

Network Analysis

Time Thieves

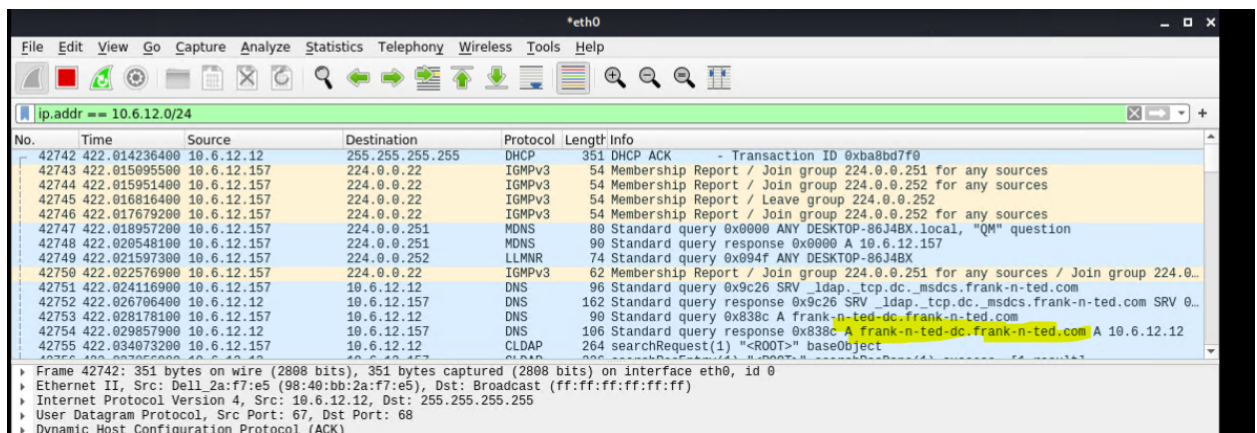
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

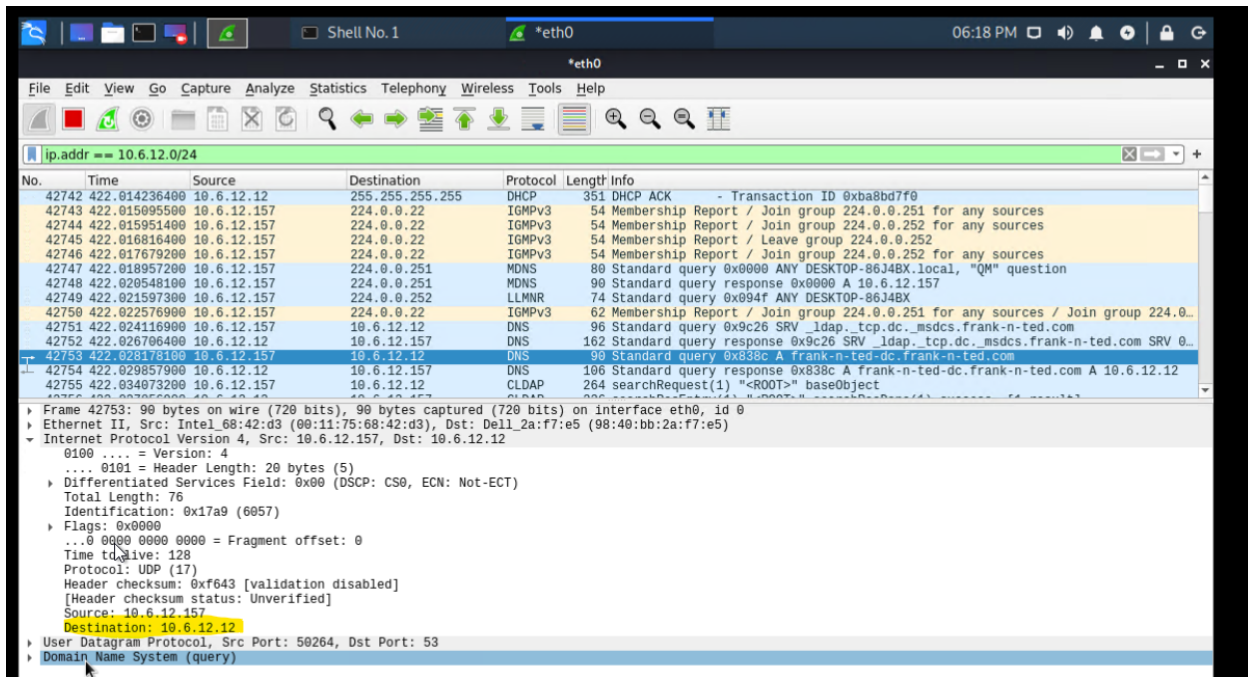
frank-n-ted-dc.frank-n-ted.com



No.	Time	Source	Destination	Protocol	Length	Info
42742	422.014236400	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
42743	422.015095500	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
42744	422.015951400	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
42745	422.016816400	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
42746	422.017679200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
42747	422.018957200	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
42748	422.020548100	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
42749	422.021597300	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
42750	422.022576900	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group 224.0...
42751	422.024116900	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
42752	422.026706400	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com SRV 0...
42753	422.028178100	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
42754	422.029857900	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.12.12
42755	422.034073200	10.6.12.157	10.6.12.12	LDAP	264	searchRequest(1) "<R00T>" baseObject

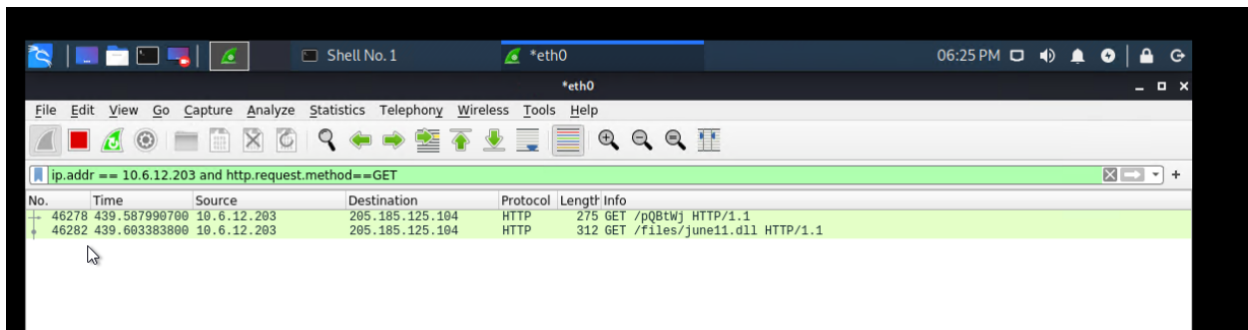
2. What is the IP address of the Domain Controller (DC) of the AD network?

10.6.12.12 (frank-n-ted-dc.frank-n-ted.com)




3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

june11.dll







4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

June11.dll is a Trojan.



d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec



Sign in

Sign up



50

/ 67

?

Community Score

50 security vendors and 1 sandbox flagged this file as malicious



d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleupdate.exe


invalid-signature overlay pedll signed spreader

549.84 KB

Size

2022-06-08 03:13:19 UTC

1 minute ago



DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
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.34712.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.Inject3.53106	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Mint.Zamg.O (B)	eScan	Trojan.Mint.Zamg.O
ESET-NOD32	Win32/Spy.Zbot.ADI	Fortinet	W32/Kryptik.DZZltr
GData	Trojan.Mint.Zamg.O	Ikarus	Trojan.Win32.Generic
Jiangmin	Trojan.Yakes.afpe	K7AntiVirus	Trojan (0056893e1)
K7GW	Trojan (0056893e1)	Kaspersky	HEUR:Trojan.Win32.Yakes.pef
Lionic	Trojan.Win32.Yakes.4lc	Malwarebytes	Trojan.Banker
MAX	Malware (ai Score=89)	MaxSecure	Trojan.Malware.102312674.susgen
McAfee	GenericRXLA-ESI2545B1548316	McAfee-GW-Edition	GenericRXLA-ESI2545B1548316
Microsoft	Ransom.Win32/Locky	NANO-Antivirus	Trojan.Win32.Yakes.hnopte
Palo Alto Networks	Generic.ml	Panda	Trj/GdSda.A
Rising	Trojan.Kryptik1.C7EF (CLASSIC)	Sangfor Engine Zero	Trojan.Win32.Save.a

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:
 - Host name: **ROTTERDAM-PC**
 - IP address: **172.16.4.4**

- MAC address: **00:59:07:b0:63:a4**

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Shell No. 1 project 3.pcapng 08:26 PM

project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==172.16.4.4 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
17185	242.548747400	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
17576	243.990284100	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP
56908	574.361690600	172.16.4.4	172.16.4.205	KRB5	204	AS-REP
56920	574.424925900	172.16.4.4	172.16.4.205	KRB5	219	TGS-REP
56965	574.665998400	172.16.4.4	172.16.4.205	KRB5	158	TGS-REP
56985	574.772316300	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP
57093	575.167164900	172.16.4.4	172.16.4.205	KRB5	204	AS-REP
57105	575.227786900	172.16.4.4	172.16.4.205	KRB5	130	TGS-REP
57132	575.310017400	172.16.4.4	172.16.4.205	KRB5	242	AS-REP
57143	575.369361400	172.16.4.4	172.16.4.205	KRB5	150	TGS-REP
57155	575.434374400	172.16.4.4	172.16.4.205	KRB5	273	TGS-REP
68241	732.475469300	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
68252	732.532578000	172.16.4.4	172.16.4.205	KRB5	72	TGS-REP

Frame 17185: 206 bytes on wire (1648 bits), 206 bytes captured (1648 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: 172.16.4.4, Dst: 172.16.4.205

Transmission Control Protocol, Src Port: 88, Dst Port: 49265, Seq: 1461, Ack: 1633, Len: 152

[2 Reassembled TCP Segments (1612 bytes): #17184(1460), #17185(152)]

Kerberos

- Record Mark: 1608 bytes
- tgs-rep
 - pvno: 5
 - msg-type: krb-tgs-rep (13)
 - crealm: MIND-HAMMER.NET
 - cname
 - name-type: KRB5-NT-PRINCIPAL (1)
 - name-string: 1 item
 - CNameString: ROTTERDAM-PCS
 - ticket
 - enc-part

Frame (206 bytes) Reassembled TCP (1612 bytes)

CNameString: Character string

Packets: 106830 · Displayed: 13 (0.0%) Profile: Default

Status: Running

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Shell No. 1 project 3.pcapng 08:28 PM

project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==172.16.4.4 and kerberos.CNameString

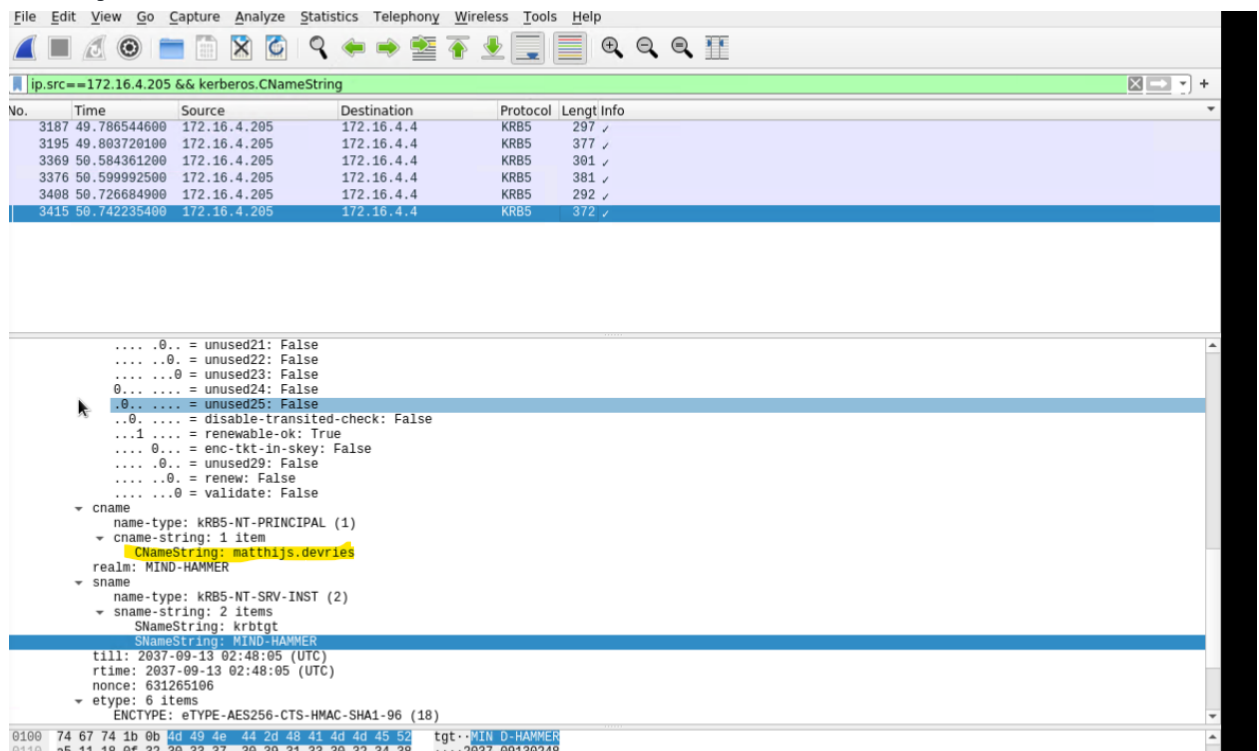
No.	Time	Source	Destination	Protocol	Length	Info
17185	242.548747400	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
17576	243.900284100	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP
56908	574.361690600	172.16.4.4	172.16.4.205	KRB5	204	AS-REP
56920	574.424925900	172.16.4.4	172.16.4.205	KRB5	219	TGS-REP
56965	574.665998400	172.16.4.4	172.16.4.205	KRB5	158	TGS-REP
56985	574.772316300	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP
57093	575.167164900	172.16.4.4	172.16.4.205	KRB5	204	AS-REP
57105	575.227786900	172.16.4.4	172.16.4.205	KRB5	130	TGS-REP
57132	575.310017400	172.16.4.4	172.16.4.205	KRB5	242	AS-REP
57143	575.369361400	172.16.4.4	172.16.4.205	KRB5	150	TGS-REP
57155	575.434374400	172.16.4.4	172.16.4.205	KRB5	273	TGS-REP
68241	732.475469300	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
68252	732.532578000	172.16.4.4	172.16.4.205	KRB5	72	TGS-REP

Frame 17185: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface eth0, id 0

- Interface id: 0 (eth0)
- Encapsulation type: Ethernet (1)
- Arrival Time: Jun 7, 2022 17:38:41.860593400 PDT
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1654648721.860593400 seconds
- [Time delta from previous captured frame: 0.003307600 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 242.548747400 seconds]
- Frame Number: 17185
- Frame Length: 206 bytes (1648 bits)
- Capture Length: 206 bytes (1648 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp:kerberos]
- [Coloring Rule Name: TCP]
- [Coloring Rule String: tcp]
- Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
 - Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
 - Source: Dell_19:49:50 (a4:ba:db:19:49:50)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205
- Transmission Control Protocol, Src Port: 88, Dst Port: 49265, Seq: 1461, Ack: 1633, Len: 152
- [2 Reassembled TCP Segments (1612 bytes): #17184(1460), #17185(152)]
- Kerberos

2. What is the username of the Windows user whose computer is infected?

Matthijs.devries



The image shows a Wireshark network capture of Kerberos traffic. The top pane displays a list of packets, all of which are Kerberos messages (protocol KRBS) between source IP 172.16.4.205 and destination IP 172.16.4.4. The bottom pane shows the detailed view of a selected Kerberos message (packet 3415). The message structure is as follows:

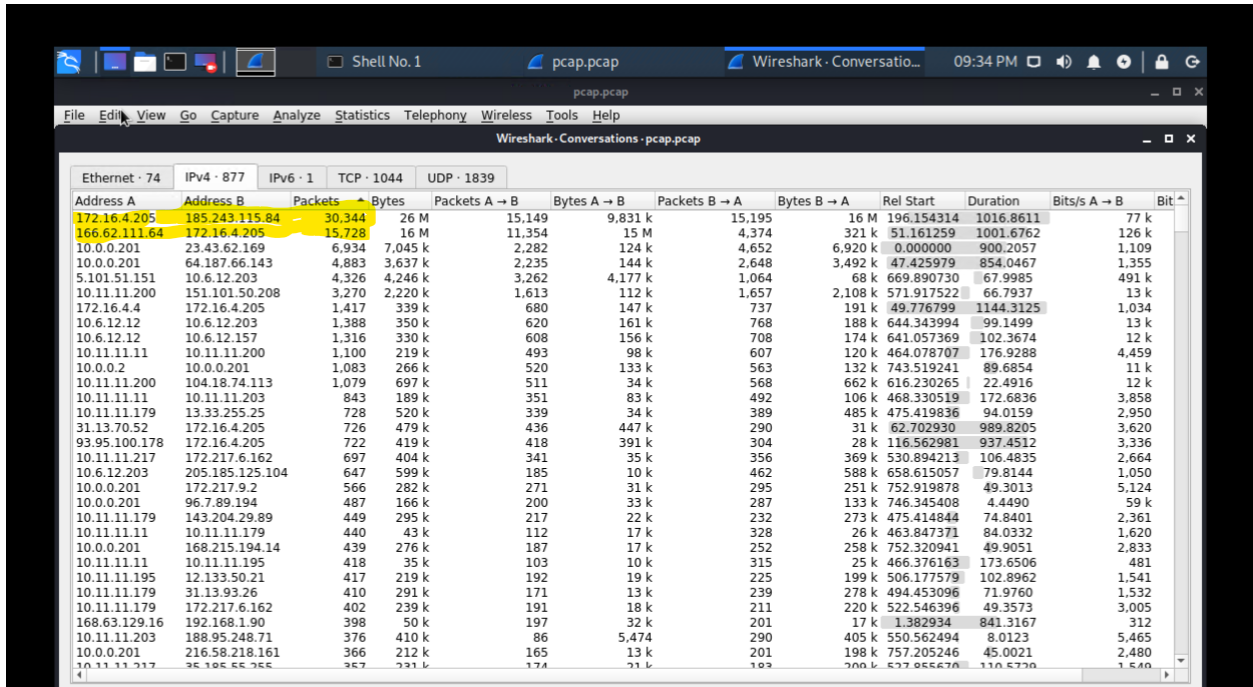
-0.. = unused21: False
-0.. = unused22: False
-0.. = unused23: False
- 0... .. = unused24: False
- .0.. = unused25: False
- ..0. = disable-transited-check: False
- ...1 = renewable-ok: True
- ... 0... = enc-tgt-in-skey: False
-0.. = unused29: False
-0.. = renew: False
-0.. = validate: False
- ▼ cname
 - name-type: kRB5-NT-PRINCIPAL (1)
 - ▼ cname-string: 1 item
 - CNameString: matthijs.devries
- realm: MIND-HAMMER
- ▼ sname
 - name-type: kRB5-NT-SRV-INST (2)
 - ▼ sname-string: 2 items
 - SNameString: krbtgt
 - SNameString: MIND-HAMMER
- till: 2037-09-13 02:48:05 (UTC)
- rtime: 2037-09-13 02:48:05 (UTC)
- nonce: 631265106
- ▼ etype: 6 items
 - ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)

The bottom of the detailed view shows the raw packet data in hexadecimal and ASCII format.

3. What are the IP addresses used in the actual infection traffic?

The conversation chart show that the IPs: 172.16.4.205, 185.243.115.84, 166.62.111.64 are the infected traffic due to the abnormal high number of packets in

comparison to the rest.



The image shows a Wireshark network traffic capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top status bar shows 'Shell No. 1', 'pcap.pcap', 'Wireshark - Conversatio...', and the time '09:34 PM'. The main window displays a list of network packets. The first two packets are highlighted in yellow:

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bit
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611	77 k	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762	126 k	

Illegal Downloads

- Find the following information about the machine with IP address 10.0.0.201 :
 - MAC address: **00:16:17:18:66:c8**
 - Windows username: **elmer.blanco**

c. OS version: **BLANCO-DESKTOP**

The image shows a Wireshark packet capture of a Kerberos AS-REQ. The packet list shows a packet from 10.0.0.201 to 10.0.0.2. The packet details show the following structure:

- Frame 67644: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface eth0, id 0
- Ethernet II, Src: Msi_18:66:c8 (08:16:17:18:66:c8), Dst: Dell_f4:3b:96 (08:12:3f:f4:3b:96)
- Destination: Dell_f4:3b:96 (08:12:3f:f4:3b:96)
- Source: Msi_18:66:c8 (08:16:17:18:66:c8)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.2
- Transmission Control Protocol, Src Port: 49745, Dst Port: 88, Seq: 1, Ack: 1, Len: 316
- Kerberos
 - Record Mark: 312 bytes
 - as-req
 - pvno: 5
 - msg-type: krb-as-req (10)
 - padata: 2 items
 - req-body
 - Padding: 0
 - kdc-options: 40810010
 - cname
 - name-type: kRB5-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: **elmer.blanco**
 - realm: DOGOFTHEYEAR
 - sname
 - name-type: kRB5-NT-SRV-INST (2)
 - sname-string: 2 items
 - SNameString: krbtgt
 - SNameString: DOGOFTHEYEAR

```

▼ cname
  name-type: kRB5-NT-PRINCIPAL (1)
  ▼ cname-string: 1 item
    CNameString: BLANCO-DESKTOP$
▼ ticket

```

2. Which torrent file did the user download?

a. Betty_Boop_Rythm_on_the_Reservation.avi.torrent

pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
69142	765.263272500	10.0.0.201	168.215.194.14	HTTP	471	
69150	765.279673000	10.0.0.201	172.217.9.2	HTTP	434	
69155	765.290109300	10.0.0.201	50.18.44.131	HTTP	412	
69167	765.416418700	10.0.0.201	168.215.194.14	HTTP	500	
69213	765.837950500	10.0.0.201	168.215.194.14	HTTP	465	
69298	766.857868300	10.0.0.201	52.94.240.125	HTTP	415	
69347	767.585292600	10.0.0.201	168.215.194.14	HTTP	531	
69434	768.625230500	10.0.0.201	52.94.240.125	HTTP	427	
69470	768.919511100	10.0.0.201	74.21.202.62	HTTP	885	
69542	769.560506300	10.0.0.201	52.94.233.131	HTTP	1067	
69706	770.366956400	10.0.0.201	168.215.194.14	HTTP	589	
69750	770.563257500	10.0.0.201	140.211.166.134	HTTP	195	
69754	770.572697300	10.0.0.201	91.189.95.21	HTTP	423	
69980	771.231145500	10.0.0.201	168.215.194.14	HTTP	434	

Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 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)

- Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
- Source: Msi_18:66:c8 (00:16:17:18:66:c8)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14

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_Reservation.avi.torrent HTTP/1.1\r\n]