

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



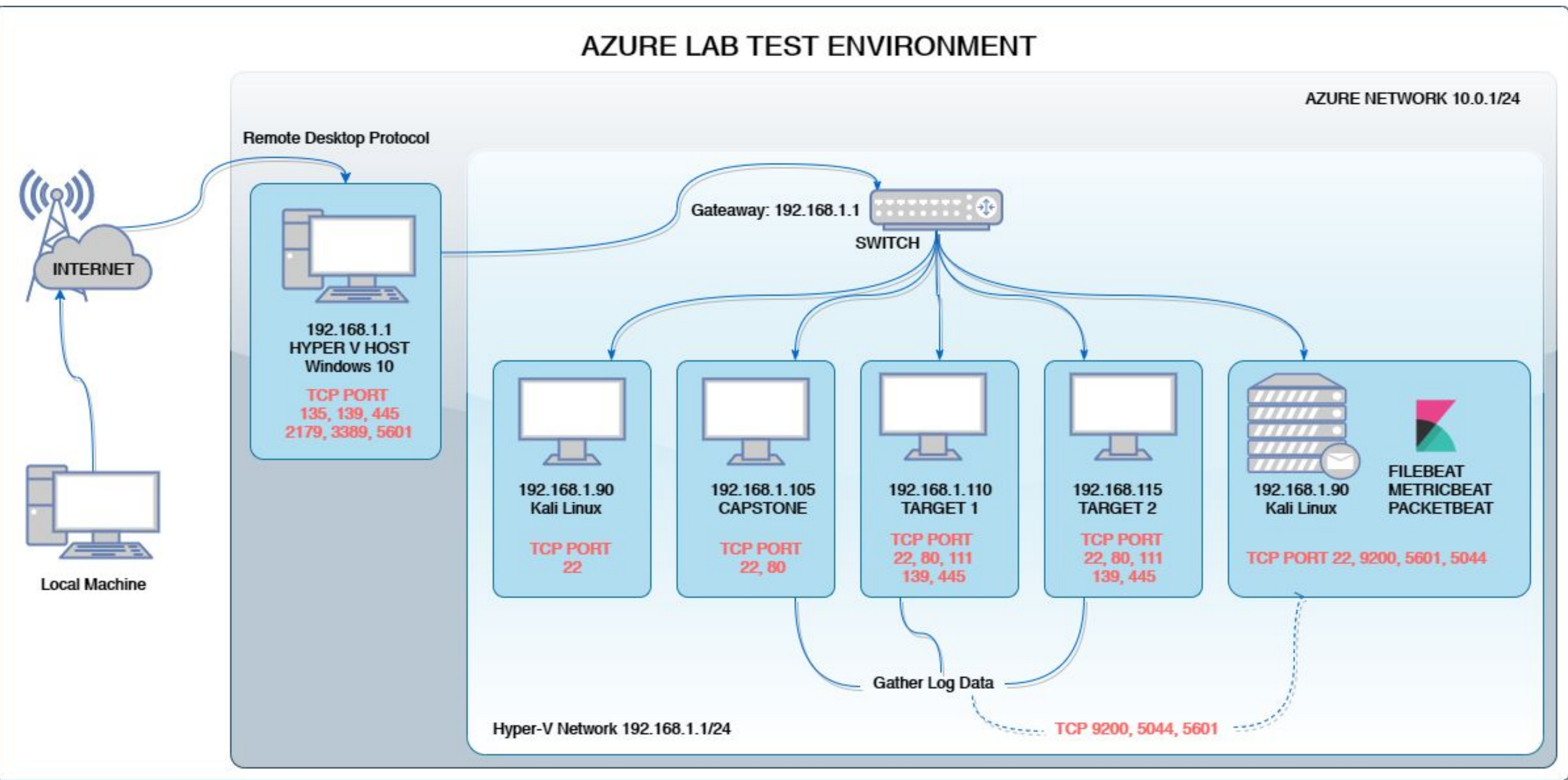
Normal Activity



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: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
Hostname: ELK

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
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

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 172.16.4.205	Machines that sent the most traffic.
Most Common Protocols	HTTP, TCP, UDP	Three most common protocols on the network.
# of Unique IP Addresses	808 +2 (IPv4 +IPv6)	Count of observed IP addresses.
Subnets	10.6.12.0/24 172.16.4.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	june11.dll	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

- Web browsing, dns queries, dhcp request.

Suspicious Activity

- malware downloaded, malware outbound traffic, torrent downloads

The background of the slide is a dark gray field filled with a complex, repeating pattern of geometric shapes. These shapes include squares and triangles of various sizes, some of which are further divided into smaller triangles, creating a tessellated effect. The colors are monochromatic, ranging from very dark gray to a slightly lighter, charcoal gray, which gives the background a textured, three-dimensional appearance.

Normal Activity

Web Browsing

Summarize the following:

- What kind of traffic did you observe? **Browsing the internet - HTTP Traffic**
- Which protocol(s)? **Common Protocol Used: HTTP using TCP Port:80**
- What, specifically, was the user doing? Which site were they browsing? Etc.

Downloading Files <http://detectportal.firefox.com/success.txt>

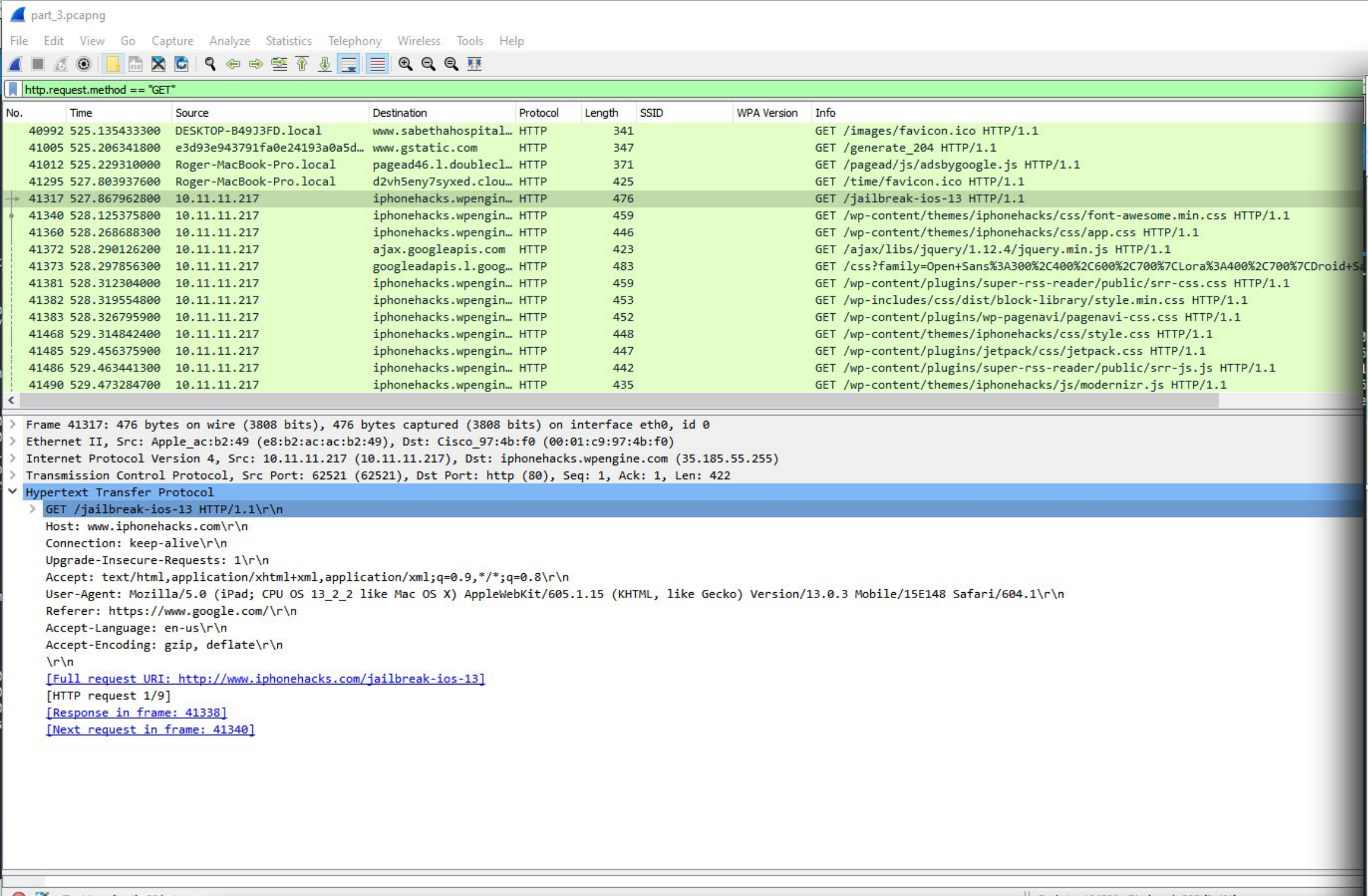
Uploading Files <http://mysocalledchaos.com/wp-content/upload/2018/02/Beauty.jpg>

Online Shopping <http://www.assoc-amazon.com/s/ads.js>

Searching <http://www.iphonehacks.com/jailbreak-ios-13>

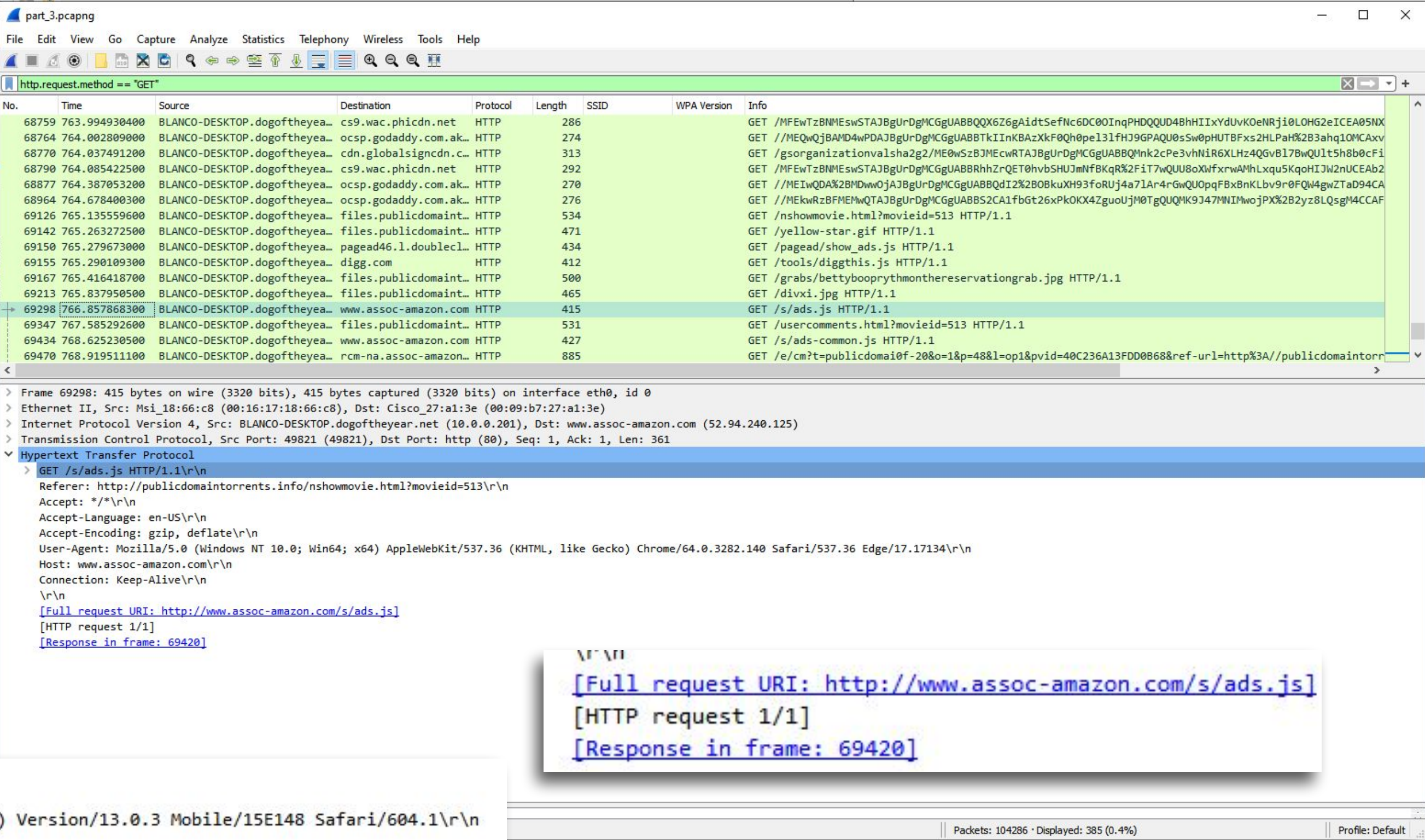
Web Brosing

Searching (Example)



Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (iPad; CPU OS 13_2_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1\r\n
Referer: https://www.google.com/\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
\r\n
[Full request URI: http://www.iphonehacks.com/jailbreak-ios-13]
[HTTP request 1/9]
[Response in frame: 41338]
[Next request in frame: 41340]

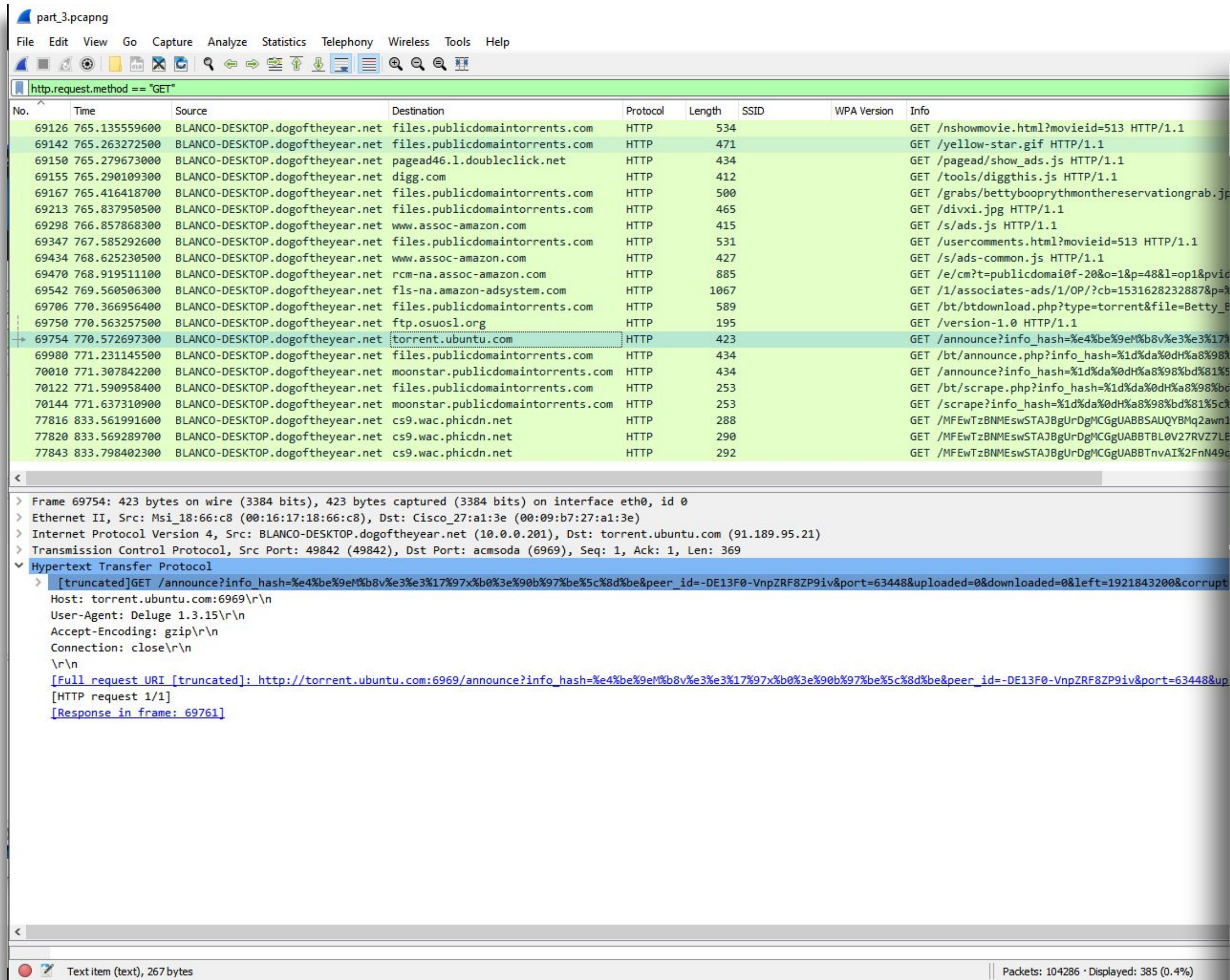
Online Shopping, Browsing ads (Example)



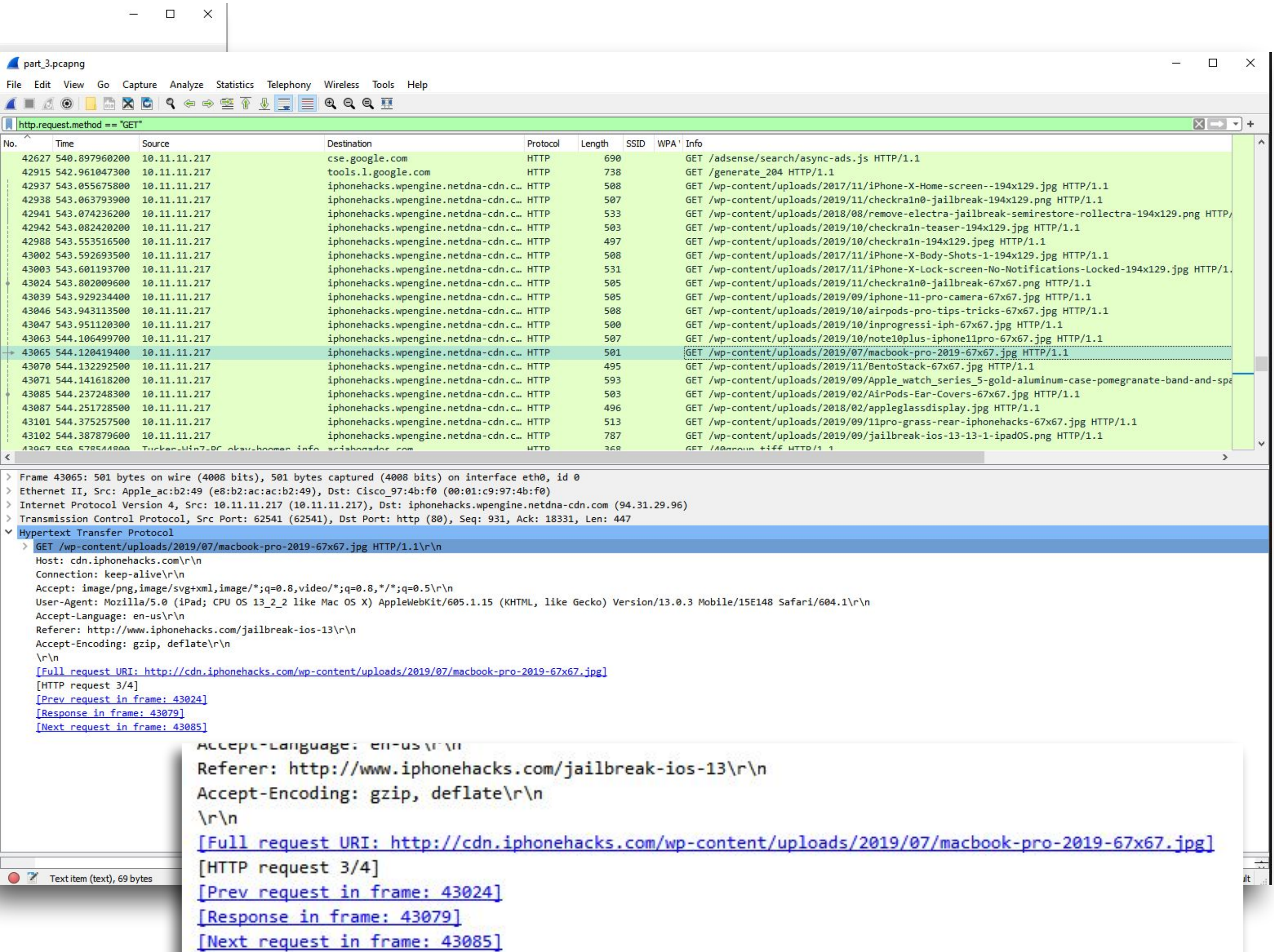
Full request URI: http://www.assoc-amazon.com/s/ads.js
[HTTP request 1/1]
[Response in frame: 69420]

Web Browsing

Downloading a File (Example)



Uploading a File (Example)



Torrent Application Download

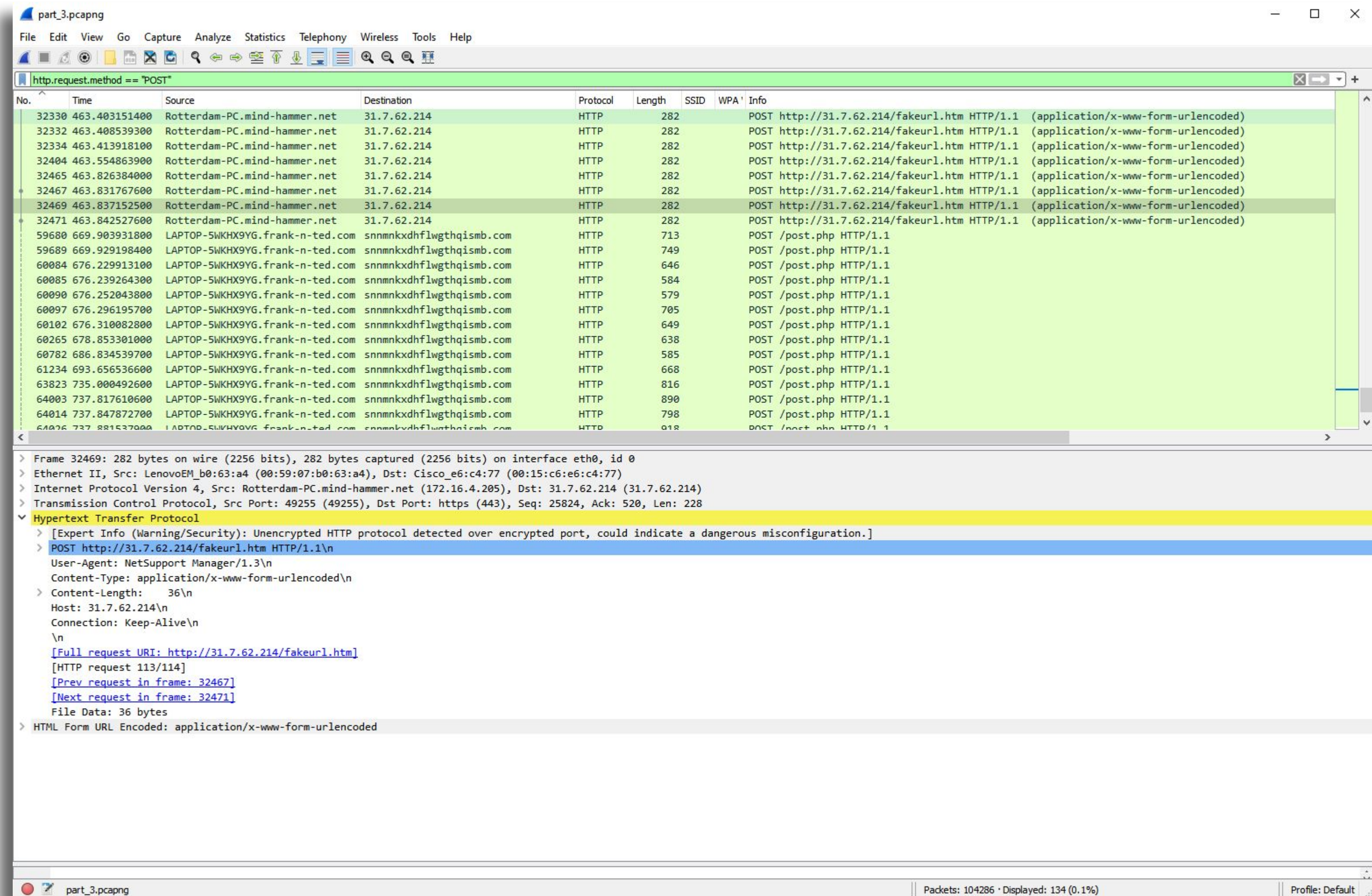
A file downloaded request from a Torrent Site



HTTP POST Request Method - Interesting Traffic

A post request method using secure HTTP connection

- What kind of traffic did you observe? Which protocol(s)?
 - The warning indicates that “Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous configuration”
 - The POST request Method is using a secure HTTP protocol TCP Port 443
 - There are multiple traffic found on the same request.



DHCP Request

DHCP Protocol using UDP Port 67 and 68

part_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	SSID	WPA Version	Info
3312	50.38222800	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x45714260
23687	335.628617000	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-hammer.net	DHCP	342			DHCP ACK - Transaction ID 0x463c3b47
23708	336.029724400	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x463c3b47
31783	461.405481600	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-hammer.net	DHCP	342			DHCP ACK - Transaction ID 0x8b4f027d
31788	461.414812500	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x8b4f027d
55419	641.041865800	0.0.0.0	255.255.255.255	DHCP	378			DHCP Request - Transaction ID 0xba8bd7f0
55420	641.047496500	Frank-n-Ted-DC.frank-n-ted...	255.255.255.255	DHCP	351			DHCP ACK - Transaction ID 0xba8bd7f0
56171	644.329009000	0.0.0.0	255.255.255.255	DHCP	380			DHCP Request - Transaction ID 0x6b0e1d90
56172	644.334065400	Frank-n-Ted-DC.frank-n-ted...	255.255.255.255	DHCP	342			DHCP NAK - Transaction ID 0x6b0e1d90
65433	743.503872800	0.0.0.0	255.255.255.255	DHCP	379			DHCP Request - Transaction ID 0x20640255
65434	743.509344200	10.0.0.1	BLANCO-DESKTOP.dogoftheyear.net	DHCP	342			DHCP ACK - Transaction ID 0x20640255
82231	902.090777100	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x45714260
1025...	1187.337161400	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-hammer.net	DHCP	342			DHCP ACK - Transaction ID 0x463c3b47
1026...	1187.738262900	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x463c3b47

<

> Frame 102583: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
> Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
> Internet Protocol Version 4, Src: mind-hammer-dc.mind-hammer.net (172.16.4.4), Dst: Rotterdam-PC.mind-hammer.net (172.16.4.205)
> User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Dynamic Host Configuration Protocol (ACK)
 Message type: Boot Reply (2)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x463c3b47
 Seconds elapsed: 0
 Bootp flags: 0x0000 (Unicast)
 Client IP address: Rotterdam-PC.mind-hammer.net (172.16.4.205)
 Your (client) IP address: 0.0.0.0 (0.0.0.0)
 Next server IP address: 0.0.0.0 (0.0.0.0)
 Relay agent IP address: 0.0.0.0 (0.0.0.0)
 Client MAC address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 Option: (53) DHCP Message Type (ACK)
 Option: (54) DHCP Server Identifier (172.16.4.4)
 Option: (1) Subnet Mask (255.255.255.0)
 Option: (43) Vendor-Specific Information
 Option: (15) Domain Name
 Option: (3) Router

mind-hammer-dc.mind-hammer.net (172.16.4.4)
Dst Port: bootpc (68)

part_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	SSID	WPA Version	Info
3312	50.38222800	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x45714260
23687	335.628617000	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-hammer.net	DHCP	342			DHCP ACK - Transaction ID 0x463c3b47
23708	336.029724400	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x463c3b47
31783	461.405481600	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-hammer.net	DHCP	342			DHCP ACK - Transaction ID 0x8b4f027d
31788	461.414812500	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x8b4f027d
55419	641.041865800	0.0.0.0	255.255.255.255	DHCP	378			DHCP Request - Transaction ID 0xba8bd7f0
55420	641.047496500	Frank-n-Ted-DC.frank-n-ted...	255.255.255.255	DHCP	351			DHCP ACK - Transaction ID 0xba8bd7f0
56171	644.329009000	0.0.0.0	255.255.255.255	DHCP	380			DHCP Request - Transaction ID 0x6b0e1d90
56172	644.334065400	Frank-n-Ted-DC.frank-n-ted...	255.255.255.255	DHCP	342			DHCP NAK - Transaction ID 0x6b0e1d90
65433	743.503872800	0.0.0.0	255.255.255.255	DHCP	379			DHCP Request - Transaction ID 0x20640255
65434	743.509344200	10.0.0.1	BLANCO-DESKTOP.dogoftheyear.net	DHCP	342			DHCP ACK - Transaction ID 0x20640255
82231	902.090777100	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x45714260
1025...	1187.337161400	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-hammer.net	DHCP	342			DHCP ACK - Transaction ID 0x463c3b47
1026...	1187.738262900	Rotterdam-PC.mind-hammer.n...	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x463c3b47

<

> Frame 82231: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
> Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 255.255.255.255 (255.255.255.255)
> User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Dynamic Host Configuration Protocol (Inform)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x45714260
 Seconds elapsed: 0
 Bootp flags: 0x0000 (Unicast)
 Client IP address: Rotterdam-PC.mind-hammer.net (172.16.4.205)
 Your (client) IP address: 0.0.0.0 (0.0.0.0)
 Next server IP address: 0.0.0.0 (0.0.0.0)
 Relay agent IP address: 0.0.0.0 (0.0.0.0)
 Client MAC address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 Option: (53) DHCP Message Type (Inform)
 Option: (61) Client identifier
 Option: (12) Host Name
 Option: (60) Vendor class identifier

Rotterdam-PC.mind-hammer.net (172.16.4.205)
Dst Port: bootps (67)

14

DNS Queries using UDP Port 53

15

Malicious Activity

Torrenting copyright material

- What kind of traffic did you observe? **Downloading jpg from Torrent site**
- Which protocol(s)? **HTTP port 80**
- What, specifically, was the user doing? Which site were they browsing? Etc.

<http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrap.jpg>

part_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.0.0.0/24 && http.request.method == "GET"

No.	Time	Source	Destination	Protocol	Length	SSID	WPA Version	Info
68756	763.988411900	BLANCO-DESKTOP.dogoftheyea...	cs9.wac.phicdn.net	HTTP	286			GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBBQX6Z6gAidtSefNc6DC00InqPHDQQUD4BhHIIxYdUvK0eNRji0LOHG2eI
68759	763.994930400	BLANCO-DESKTOP.dogoftheyea...	cs9.wac.phicdn.net	HTTP	286			GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBBQX6Z6gAidtSefNc6DC00InqPHDQQUD4BhHIIxYdUvK0eNRji0LOHG2eI
68764	764.002809000	BLANCO-DESKTOP.dogoftheyea...	ocsp.godaddy.com.akadns.net	HTTP	274			GET //MEQwQjBAMD4wPDAJBgUrDgMCGgUABBTkIInKBAzXkf0Qh0pe131fHJ9GPAQU0sSw0pHUTBFxs2HLPaH%2B3ahq
68770	764.037491200	BLANCO-DESKTOP.dogoftheyea...	cdn.globalsigncdn.com.cdn.cloudf...	HTTP	313			GET /gsorganizationvalsha2g2/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBBQmNk2cPe3vhnIR6XLHz4Q6vB17BwQU1t5
68790	764.085422500	BLANCO-DESKTOP.dogoftheyea...	cs9.wac.phicdn.net	HTTP	292			GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRhhZrQET0hvbSHUJmNfBKqR%2FiT7wQUU8oXWfXrwAMhLxqu5KqoHIJW2
68877	764.387053200	BLANCO-DESKTOP.dogoftheyea...	ocsp.godaddy.com.akadns.net	HTTP	270			GET //MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBBQdI2%2B0BkuXH93foRUj4a71Ar4rGwQU0pqFBxBnKLbv9r0FQW4gwZ
68964	764.678400300	BLANCO-DESKTOP.dogoftheyea...	ocsp.godaddy.com.akadns.net	HTTP	276			GET //MEKwRzBFMEMwQTAJBgUrDgMCGgUABBS2CA1fbgt26xPkOKX4ZguoUjM0TgQUQMK9J47MNIWojPX%2B2yz8LQs
69126	765.135559600	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	534			GET /nshowmovie.html?movieid=513 HTTP/1.1
69142	765.263272500	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	471			GET /yellow-star.gif HTTP/1.1
69150	765.279673000	BLANCO-DESKTOP.dogoftheyea...	pagead46.l.doubleclick.net	HTTP	434			GET /pagead/show_ads.js HTTP/1.1
69155	765.290109300	BLANCO-DESKTOP.dogoftheyea...	digg.com	HTTP	412			GET /tools/diggethis.js HTTP/1.1
69167	765.416418700	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	500			GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213	765.837950500	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	465			GET /divxi.jpg HTTP/1.1
69298	766.857868300	BLANCO-DESKTOP.dogoftheyea...	www.assoc-amazon.com	HTTP	415			GET /s/ads.js HTTP/1.1

> Frame 69167: 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: BLANCO-DESKTOP.dogoftheyea.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
> Transmission Control Protocol, Src Port: 49817 (49817), Dst Port: http (80), Seq: 481, Ack: 11057, Len: 446

Hypertext Transfer Protocol

> GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\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
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]
[HTTP request 2/2]
[Prev request in frame: 69126]
[Response in frame: 69417]

Connection: Keep-Alive\r\n
\r\n

[Full request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]

[HTTP request 2/2]

[Prev request in frame: 69126]

[Response in frame: 69417]

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



Malware download

part_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	SSID	WPA Version	Info
53609	636.442537900	Gilbert-Win7-PC.okay-boome...	awseb-e-i-awseb1oa-5f3ihws149wt-...	HTTP	433			GET /js/v2/ktag.js?tid=KT-N2BAB-3ED HTTP/1.1
53862	637.188732800	Gilbert-Win7-PC.okay-boome...	match-975362022.us-east-1.elb.am...	HTTP	706			GET /track/cmfrightmedia?xid=I59ixguB5j05zerq4R0JN_yU&gdpr=0&gdpr_cc
53951	637.350691200	10.11.11.217	iphonehacks.wpengine.com	HTTP	803			GET /wp-content/themes/iphonehacks/favicon.ico HTTP/1.1
53952	637.363545000	10.11.11.217	iphonehacks.wpengine.com	HTTP	803			GET /wp-content/themes/iphonehacks/favicon.png HTTP/1.1
53985	637.441169700	10.11.11.121	orbike.com	HTTP	605			GET / HTTP/1.1
54007	637.630697100	10.11.11.121	orbike.com	HTTP	524			GET / HTTP/1.1
57901	652.318762000	DESKTOP-86J4BX.frank-n-ted...	cardboardspaceshiptoys.com	HTTP	513			GET /logs/invoice-86495.doc HTTP/1.1
58748	658.621258400	LAPTOP-5WKHX9YG.frank-n-te...	205.185.125.104	HTTP	275			GET /pQ8twj HTTP/1.1
58752	658.636633700	LAPTOP-5WKHX9YG.frank-n-te...	205.185.125.104	HTTP	312			GET /files/june11.dll HTTP/1.1
67268	752.331198600	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	463			GET /nshowcat.html?category=animation HTTP/1.1
67282	752.441022900	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	474			GET /srsbanner.gif HTTP/1.1
67308	752.676394600	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	477			GET /grabs/hdsale.png HTTP/1.1
67328	752.881136800	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	469			GET /ipod.jpg HTTP/1.1
67330	752.889450700	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	468			GET /pda.jpg HTTP/1.1
67333	752.898433200	BLANCO-DESKTOP.dogoftheyea...	files.publicdomaintorrents.com	HTTP	470			GET /pda.jpg HTTP/1.1

> Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0

> 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

> Hypertext Transfer Protocol

> GET /files/june11.dll HTTP/1.1\r\n

Accept: */*\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

Host: 205.185.125.104\r\n

Connection: Keep-Alive\r\n

> Cookie: _subid=3mmhfnd8jp\r\n\r\n

[Full request URI: http://205.185.125.104/files/june11.dll]

[HTTP request 2/2]

[Prev request in frame: 58748]

[Response in frame: 59388]

> Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on in

> Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec

> Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203),

> Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq

> Hypertext Transfer Protocol

> GET /files/june11.dll HTTP/1.1\r\n

Accept: */*\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Triden

Host: 205.185.125.104\r\n

Connection: Keep-Alive\r\n

> Cookie: _subid=3mmhfnd8jp\r\n\r\n

[Full request URI: http://205.185.125.104/files/june11.dll]

[HTTP request 2/2]

[Prev request in frame: 58748]

[Response in frame: 59388]

- What kind of traffic did you observe? **Downloading june11.dll file**
- Which protocol(s)? **HTTP port 80**
- What, specifically,
- was the user doing?

Which site were they browsing?

http://205.185.125.104/files/june11.dll



The End