

# **Final Engagement**

**Attack, Defense & Analysis of a Vulnerable Network**

# Table of Contents

---

This document contains the following resources:



**Network Topology & Critical Vulnerabilities**



**Traffic Profile**



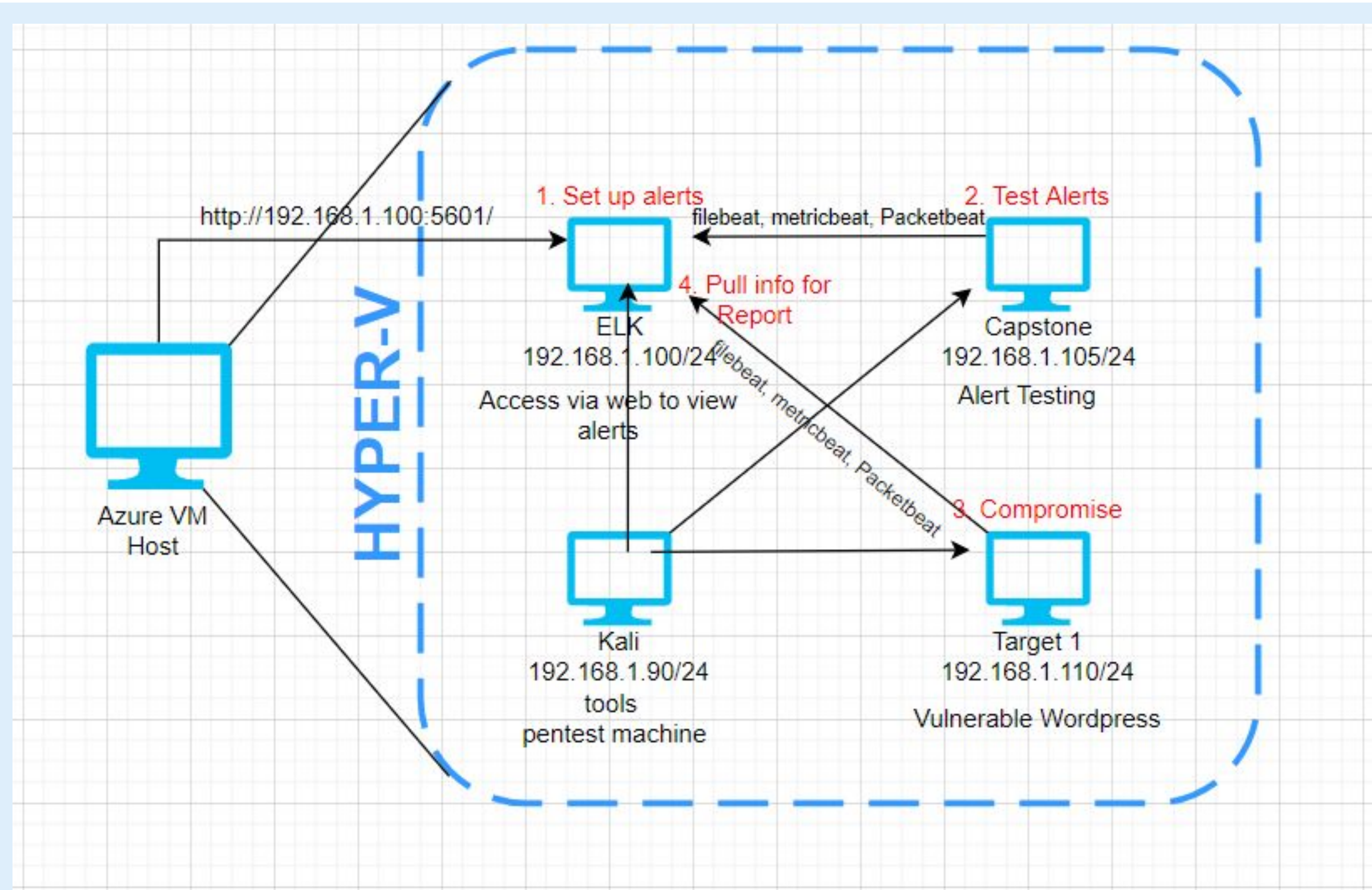
**Normal Activity**



**Malicious Activity**

# Network Topology & Critical Vulnerabilities

# Network Topology



## Network

Address

Range:192.168.1.0/24

Netmask:255.255.255.0

Gateway:

## Machines

IPv4: 192.168.1.100/24

OS: Ubuntu 18.04.4

Hostname: ELK

IPv4:192.168.1.105/24

OS: Ubuntu 18.04.1

Hostname:Capstone

IPv4:192.168.1.90/24

OS: Kali GNU/Linux

2020.1

Hostname:Kali

IPv4:192.168.1.110/24

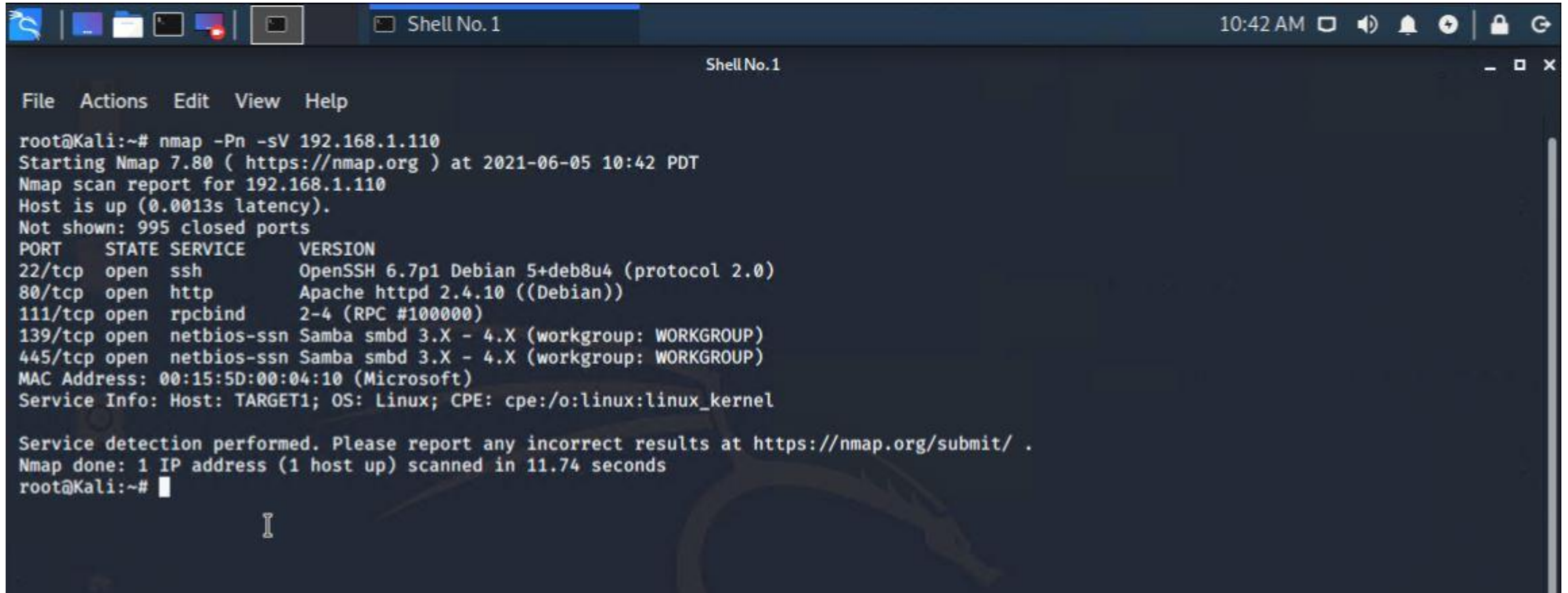
OS: Debian GNU/Linux 8

Hostname: Target 1



# Exposed Services: Target 1

## Nmap Scan :



```
root@Kali:~# nmap -Pn -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-05 10:42 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0013s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.74 seconds
root@Kali:~#
```

# Exposed Services: Target 1

---

Our assessment uncovered the following critical Exposed Services in **Target 1**.

Vulnerability	Description	Impact
Port 22 : Open	Provides access to SSH into target machine.	If credentials are discovered or cracked could allow for external access.
Port 80 : Open	Provides access to unencrypted packets.	Can provide direct access to the http server / web browser.

# Critical Vulnerabilities: Target 1

---

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

Vulnerability	Description	Impact
Weak Password Policy	We were able to guess user michael's password on our first attempt. It was his username.	This provided access to SSH directly into the system with no resistance.
CVE-2017-3167	Apache versions before 2.4.26 allows for the use of use of : <code>ap_get_basic_auth_pw()</code> to bypass authentication requirements.	Potentially allows for escalation for an attacker if access established.
CVE-2014-3583	Apache version 2.4.10 is vulnerable to DOS attacks via buffer-over-read from long response headers.	This provides an easy target for DOS attacks and may affect availability of a system if exploited.



# Critical Vulnerabilities: Target 1

---

Continuation of critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
CVE-2016-0777	In OpenSSH Version prior to 7.1p2, entire buffers from system memory can be requested remotely, allowing sensitive information to become compromised.	This may impact Confidentiality of data if used as an attack vector.
CVE-2016-6210	In OpenSSH prior to 7.3, users can enumerate user credentials by leveraging timing differences in response times when a large password is employed. A different form of hashing (Blowfish instead of SHA256 or SHA512) is used when a User does not exist.	The enumeration of users combined with a potentially weak password policy could allow easy access to malicious actors.
CVE-2015-8325	In OpenSSH through 7.2p2, under certain conditions, users can easily gain privileges by triggering a crafted environment for the /bin/login program.	This would potentially be an avenue for a malicious actor, who has gained access, to escalate the privileges of a user that has been compromised.



# Critical Vulnerabilities: Target 1

## WP Scan :

```
[+] URL: http://192.168.1.110/wordpress/
[+] Started: Sat Jun 5 10:11:20 2021

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
| Interesting Entry: Server: Apache/2.4.10 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] http://192.168.1.110/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://192.168.1.110/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] http://192.168.1.110/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.17 identified (Latest, released on 2021-05-13).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.17'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.17'
```



# Critical Vulnerabilities: Target 1

---

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

Vulnerability	Description	Impact
WordPress XMLRPC GHOST Vulnerability Scanner CVE-2015-0235	Determines hosts vulnerable to the GHOST vulnerability via a call to the WordPress XMLRPC Interface	If target is vulnerable, the system will segfault and return a server error
Wordpress XMLRPC DoS CVE-2014-5266	Wordpress XMLRPC parsing is vulnerable to a XML based denial of service	This vulnerability affects Wordpress 3.5-3.9.2 (3.8.4 and 3.7.4 are also patched)
Wordpress XML-RPC Username/Password Login Scanner CVE-1999-0502	attempts to authenticate against a Wordpress-site (via XMLRPC) using username and password combinations indicated by the USER_FILE, PASS_FILE, and USERPASS_FILE options.	Can provide Login access
Wordpress Pingback Locator CVE-2013-0235	This module will scan for wordpress sites with the Pingback API enabled.	By interfacing with the API an attacker can cause the wordpress site to port scan an external target and return results

# 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 (45M Bytes) 166.62.111.64 (16M Bytes) 185.243.115.84 (26M Bytes)	Machines that sent the most traffic.
Most Common Protocols	UDP TCP TLSv1.2	Three most common protocols on the network.
# of Unique IP Addresses	808	Count of observed IP addresses.
Subnets	24-bit Block	Observed subnet ranges.
# of Malware Species	1 Trojan (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**

- Visiting web URLs
- Viewing pictures
- Social media

### **Suspicious Activity**

- “Time Thieves” are wasting company time by watching YouTube Videos.
- Creation of a personal web server on the corporate Network: Frank-n-Ted.com
- Malware Downloaded onto Machine (10.6.12.203). The Malware downloaded, June11.d11, was determined to be a Trojan Horse.
- Downloaded Torrent File: Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent. (The company has a strict policy on copyright infringement.)

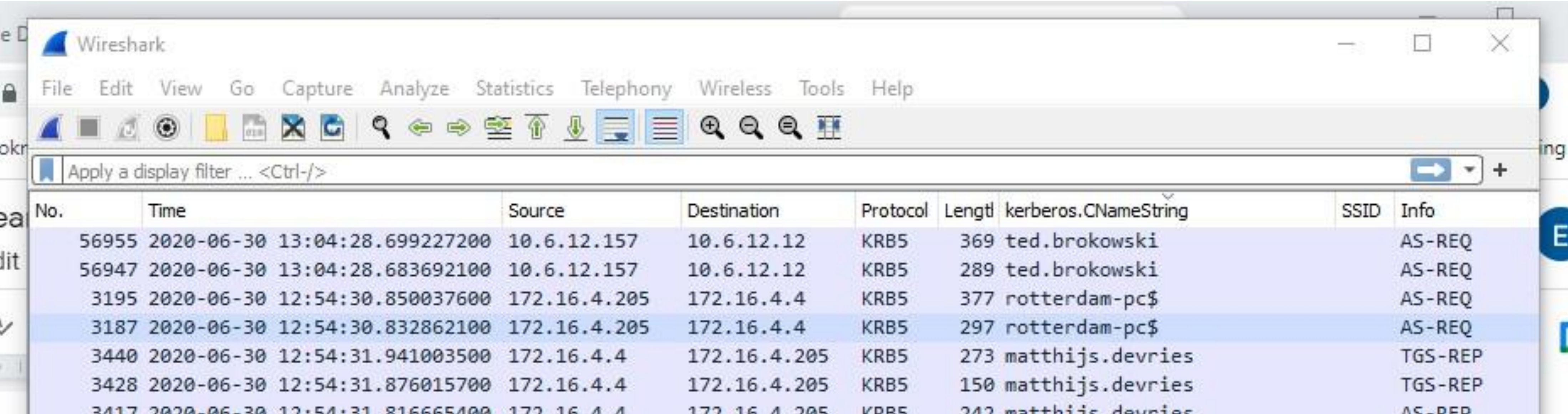


Normal Activity



# Normal Behaviors

## Identified users who are participating in non-malicious traffic

A screenshot of the Wireshark network protocol analyzer interface. The main display area shows a list of captured packets. The selected packet is number 3187, a Kerberos AS-REQ from 172.16.4.205 to 172.16.4.4. The packet details pane on the right shows the 'kerberos.CNameString' field with the value 'rotterdam-pc\$'. The packet bytes pane is empty. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The status bar at the bottom shows 'Apply a display filter ... <Ctrl-/>'.

No.	Time	Source	Destination	Protocol	Length	kerberos.CNameString	SSID	Info
56955	2020-06-30 13:04:28.699227200	10.6.12.157	10.6.12.12	KRB5	369	ted.brokowski		AS-REQ
56947	2020-06-30 13:04:28.683692100	10.6.12.157	10.6.12.12	KRB5	289	ted.brokowski		AS-REQ
3195	2020-06-30 12:54:30.850037600	172.16.4.205	172.16.4.4	KRB5	377	rotterdam-pc\$		AS-REQ
3187	2020-06-30 12:54:30.832862100	172.16.4.205	172.16.4.4	KRB5	297	rotterdam-pc\$		AS-REQ
3440	2020-06-30 12:54:31.941003500	172.16.4.4	172.16.4.205	KRB5	273	matthijs.devries		TGS-REP
3428	2020-06-30 12:54:31.876015700	172.16.4.4	172.16.4.205	KRB5	150	matthijs.devries		TGS-REP
3417	2020-06-30 12:54:31.816665400	172.16.4.4	172.16.4.205	KRB5	242	matthijs.devries		AS-REQ

User	Ip Addr of Device	Protocol	Website	Description
ted.brokowski	10.6.12.157	HTTP	<a href="https://cardboardspaceshiptoy.com">cardboardspaceshiptoy.com</a>	Viewing an invoice
matthijs.devries	172.16.4.205	HTTP	<a href="https://mysocalledchaos.com">mysocalledchaos.com</a>	Surfing the web
		HTTP	<a href="https://green.mattingsolutions.co">green.mattingsolutions.co</a>	Downloading wallpaper image
candice.tucker	10.11.11.203	HTTP	<a href="https://acjabogados.com/">https://acjabogados.com/</a>	Surfing the web
brandon.gilbert	10.11.11.200	HTTP	<a href="https://www.vinylmeplease.com">www.vinylmeplease.com</a>	Surfing the web
frank.brokowski	10.6.12.203			abnormal - Getting june11
elmer.blanco	10.0.0.201			abnormal - watching movies , animations, torrents



# Viewing an invoice by ted.brokowski

ip.addr==10.6.12.157

No.	Time	Source	Destination	Protocol	Length	kerberos.CNameString	Information
57173	2020-06...	10.6.12.157	224.0.0.22	IGMPv3	54		Membership Report / Join group 239.
55428	2020-06...	10.6.12.157	224.0.0.22	IGMPv3	62		Membership Report / Join group 224.
55424	2020-06...	10.6.12.157	224.0.0.22	IGMPv3	54		Membership Report / Join group 224.
55423	2020-06...	10.6.12.157	224.0.0.22	IGMPv3	54		Membership Report / Leave group 224.
55422	2020-06...	10.6.12.157	224.0.0.22	IGMPv3	54		Membership Report / Join group 224.
55421	2020-06...	10.6.12.157	224.0.0.22	IGMPv3	54		Membership Report / Join group 224.
57913	2020-06...	172.93.120.242	10.6.12.157	HTTP	561		HTTP/1.1 302 Found (text/html)
57901	2020-06...	10.6.12.157	172.93.120.242	HTTP	513		GET /logs/invoice-86495.doc HTTP/1.
58540	2020-06...	10.6.12.12	10.6.12.157	EPM	226		Map response, DRSUAPI, 32bit NDR
58539	2020-06...	10.6.12.157	10.6.12.12	EPM	222		Map request, DRSUAPI, 32bit NDR
58523	2020-06...	10.6.12.12	10.6.12.157	EPM	226		Map response, DRSUAPI, 32bit NDR
58522	2020-06...	10.6.12.157	10.6.12.12	EPM	222		Map request, DRSUAPI, 32bit NDR
58306	2020-06...	10.6.12.12	10.6.12.157	EPM	226		Map response, DRSUAPI, 32bit NDR
58305	2020-06...	10.6.12.157	10.6.12.12	EPM	222		Map request, DRSUAPI, 32bit NDR
58289	2020-06...	10.6.12.12	10.6.12.157	EPM	226		Map response, DRSUAPI, 32bit NDR
58288	2020-06...	10.6.12.157	10.6.12.12	EPM	222		Map request, DRSUAPI, 32bit NDR
57004	2020-06...	10.6.12.12	10.6.12.157	EPM	226		Map response, DRSUAPI, 32bit NDR
57003	2020-06...	10.6.12.157	10.6.12.12	EPM	222		Map request, DRSUAPI, 32bit NDR
56013	2020-06...	10.6.12.12	10.6.12.157	EPM	226		Map response, DRSUAPI, 32bit NDR

Wireshark · Packet 57901 · part\_3.pcapng

> Internet Protocol Version 4, Src: 10.6.12.157, Dst: 172.93.120.242

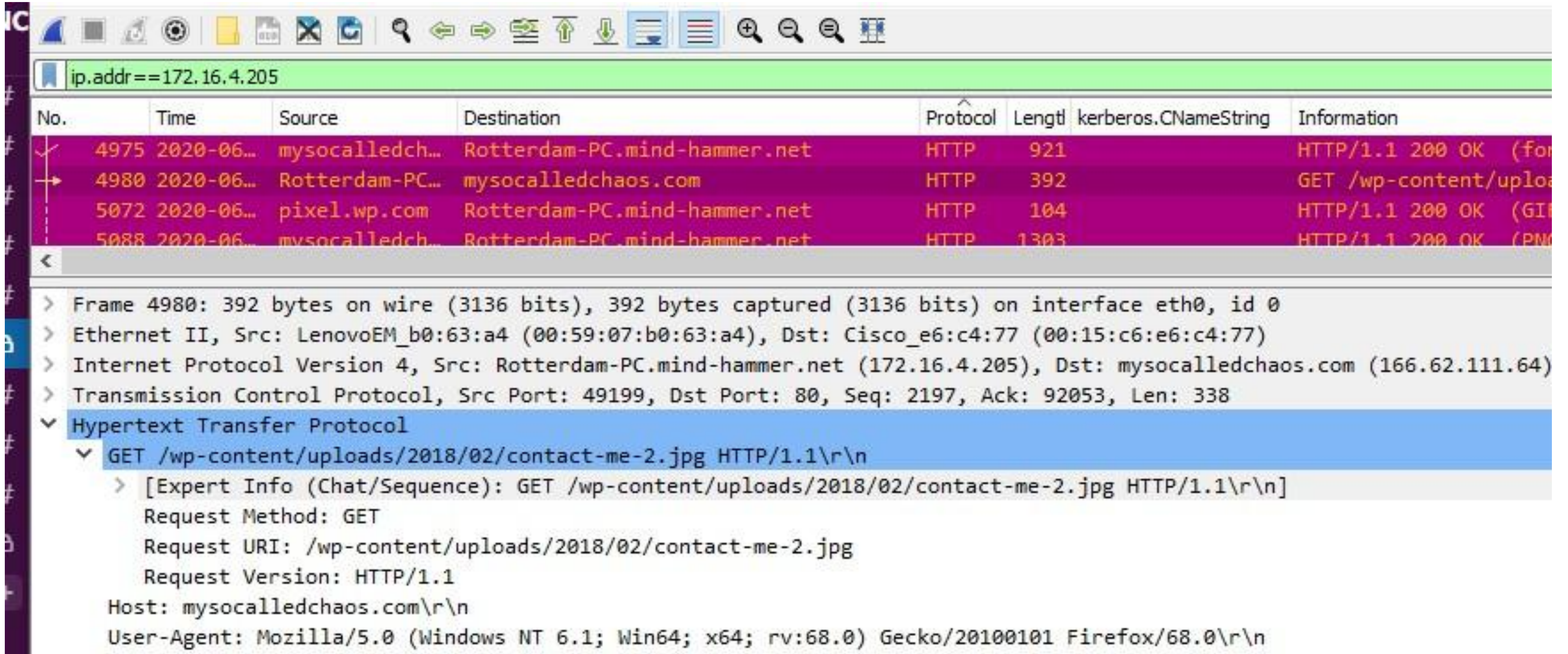
> Transmission Control Protocol, Src Port: 49728, Dst Port: 80, Seq: 1, Ack: 1, Len: 459

> Hypertext Transfer Protocol

> GET /logs/invoice-86495.doc HTTP/1.1\r\nHost: cardboardspaceshiptoy.com\r\nConnection: keep-alive\r\n



# Surfing the web by matthijs.devries



The image shows a Wireshark packet capture interface. The top toolbar contains various icons for file operations, navigation, and analysis. Below the toolbar, a green filter bar displays the filter `ip.addr==172.16.4.205`. The main packet list pane shows four packets, with packet 4980 selected. The packet details pane on the right shows the structure of packet 4980, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing a GET request for `/wp-content/uploads/2018/02/contact-me-2.jpg` with various headers like Host, User-Agent, and Request Method.

No.	Time	Source	Destination	Protocol	Length	kerberos.CNameString	Information
✓ 4975	2020-06...	mysocalledch...	Rotterdam-PC.mind-hammer.net	HTTP	921		HTTP/1.1 200 OK (for
→ 4980	2020-06...	Rotterdam-PC...	mysocalledchaos.com	HTTP	392		GET /wp-content/uploa
5072	2020-06...	pixel.wp.com	Rotterdam-PC.mind-hammer.net	HTTP	104		HTTP/1.1 200 OK (GI
5088	2020-06...	mysocalledch...	Rotterdam-PC.mind-hammer.net	HTTP	1303		HTTP/1.1 200 OK (PM

<

- > Frame 4980: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface eth0, id 0
- > Ethernet II, Src: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco\_e6:c4:77 (00:15:c6:e6:c4:77)
- > Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: mysocalledchaos.com (166.62.111.64)
- > Transmission Control Protocol, Src Port: 49199, Dst Port: 80, Seq: 2197, Ack: 92053, Len: 338
- ▼ Hypertext Transfer Protocol
  - ▼ GET /wp-content/uploads/2018/02/contact-me-2.jpg HTTP/1.1\r\n
    - > [Expert Info (Chat/Sequence): GET /wp-content/uploads/2018/02/contact-me-2.jpg HTTP/1.1\r\n]Request Method: GETRequest URI: /wp-content/uploads/2018/02/contact-me-2.jpgRequest Version: HTTP/1.1Host: mysocalledchaos.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n



# Downloading wallpaper image by matthijs.devries

The image shows a Wireshark packet capture window. The filter bar at the top displays the filter `ip.addr==172.16.4.205`. The packet list pane shows six packets, all of which are HTTP POST requests originating from 172.16.4.205. The first packet (No. 26139) is a POST to http://31.7.62.214. The second (No. 27702) is a POST to /empty.gif on 185.243.115.84. The third (No. 27704) is an HTTP/1.1 200 OK response from 185.243.115.84 to 172.16.4.205. The fourth (No. 28546) is a POST to http://31.7.62.214. The fifth (No. 31329) is a POST to http://31.7.62.214. The sixth (No. 31721) is a POST to /empty.gif on 185.243.115.84. The packet details pane for the selected packet (No. 27702) shows the HTTP structure, including the status line 200 OK and the Content-Type application/javascript.

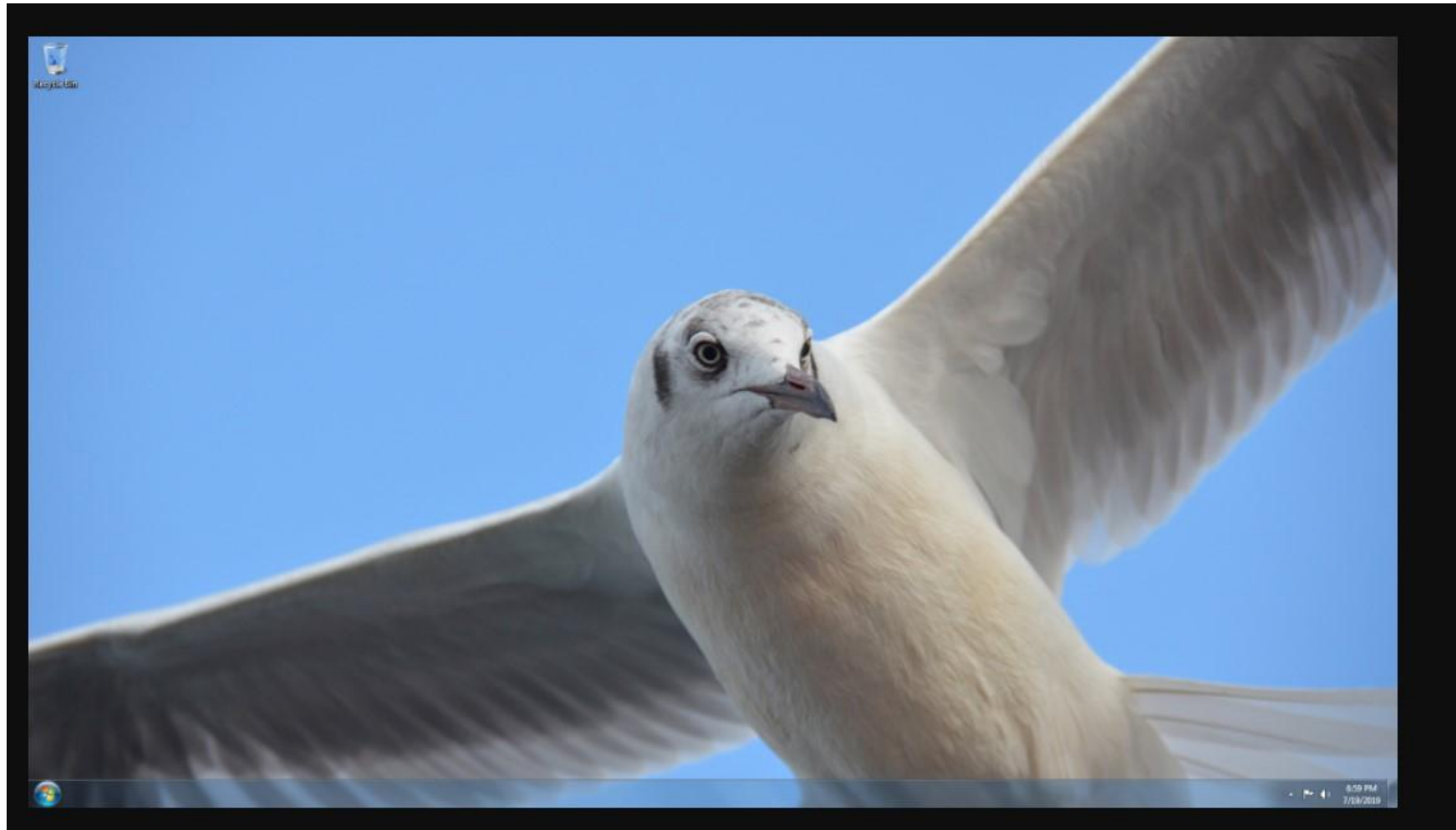
No.	Time	Source	Destination	Protocol	Length	kerberos.CNameString	Information
26139	2020-06...	172.16.4.205	31.7.62.214	HTTP	282		POST http://31.7.62.214
27702	2020-06...	172.16.4.205	185.243.115.84	HTTP	496		POST /empty.gif
27704	2020-06...	185.243.115.84	172.16.4.205	HTTP	341		HTTP/1.1 200 OK
28546	2020-06...	172.16.4.205	31.7.62.214	HTTP	282		POST http://31.7.62.214
31329	2020-06...	172.16.4.205	31.7.62.214	HTTP	282		POST http://31.7.62.214
31721	2020-06...	172.16.4.205	185.243.115.84	HTTP	1366		POST /empty.gif

```
> Request URI: /empty.gif?ss&sslimg
Request Version: HTTP/1.1
Accept: */*\r\n
Accept-Language: en-US\r\n
Age: 911068f789126eb9\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729)\r\n
Host: b5689023.green.mattingsolutions.co\r\n
> Content-Length: 3592206\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://b5689023.green.mattingsolutions.co/empty.gif?ss&sslimg]
[HTTP request 4/5]
```



# Downloading wallpaper image by matthijs.devries

---





# Surfing the web by candice.tucker

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

ip.addr==10.11.11.203

No.	Time	Source	Destination	Protocol	Length	kerberos.CNameString	Information
35903	2020-06...	okay-boomer-...	Tucker-Win7-PC.okay-boomer.info	EPM	226		Map response, DRSUAPI, 32bit NDR
45039	2020-06...	Tucker-Win7-...	okay-boomer-dc.okay-boomer.info	EPM	222		Map request, LSARPC, 32bit NDR
45040	2020-06...	okay-boomer-...	Tucker-Win7-PC.okay-boomer.info	EPM	226		Map response, LSARPC, 32bit NDR
43967	2020-06...	Tucker-Win7-...	acjabogados.com	HTTP	368		GET /40group.tiff HTTP/1.1
44537	2020-06...	acjabogados...	Tucker-Win7-PC.okay-boomer.info	HTTP	1072		HTTP/1.1 200 OK (image/tiff)
34329	2020-06...	Tucker-Win7-...	igmp.mcast.net	IGMPv3	60		Membership Report / Join group 224.0.0.252 f
34331	2020-06...	Tucker-Win7-	igmp.mcast.net	IGMPv3	60		Membership Report / Join group 224.0.0.252 f

> Internet Protocol Version 4, Src: Tucker-Win7-PC.okay-boomer.info (10.11.11.203), Dst: acjabogados.com (188.95.248.71)

> Transmission Control Protocol, Src Port: 49196, Dst Port: 80, Seq: 1, Ack: 1, Len: 314

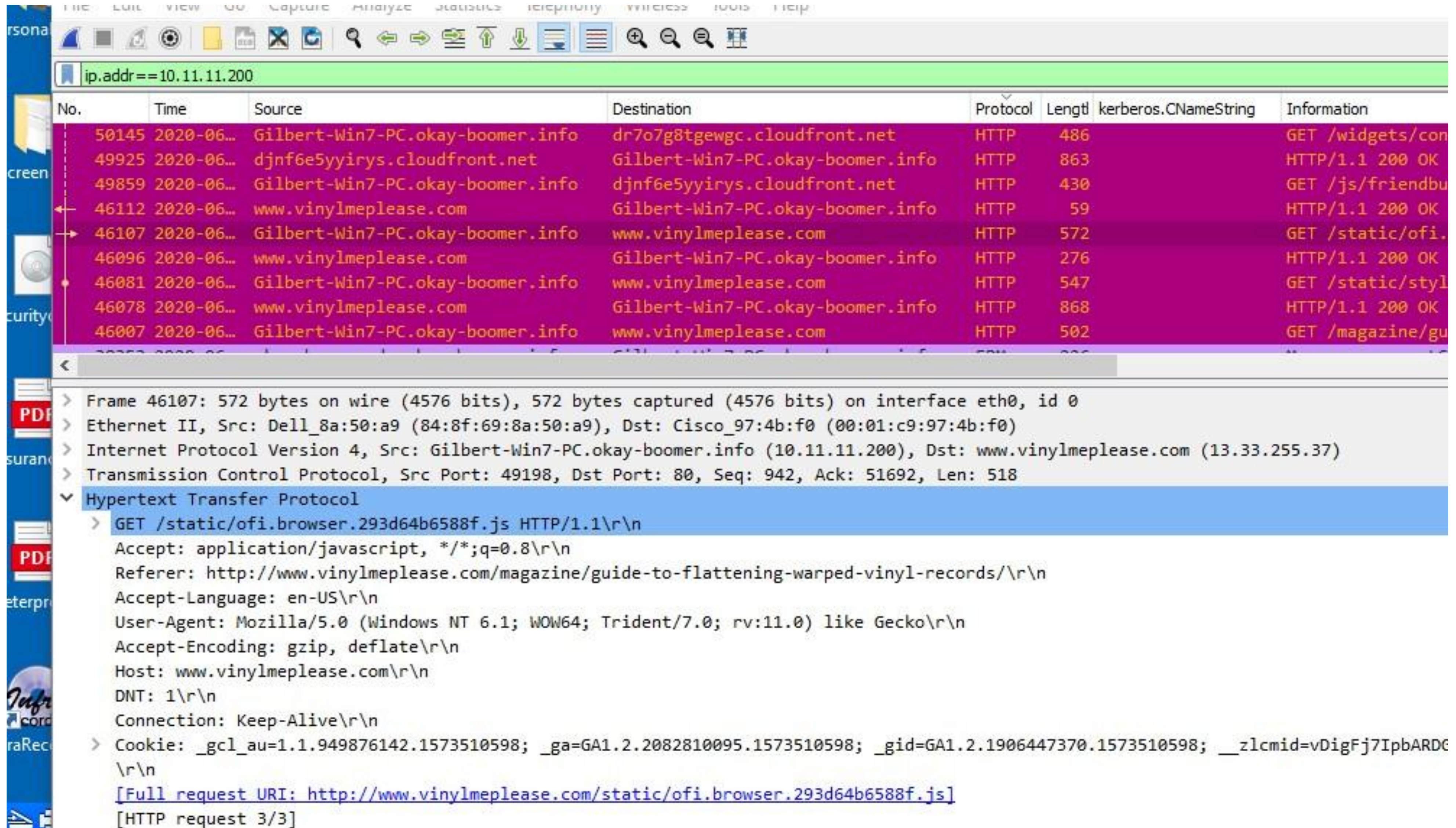
> Hypertext Transfer Protocol

> GET /40group.tiff HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /40group.tiff HTTP/1.1\r\nRequest Method: GETRequest URI: /40group.tiffRequest Version: HTTP/1.1Accept: \*/\*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.0...Host: acjabogados.com\r\nConnection: Keep-Alive\r\n\r\n[Full request URI: http://acjabogados.com/40group.tiff]



# Surfing the web by brandon.gilbert



The image shows a Wireshark network traffic capture. The top pane displays a list of network packets. The bottom pane shows the details of the selected packet (No. 46107).

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	kerberos.CNameString	Information
50145	2020-06...	Gilbert-Win7-PC.okay-boomer.info	dr7o7g8tgewgc.cloudfront.net	HTTP	486		GET /widgets/con
49925	2020-06...	djnf6e5yyirys.cloudfront.net	Gilbert-Win7-PC.okay-boomer.info	HTTP	863		HTTP/1.1 200 OK
49859	2020-06...	Gilbert-Win7-PC.okay-boomer.info	djnf6e5yyirys.cloudfront.net	HTTP	430		GET /js/friendbu
46112	2020-06...	www.vinylmeplease.com	Gilbert-Win7-PC.okay-boomer.info	HTTP	59		HTTP/1.1 200 OK
46107	2020-06...	Gilbert-Win7-PC.okay-boomer.info	www.vinylmeplease.com	HTTP	572		GET /static/ofi.
46096	2020-06...	www.vinylmeplease.com	Gilbert-Win7-PC.okay-boomer.info	HTTP	276		HTTP/1.1 200 OK
46081	2020-06...	Gilbert-Win7-PC.okay-boomer.info	www.vinylmeplease.com	HTTP	547		GET /static/styl
46078	2020-06...	www.vinylmeplease.com	Gilbert-Win7-PC.okay-boomer.info	HTTP	868		HTTP/1.1 200 OK
46007	2020-06...	Gilbert-Win7-PC.okay-boomer.info	www.vinylmeplease.com	HTTP	502		GET /magazine/gu

**Packet Details (Frame 46107):**

- Frame 46107: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits) on interface eth0, id 0
- Ethernet II, Src: Dell\_8a:50:a9 (84:8f:69:8a:50:a9), Dst: Cisco\_97:4b:f0 (00:01:c9:97:4b:f0)
- Internet Protocol Version 4, Src: Gilbert-Win7-PC.okay-boomer.info (10.11.11.200), Dst: www.vinylmeplease.com (13.33.255.37)
- Transmission Control Protocol, Src Port: 49198, Dst Port: 80, Seq: 942, Ack: 51692, Len: 518
- Hypertext Transfer Protocol
  - GET /static/ofi.browser.293d64b6588f.js HTTP/1.1\r\n
  - Accept: application/javascript, \*/\*;q=0.8\r\n
  - Referer: http://www.vinylmeplease.com/magazine/guide-to-flattening-warped-vinyl-records/\r\n
  - Accept-Language: en-US\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Host: www.vinylmeplease.com\r\n
  - DNT: 1\r\n
  - Connection: Keep-Alive\r\n
  - Cookie: \_gcl\_au=1.1.949876142.1573510598; \_ga=GA1.2.2082810095.1573510598; \_gid=GA1.2.1906447370.1573510598; \_\_zlcmid=vDigFj7IpbARDC\r\n
  - [Full request URI: http://www.vinylmeplease.com/static/ofi.browser.293d64b6588f.js]
  - [HTTP request 3/3]



# Surfing the web by frank.brokowski

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

ip.addr==10.6.12.203

No.	Time	Source	Destination	Protocol	Length	kerberos.CNameString	Information
59689	2020-06...	LAPTOP-5WKHX...	snnmnkxdhflwgthqismb.com	HTTP	749		POST /post.php HTTP/1.1
59682	2020-06...	snnmnkxdhflw...	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	436		HTTP/1.1 200 OK (text/html)
59680	2020-06...	LAPTOP-5WKHX...	snnmnkxdhflwgthqismb.com	HTTP	713		POST /post.php HTTP/1.1
59388	2020-06...	205.185.125....	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	946		HTTP/1.1 200 OK
58752	2020-06...	LAPTOP-5WKHX...	205.185.125.104	HTTP	312		GET /files/june11.dll HTTP/1.1
58750	2020-06...	205.185.125....	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	542		HTTP/1.1 302 Found
58748	2020-06...	LAPTOP-5WKHX...	205.185.125.104	HTTP	275		GET /pQBtWj HTTP/1.1
65147	2020-06...	Frank-n-Ted-...	LAPTOP-5WKHX9YG.frank-n-ted.com	EPM	226		Map response, DRSUAPI, 32bit NDR
65146	2020-06...	LAPTOP-5WKHX...	Frank-n-Ted-DC.frank-n-ted.com	EPM	222		Map request, DRSUAPI, 32bit NDR

<

> 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, Dst Port: 80, Seq: 222, Ack: 489, Len: 258

> Hypertext Transfer Protocol

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

> [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\nRequest Method: GETRequest URI: /files/june11.dllRequest Version: HTTP/1.1Accept: \*/\*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\nHost: 205.185.125.104\r\nConnection: Keep-Alive\r\nCookie: \_subid=3mmhfnd8jp\r\n



# Malicious Activity

# Trojan Horse

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)? Traffic from 10.6.12.203 and the web domain 205.185.125.104; Hypertext transfer Protocol
- What, specifically, was the user doing? Which site were they browsing? Etc. The user requested to download june11.dll from IP 205.185.125.104

The image shows a Wireshark packet capture window with the filter `http.request.method==GET and ip.addr==10.6.12.203`. The packet list shows two HTTP GET requests from `LAPTOP-5WKHX9YG.fra...` to `205.185.125.104`. The first request is for `/pQBtWj` (275 bytes) and the second is for `/files/june11.dll` (312 bytes). The packet details for the second request are expanded, showing the Hypertext Transfer Protocol section with the following fields:

```
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=3mmhfd8jp\r\n
\r\n
```

The full request URI is `http://205.185.125.104/files/june11.dll`. The packet is also shown in the packet bytes panel with the following details:

```
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=3mmhfd8jp\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]
```



# Continued

## Virustotal.com & Whatismyip.com

53

69

?

Community Score

✓

53 security vendors flagged this file as malicious

Refresh

Details

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB

2021-06-05 03:21:09 UTC

2 days ago

DLL

June11.dll

invalid-signature overlay pedll signed

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 2

Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	Trojan.Win32.Yakes.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy.Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	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.34722.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware1	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)

Status: Running

ASN: 53667 ?

ISP: Frantech Solutions

Host Name: 205.185.125.104

McAfee WebAdvisor

Website status: Suspicious

http://205.185.125.104/

This site looks a little risky to us, so we flagged it just in case. Make sure you trust this site if you choose to proceed. Better safe than sorry!

PUPs

Get colour-coded search results

Visit anyway

Go back

Choosing to visit anyway will add the blocked URL to your list of trusted sites.

# Continued

---

**Two users have created their own web server on the corporate network.**

**Risks associated with loose user restrictions:**

1. Unrestricted User Access Can Lead to Accidental Data Exposure
2. User Access Can Lead to Intentional Privilege Misuse & Abuse
  - a. i.e. two employees were watching youtube
3. Hackers Can Use Compromised User Credentials
  - a. i.e. A malicious files was downloaded infecting anyone that downloaded it.

**Giving employees and contractors unrestricted user permissions and user access could spell disaster for many businesses because doing so creates unnecessary cybersecurity risks.**

**Best Prevention Practices:**

- Check the existing roles to see if they meet your needs
- Make a duplicate of an existing role, then add or remove permissions as needed
- Test your customized role to ensure it behaves as expected
- Assign your custom role to users



# [Torrent Download]

---

- What kind of traffic did you observe? Which protocol(s)? Traffic between ip 10.0.0.201 and web domains; Hyper Text Transfer Protocol - HTTP
- What, specifically, was the user doing? Which site were they browsing? Etc. The user (elmer.blanco) was downloading the torrent from a website: <http://publicdomaintorrents.com>
- Include screenshots of packets justifying your conclusions.
- Include a description of any interesting files. "Betty\_Boop\_Rhythm\_on\_the\_Reservation" which is a torrent downloaded, which is prohibited from the company's policy.

```
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
      [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on
        [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
        [Severity level: Chat]
        [Group: Sequence]
```



# Torrent Download Continued..

---



**X-CORP's Security team does not forbid the use of torrents for legitimate purposes. However, this one may go against their policy on copyright infringement.**

Risks associated with Torrent Download:

- A good portion of the files available through P2P networks contain copyrighted materials, making this illegal.
- Downloading Torrents are far less safe than most think.
  - Most torrents are a big target for Hackers to use to compromise a system or network.
  - They can easily disguise Malware with a more desirable name to trick someone into infecting their system with this.
- It is best practice to only download authorized Torrents, pertinent to getting the job done from a known trusted source, and still scanning for Malware before downloading.

# The End

