7	93.7	—
Average packet size, B	902	902	—
Bytes	92414930	92414930 (100.0%)	0
Average bytes/s	84 k	84 k	—
Average bits/s	676 k	676 k	—

IPv4 · 810		IPv6 · 7					
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Count
172.16.4.205	45,888	40 M	22,562	16 M	23,326	24 M	—
185.243.115.84	34,199	30 M	15,659	15 M	18,540	15 M	—
10.0.0.201	16,357	9,873 k	7,281	781 k	9,076	9,091 k	—
10.11.11.200	8,034	4,032 k	4,199	468 k	3,835	3,564 k	—
166.62.111.64	7,864	8,082 k	5,677	7,921 k	2,187	160 k	—
10.6.12.203	7,410	5,574 k	2,567	399 k	4,843	5,175 k	—
10.11.11.179	6,297	3,369 k	3,245	364 k	3,052	3,004 k	—
10.11.11.11	5,472	975 k	2,293	397 k	3,179	578 k	—
192.168.1.90	5,184	24 M	3,358	23 M	1,826	506 k	—
192.168.1.100	5,184	24 M	1,826	506 k	3,358	23 M	—
64.187.66.143	4,688	3,493 k	2,540	3,354 k	2,148	139 k	—
5.101.51.151	4,326	4,246 k	3,262	4,177 k	1,064	68 k	—
10.11.11.217	4,197	1,989 k	2,199	252 k	1,998	1,737 k	—
23.43.62.169	4,007	4,080 k	2,697	4,008 k	1,310	71 k	—
151.101.50.208	3,270	2,220 k	1,657	2,108 k	1,613	112 k	—
10.6.12.12	2,852	700 k	1,332	329 k	1,520	371 k	—
10.6.12.157	2,408	809 k	1,231	285 k	1,177	524 k	—
10.11.11.195	2,074	779 k	1,134	103 k	940	676 k	—
10.11.11.203	1,789	716 k	982	182 k	807	533 k	—
172.16.4.4	1,451	346 k	703	142 k	748	203 k	—
172.16.4.152	1,206	677 k	614	614 k	592	62 k	—

Wireshark · Protocol Hierarchy Statistics · final.cap.pcapng

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	102464	100.0
Ethernet	100.0	102464	1.6
Internet Protocol Version 4	100.0	102449	2.2
Transmission Control Protocol	88.3	90496	91.7
Transport Layer Security	10.4	10657	13.9
Hypertext Transfer Protocol	4.2	4273	62.1
Malformed Packet	2.8	2821	0.0
VSS Monitoring Ethernet trailer	0.9	907	0.0
BitTorrent	0.9	877	0.1
NetBIOS Session Service	0.8	857	0.3
Lightweight Directory Access Protocol	0.7	679	0.4
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.6	638	0.2
Data	0.3	304	0.7
Kerberos	0.3	284	0.4
User Datagram Protocol	11.6	11838	0.1
Internet Group Management Protocol	0.1	115	0.0
Internet Protocol Version 6	0.0	15	0.0



frame contains ".dll"

No.	Time	Source	Destination	Protocol	Length	Info
46488	439.227592400	192.168.1.90	192.168.1.100	TCP	4162	48606 →
46184	437.437981600	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.c...	TCP	1514	80 → 497
45496	428.217270700	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	312	GET /fil
45494	428.211403500	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.c...	HTTP	542	HTTP/1.1

final.cap.pcapng

Packets: 102464 · Displayed: 4 (0.0%)

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Watching Youtube
- Browsing the web

Suspicious Activity

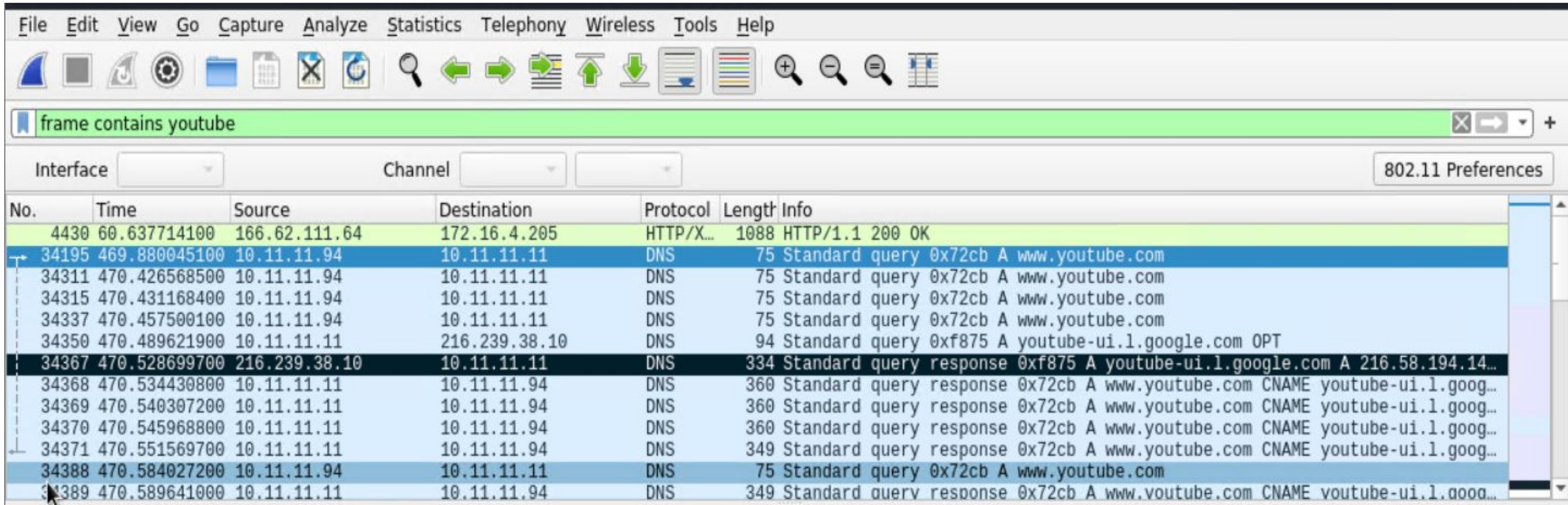
- Illegitimately downloading torrents
- Downloading malware

Normal Activity

YouTube

Summarize the following:

- The protocols observed were HTTP, DNS, TCP, TLS
- The user was searching for and watching YouTube videos



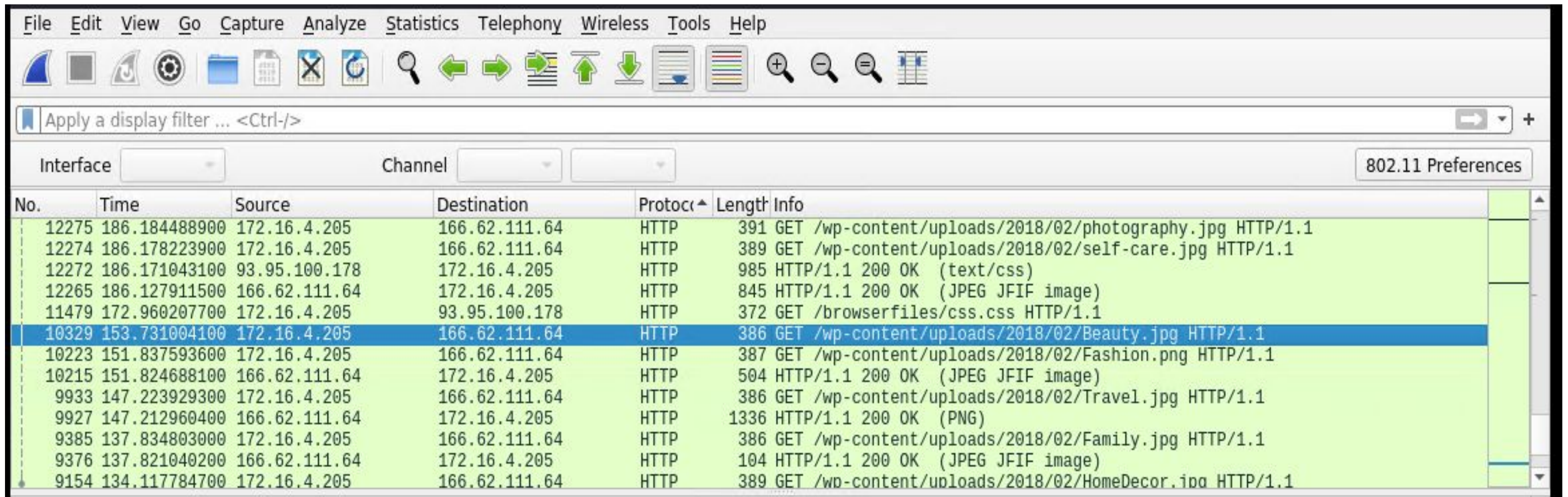
The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet manipulation. A search bar at the top of the packet list contains the text "frame contains youtube". Below the search bar are dropdown menus for "Interface" and "Channel", and a button for "802.11 Preferences". The main area displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered to show only those containing the word "youtube".

No.	Time	Source	Destination	Protocol	Length	Info
4430	60.637714100	166.62.111.64	172.16.4.205	HTTP/X...	1088	HTTP/1.1 200 OK
34195	469.880045100	10.11.11.94	10.11.11.11	DNS	75	Standard query 0x72cb A www.youtube.com
34311	470.426568500	10.11.11.94	10.11.11.11	DNS	75	Standard query 0x72cb A www.youtube.com
34315	470.431168400	10.11.11.94	10.11.11.11	DNS	75	Standard query 0x72cb A www.youtube.com
34337	470.457500100	10.11.11.94	10.11.11.11	DNS	75	Standard query 0x72cb A www.youtube.com
34350	470.489621900	10.11.11.11	216.239.38.10	DNS	94	Standard query 0xf875 A youtube-ui.l.google.com OPT
34367	470.528699700	216.239.38.10	10.11.11.11	DNS	334	Standard query response 0xf875 A youtube-ui.l.google.com A 216.58.194.14...
34368	470.534430800	10.11.11.11	10.11.11.94	DNS	360	Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.goog...
34369	470.540307200	10.11.11.11	10.11.11.94	DNS	360	Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.goog...
34370	470.545968800	10.11.11.11	10.11.11.94	DNS	360	Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.goog...
34371	470.551569700	10.11.11.11	10.11.11.94	DNS	349	Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.goog...
34388	470.584027200	10.11.11.94	10.11.11.11	DNS	75	Standard query 0x72cb A www.youtube.com
34389	470.589641000	10.11.11.11	10.11.11.94	DNS	349	Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.goog...

Web Browsing

Summarize the following:

- The traffic observed is HTTP web traffic
- The user was browsing the site mysocalledchaos.com



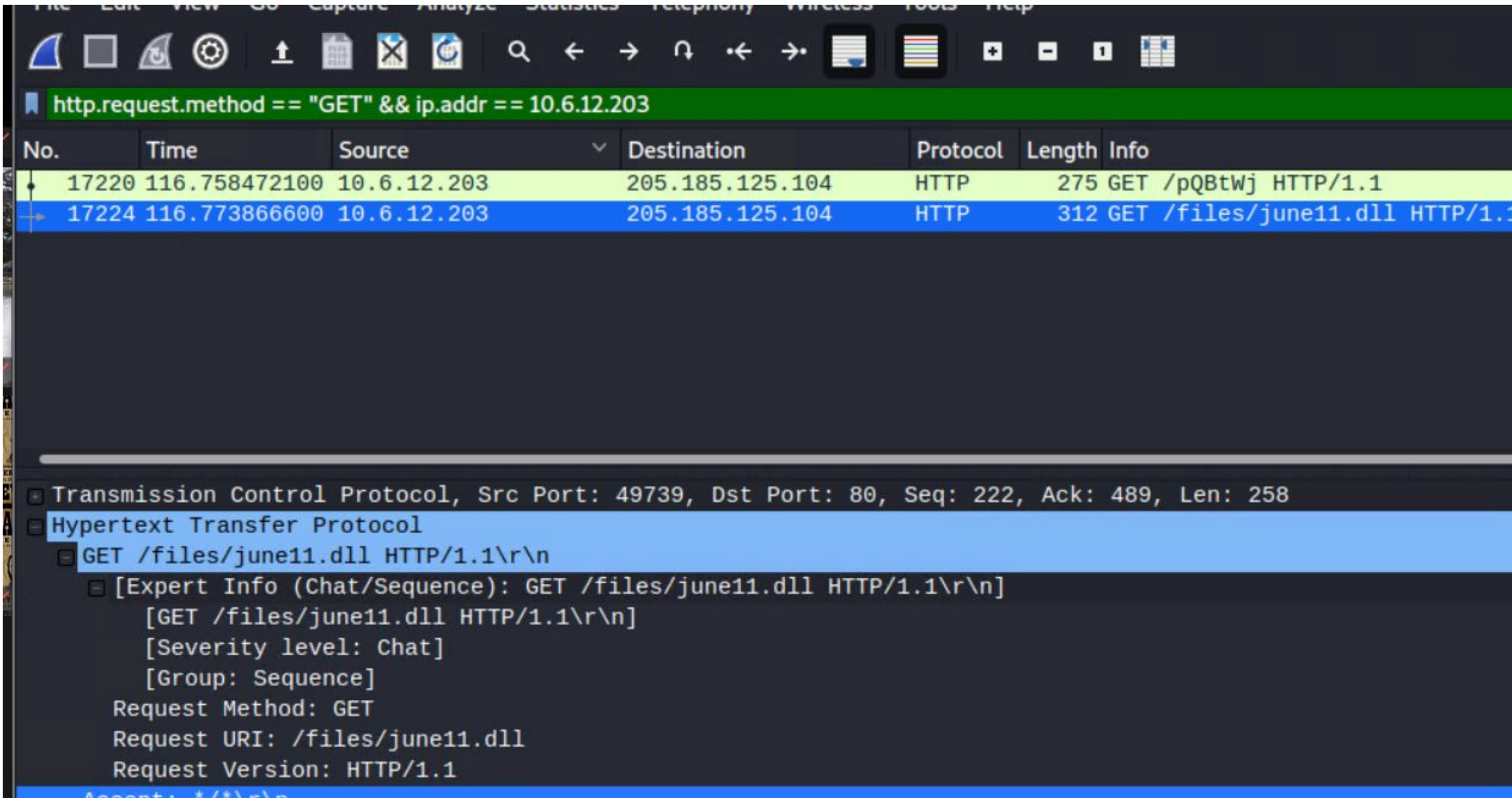
The image shows a Wireshark network traffic capture. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter bar. The main pane shows a list of network packets. The selected packet is number 10329, which is an HTTP GET request for a JPEG image from mysocalledchaos.com.

No.	Time	Source	Destination	Protocol	Length	Info
12275	186.184488900	172.16.4.205	166.62.111.64	HTTP	391	GET /wp-content/uploads/2018/02/photography.jpg HTTP/1.1
12274	186.178223900	172.16.4.205	166.62.111.64	HTTP	389	GET /wp-content/uploads/2018/02/self-care.jpg HTTP/1.1
12272	186.171043100	93.95.100.178	172.16.4.205	HTTP	985	HTTP/1.1 200 OK (text/css)
12265	186.127911500	166.62.111.64	172.16.4.205	HTTP	845	HTTP/1.1 200 OK (JPEG JFIF image)
11479	172.960207700	172.16.4.205	93.95.100.178	HTTP	372	GET /browserfiles/css.css HTTP/1.1
10329	153.731004100	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Beauty.jpg HTTP/1.1
10223	151.837593600	172.16.4.205	166.62.111.64	HTTP	387	GET /wp-content/uploads/2018/02/Fashion.png HTTP/1.1
10215	151.824688100	166.62.111.64	172.16.4.205	HTTP	504	HTTP/1.1 200 OK (JPEG JFIF image)
9933	147.223929300	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Travel.jpg HTTP/1.1
9927	147.212960400	166.62.111.64	172.16.4.205	HTTP	1336	HTTP/1.1 200 OK (PNG)
9385	137.834803000	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Family.jpg HTTP/1.1
9376	137.821040200	166.62.111.64	172.16.4.205	HTTP	104	HTTP/1.1 200 OK (JPEG JFIF image)
9154	134.117784700	172.16.4.205	166.62.111.64	HTTP	389	GET /wp-content/uploads/2018/02/HomeDecor.jpg HTTP/1.1

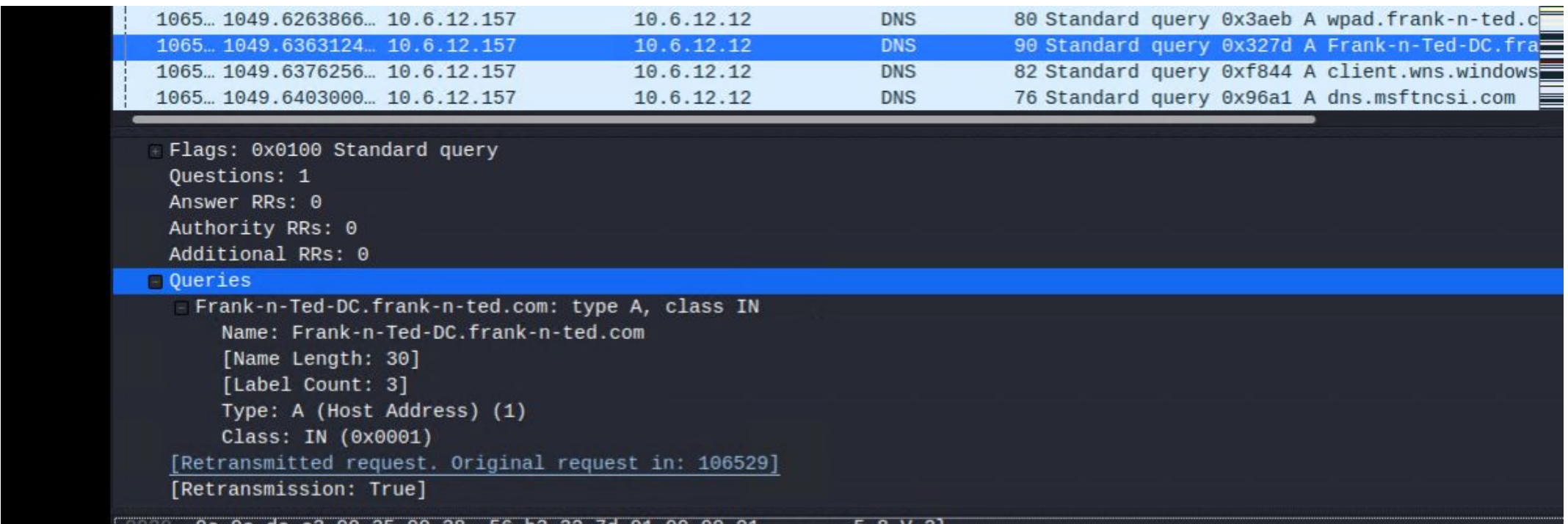
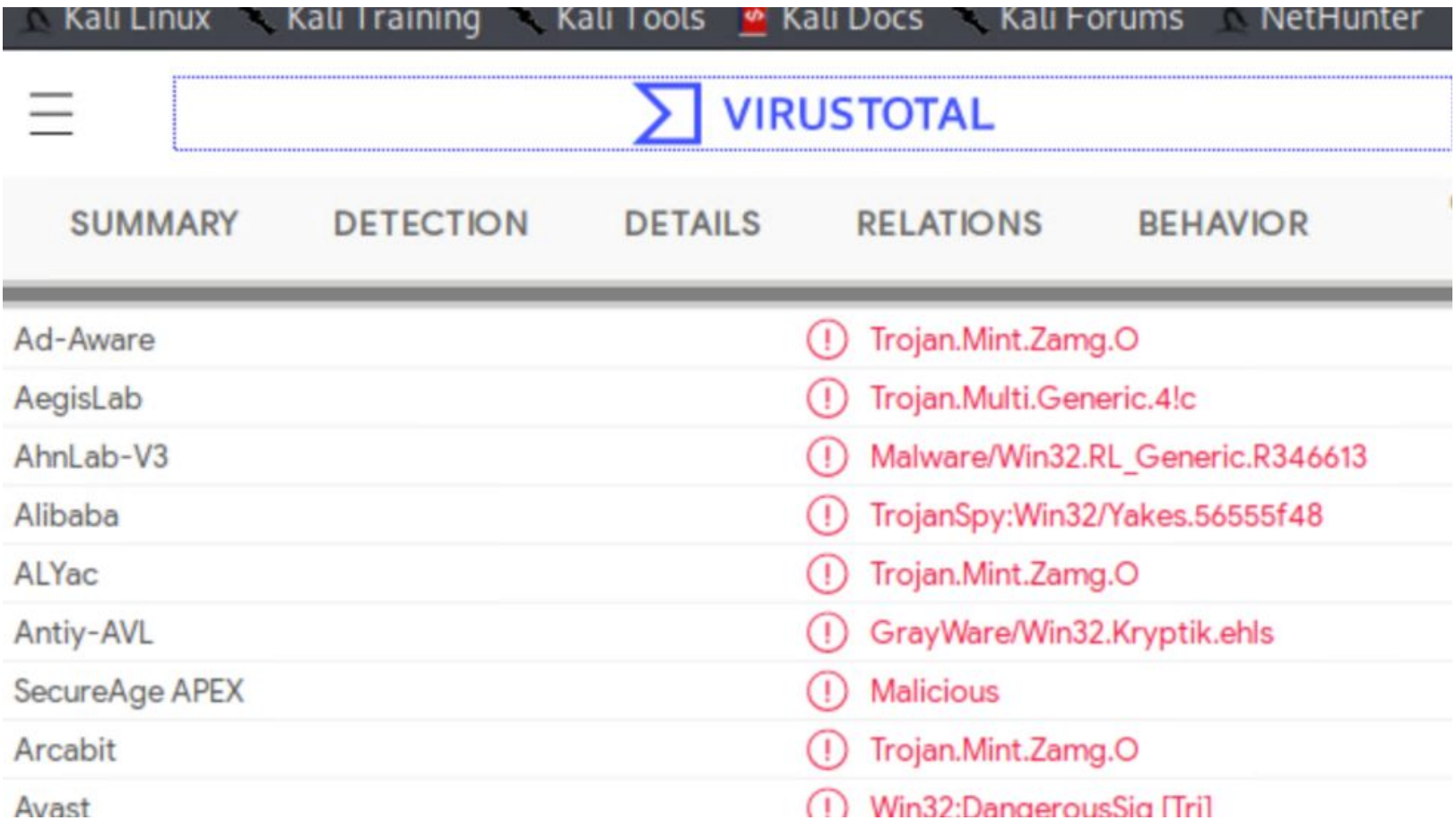
Malicious Activity

Malware Infection

- Protocols observed are HTTP, DNS, TCP, CLDAP
- User browsing YouTube and the web on Active Directory server



- June11.dll is classified as Trojan Horse



Copyright Infringement

- Protocols observed include: DNS, TCP, TLS, UDP, BitTorrent, HTTP
- User is downloading material for their workstation

No.	Time	Source	Destination	Protocol	Length	Info
28075	222.174645500	10.0.0.201	104.18.20.226	HTTP	313	GET /gsorganizationvalsha2g2/M
28095	222.222644100	10.0.0.201	72.21.91.29	HTTP	292	GET /MFEwTzBNMEswSTAJBgUrDgMCG
28182	222.524277100	10.0.0.201	50.63.243.230	HTTP	270	GET //MEIwQDA%2BMDwwOjAJBgUrDg
28269	222.815624000	10.0.0.201	50.63.243.230	HTTP	276	GET //MEkwrZBFMEMwQTAJBgUrDgMC
28431	223.272788300	10.0.0.201	168.215.194.14	HTTP	534	GET /nshowmovie.html?movieid=5
28447	223.400513900	10.0.0.201	168.215.194.14	HTTP	471	GET /yellow-star.gif HTTP/1.1
28455	223.416900800	10.0.0.201	172.217.9.2	HTTP	434	GET /pagead/show_ads.js HTTP/1
28460	223.427332400	10.0.0.201	50.18.44.131	HTTP	412	GET /tools/diggthis.js HTTP/1
28486	223.553734600	10.0.0.201	168.215.194.14	HTTP	500	GET /grabs/bettybooprythmonthe

Frame 28486: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface eth0, id 0
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14
Transmission Control Protocol, Src Port: 49817, Dst Port: 80, Seq: 481, Ack: 11057, Len: 446
Hypertext Transfer Protocol
GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n]
[GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /grabs/bettybooprythmonthereservationgrab.jpg
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n

No.	Time	Source	Destination	Protocol	Length	Info
29048	228.504185600	10.0.0.201	168.215.194.14	HTTP	589	GET /bt/btdownload.php?type=tor
29092	228.700490100	10.0.0.201	140.211.166.134	HTTP	195	GET /version-1.0 HTTP/1.1
29096	228.709912100	10.0.0.201	91.189.95.21	HTTP	423	GET /announce?info_hash=%e4%be%
29332	229.368377500	10.0.0.201	168.215.194.14	HTTP	434	GET /bt/announce.php?info_hash=9
29362	229.445135200	10.0.0.201	168.215.195.227	HTTP	434	GET /announce?info_hash=%1d%da%
29456	229.728165300	10.0.0.201	168.215.194.14	HTTP	253	GET /bt/scrape.php?info_hash=%1d
29476	229.774534900	10.0.0.201	168.215.195.227	HTTP	253	GET /scrape?info_hash=%1d%da%0d
37450	291.699226600	10.0.0.201	72.21.91.29	HTTP	288	GET /MFEwTzBNMEswSTAJBgUrDgMCGl
37454	291.706518800	10.0.0.201	72.21.91.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGl

Transmission Control Protocol, Src Port: 49834, Dst Port: 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_Reservat
Request Method: GET
Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

- Betty_Boop_Rhythm_on_the_Reservation.avi.torrent is a copyrighted video file



The End