

Network Analysis

Time Thieves

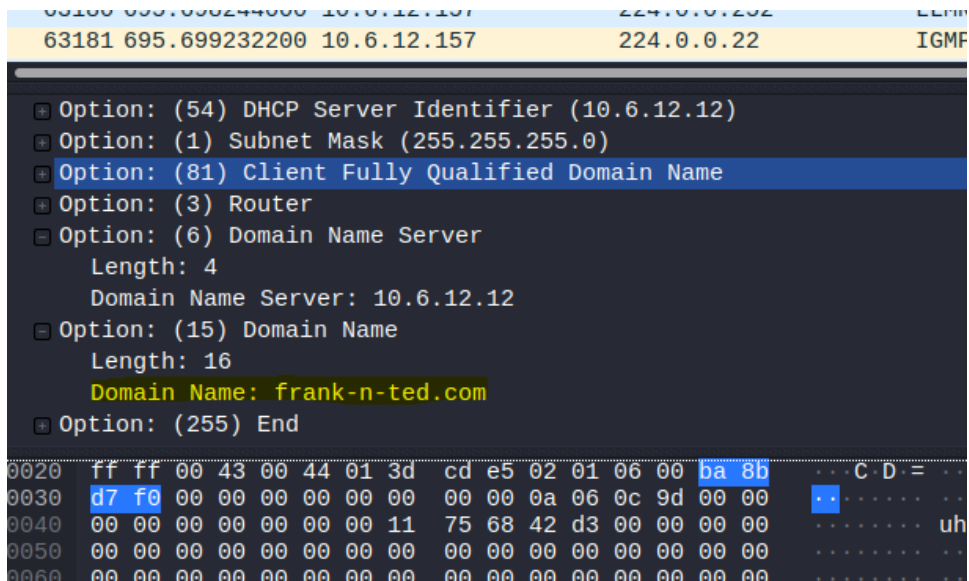
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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:

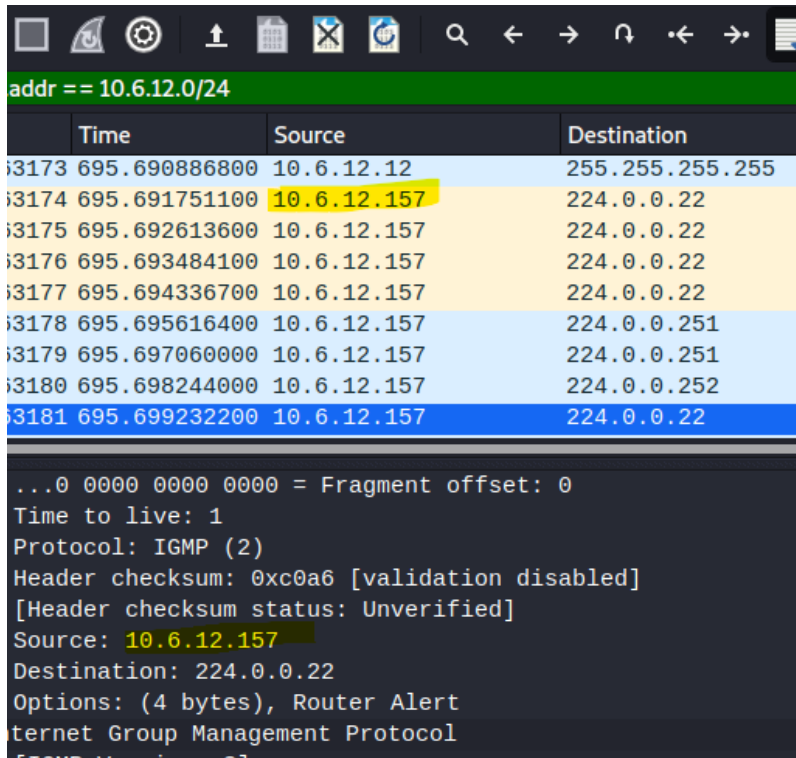
1. What is the domain name of the users' custom site?

Frank-n-ted.com



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

10.6.12.157



The image shows a Wireshark packet capture interface. At the top, a green filter bar displays 'addr == 10.6.12.0/24'. Below this is a table of captured packets. The selected packet is number 3181, an IGMPv2 message. The packet details pane shows the following information:

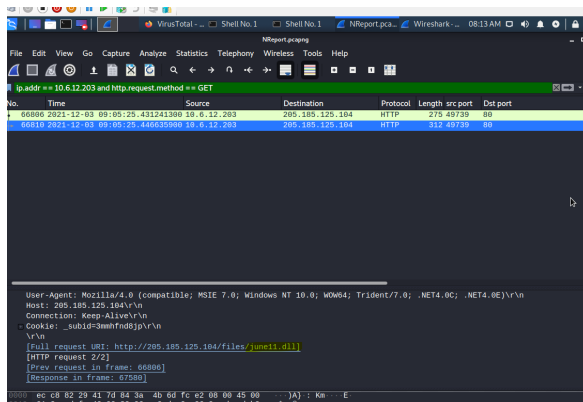
Time	Source	Destination
695.690886800	10.6.12.12	255.255.255.255
695.691751100	10.6.12.157	224.0.0.22
695.692613600	10.6.12.157	224.0.0.22
695.693484100	10.6.12.157	224.0.0.22
695.694336700	10.6.12.157	224.0.0.22
695.695616400	10.6.12.157	224.0.0.251
695.697060000	10.6.12.157	224.0.0.251
695.698244000	10.6.12.157	224.0.0.252
695.699232200	10.6.12.157	224.0.0.22

Packet 3181 details:

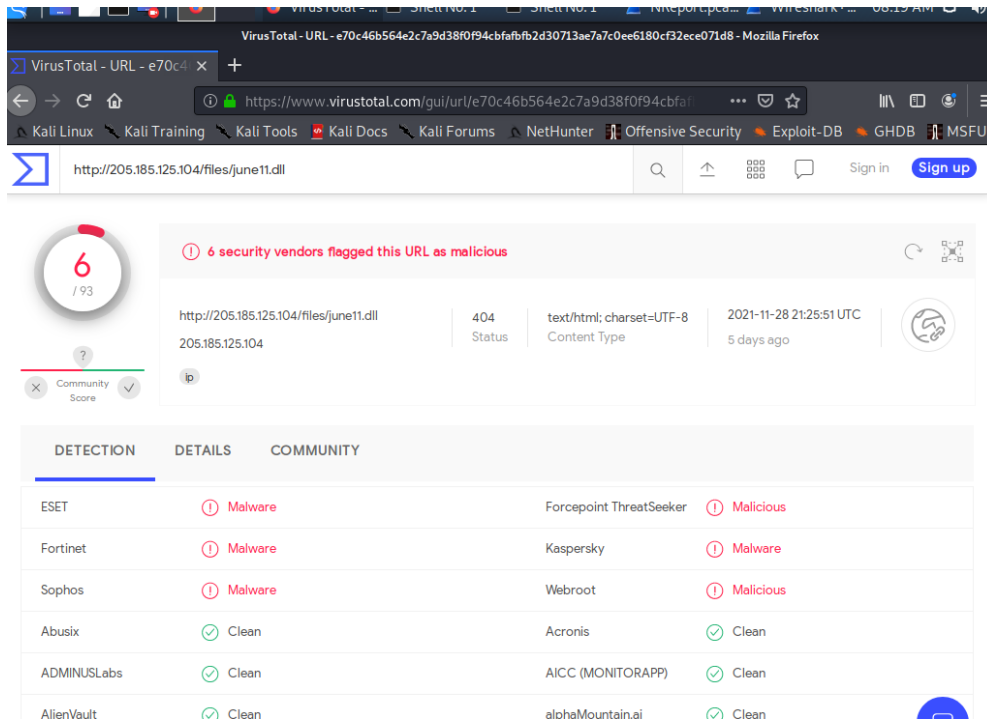
- ...0 0000 0000 0000 = Fragment offset: 0
- Time to live: 1
- Protocol: IGMP (2)
- Header checksum: 0xc0a6 [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.6.12.157
- Destination: 224.0.0.22
- Options: (4 bytes), Router Alert
- Internet Group Management Protocol
- Version: 2

- 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?



The screenshot shows the VirusTotal web interface. At the top, the browser address bar displays the URL: `https://www.virustotal.com/gui/url/e70c46b564e2c7a9d38f0f94cbfafb2d30713ae7a7c0ee6180cf32ece071d8`. Below the address bar, the file path `http://205.185.125.104/files/june11.dll` is shown. A circular badge on the left indicates a score of 6/93. A red banner states: "6 security vendors flagged this URL as malicious". Below this, the file details are listed: `http://205.185.125.104/files/june11.dll`, `205.185.125.104`, `404 Status`, `text/html; charset=UTF-8 Content Type`, and `2021-11-28 21:25:51 UTC` (5 days ago). A "Community Score" section shows a question mark and a checkmark. Below the details, a table shows detection results from various vendors.

DETECTION	DETAILS	COMMUNITY
ESET	Malware	Forcepoint ThreatSeeker Malicious
Fortinet	Malware	Kaspersky Malware
Sophos	Malware	Webroot Malicious
Abusix	Clean	Acronis Clean
ADMINUSLabs	Clean	AICC (MONITORAPP) Clean
AlienVault	Clean	alohaMountain.ai Clean

Vulnerable Windows Machines

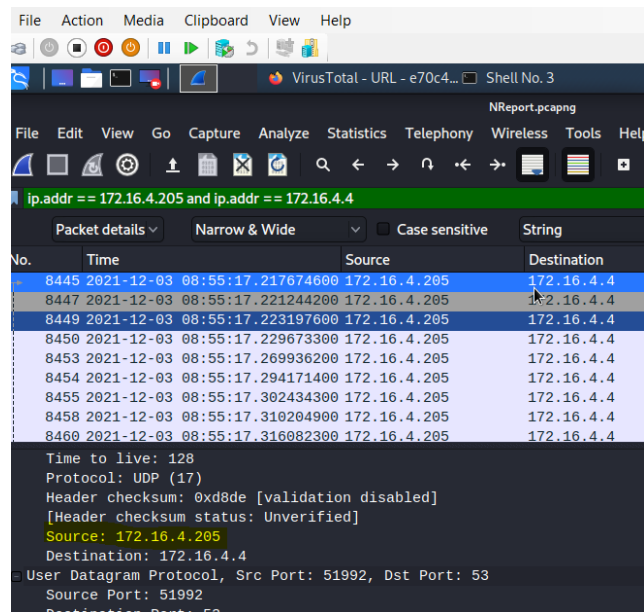
The Security team received reports of an infected Windows host on the network. They know the following:

- 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.

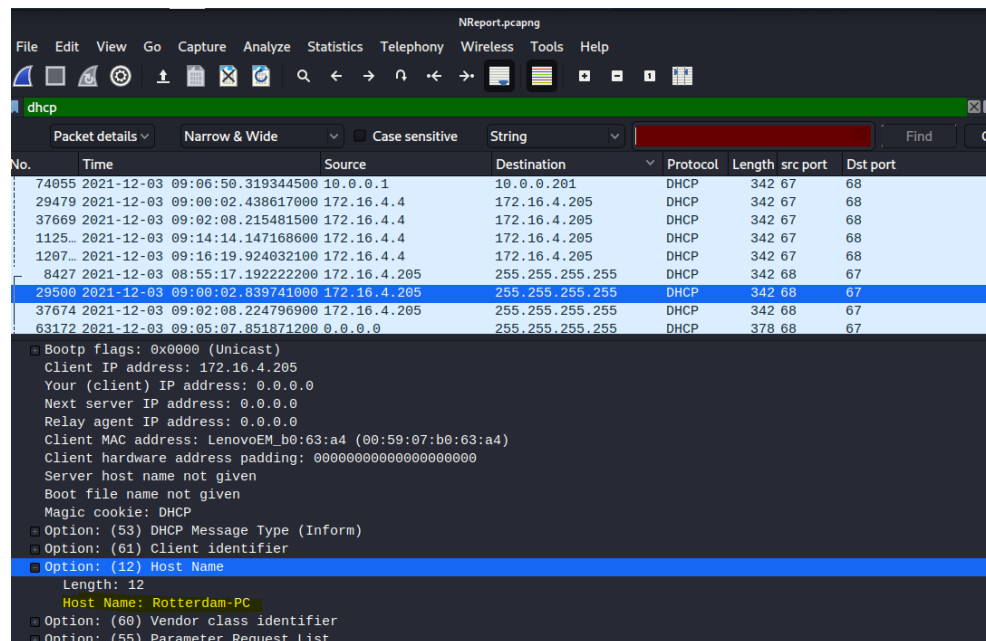
Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:

IP address: 172.16.4.205



Host name: Rotterdam-PC



MAC Address : 00:59:07:b0:63:a4

ip.addr == 172.16.4.205

No.	Time	Source	Destination	Protocol	Length	src port	Dst port
37871	2021-12-03 09:02:08.911259600	31.7.62.214	172.16.4.205	TCP	54	443	49255
37873	2021-12-03 09:02:08.916635300	31.7.62.214	172.16.4.205	TCP	54	443	49255
37875	2021-12-03 09:02:08.918778000	172.16.4.4	172.16.4.205	TCP	66	445	49272
37878	2021-12-03 09:02:08.927983200	172.16.4.4	172.16.4.205	SMB2	306	445	49272
37880	2021-12-03 09:02:08.935466500	172.16.4.4	172.16.4.205	SMB2	306	445	49272
37883	2021-12-03 09:02:08.984784000	172.16.4.4	172.16.4.205	TCP	54	445	49272
37885	2021-12-03 09:02:08.997309300	172.16.4.4	172.16.4.205	SMB2	314	445	49272
37887	2021-12-03 09:02:09.002781100	172.16.4.4	172.16.4.205	SMB2	138	445	49272
37889	2021-12-03 09:02:09.010077300	172.16.4.4	172.16.4.205	SMB2	274	445	49272

Frame 37875: 66 bytes on wire (528 bits), 66 bytes captured (528 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)
Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)

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

matthijs.devries

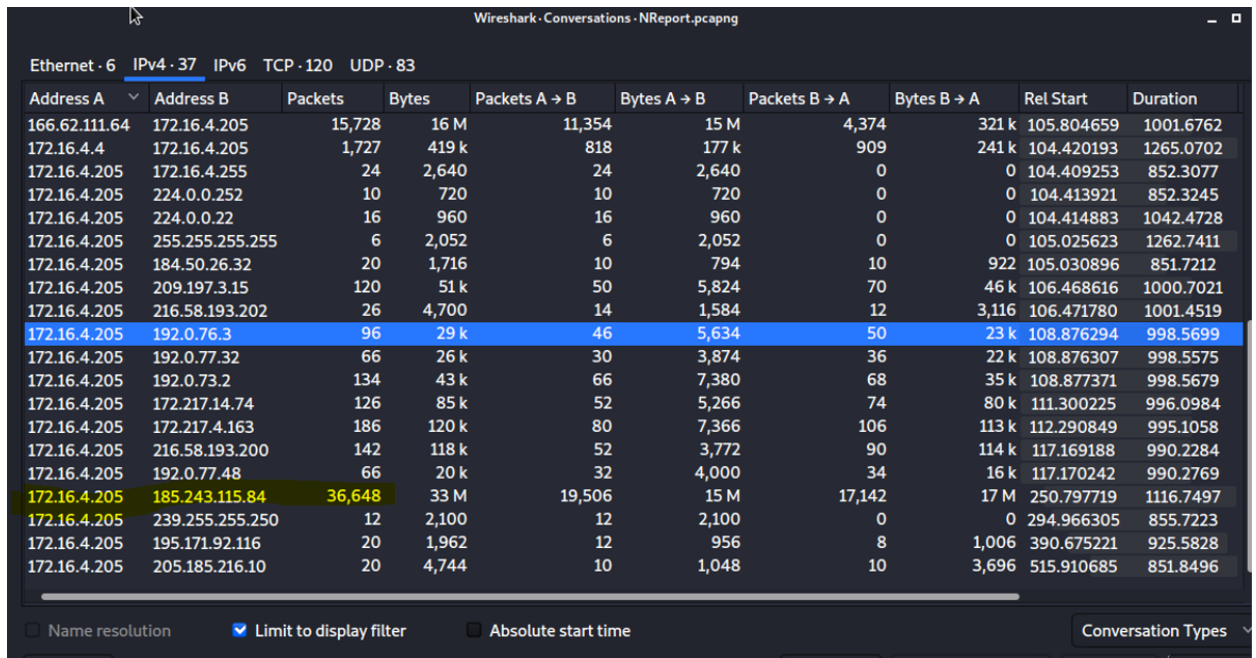
kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	src port	Dst port	CNameString
64306	2021-12-03 09:05:12.233359500	10.6.12.203	10.6.12.12	KRB5	300	49688	88	laptop-5wkxh9yg\$ AS-
64315	2021-12-03 09:05:12.249534900	10.6.12.203	10.6.12.12	KRB5	381	49689	88	laptop-5wkxh9yg\$ AS-
8519	2021-12-03 08:55:17.536688700	172.16.4.205	172.16.4.4	KRB5	292	49178	88	matthijs.devries AS-
8526	2021-12-03 08:55:17.552232200	172.16.4.205	172.16.4.4	KRB5	372	49179	88	matthijs.devries AS-
8528	2021-12-03 08:55:17.580338700	172.16.4.4	172.16.4.205	KRB5	242	88	49179	matthijs.devries AS-
8539	2021-12-03 08:55:17.639692500	172.16.4.4	172.16.4.205	KRB5	150	88	49180	matthijs.devries TG-
8551	2021-12-03 08:55:17.704681400	172.16.4.4	172.16.4.205	KRB5	273	88	49181	matthijs.devries TG-
8301	2021-12-03 08:55:16.596540500	172.16.4.205	172.16.4.4	KRB5	297	49163	88	rotterdam-pc\$ AS-
8309	2021-12-03 08:55:16.613724000	172.16.4.205	172.16.4.4	KRB5	377	49164	88	rotterdam-pc\$ AS-

TCP payload (188 bytes)
[PDU Size: 1648]
TCP segment data (188 bytes)
[2 Reassembled TCP Segments (1648 bytes): #8527(1460), #8528(188)]
Kerberos
Record Mark: 1644 bytes
0... = Reserved: Not set
0000 0000 0000 0000 0110 0110 1100 = Record Length: 1644
as-rep
pvno: 5
msg-type: krb-as-rep (11)
padata: 1 item
crealm: MIND-HAMMER.NET
cname
name-type: kRB5-NT-PRINCIPAL (1)
cname-string: 1 item
CNameString: matthijs.devries
ticket
enc-part

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

185.243.115.84



Wireshark - Conversations - NReport.pcapng

Ethernet · 6 IPv4 · 37 IPv6 TCP · 120 UDP · 83

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	105.804659	1001.6762
172.16.4.4	172.16.4.205	1,727	419 k	818	177 k	909	241 k	104.420193	1265.0702
172.16.4.205	172.16.4.255	24	2,640	24	2,640	0	0	104.409253	852.3077
172.16.4.205	224.0.0.252	10	720	10	720	0	0	104.413921	852.3245
172.16.4.205	224.0.0.22	16	960	16	960	0	0	104.414883	1042.4728
172.16.4.205	255.255.255.255	6	2,052	6	2,052	0	0	105.025623	1262.7411
172.16.4.205	184.50.26.32	20	1,716	10	794	10	922	105.030896	851.7212
172.16.4.205	209.197.3.15	120	51 k	50	5,824	70	46 k	106.468616	1000.7021
172.16.4.205	216.58.193.202	26	4,700	14	1,584	12	3,116	106.471780	1001.4519
172.16.4.205	192.0.76.3	96	29 k	46	5,634	50	23 k	108.876294	998.5699
172.16.4.205	192.0.77.32	66	26 k	30	3,874	36	22 k	108.876307	998.5575
172.16.4.205	192.0.73.2	134	43 k	66	7,380	68	35 k	108.877371	998.5679
172.16.4.205	172.217.14.74	126	85 k	52	5,266	74	80 k	111.300225	996.0984
172.16.4.205	172.217.4.163	186	120 k	80	7,366	106	113 k	112.290849	995.1058
172.16.4.205	216.58.193.200	142	118 k	52	3,772	90	114 k	117.169188	990.2284
172.16.4.205	192.0.77.48	66	20 k	32	4,000	34	16 k	117.170242	990.2769
172.16.4.205	185.243.115.84	36,648	33 M	19,506	15 M	17,142	17 M	250.797719	1116.7497
172.16.4.205	239.255.255.250	12	2,100	12	2,100	0	0	294.966305	855.7223
172.16.4.205	195.171.92.116	20	1,962	12	956	8	1,006	390.675221	925.5828
172.16.4.205	205.185.216.10	20	4,744	10	1,048	10	3,696	515.910685	851.8496

☐ Name resolution ☒ Limit to display filter ☐ Absolute start time Conversation Types

4. As a bonus, retrieve the desktop background of the Windows host.

Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

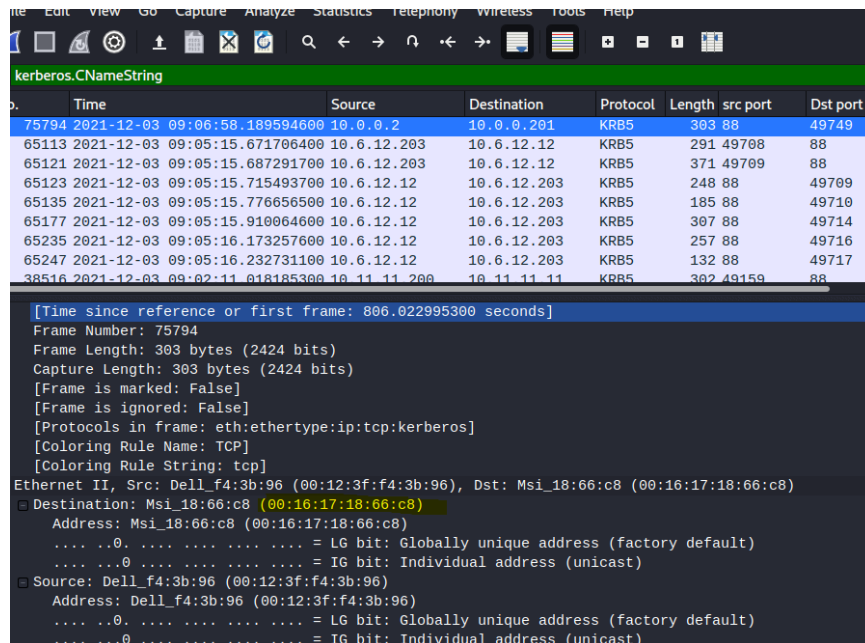
1. Find the following information about the machine with IP address 10.0.0.201:

Windows Username: Elmer. Blanco

No.	Time	Source	Destination	Protocol	Length	src port	Dst port	CNameString	in
75794	2021-12-03 09:06:58.189594600	10.0.0.2	10.0.0.201	KRB5	303	88	49749	elmer.blanco	TC
65113	2021-12-03 09:05:15.671706400	10.6.12.203	10.6.12.12	KRB5	291	49708	88	frank.brokowski	AS
65121	2021-12-03 09:05:15.687291700	10.6.12.203	10.6.12.12	KRB5	371	49709	88	frank.brokowski	AS
65123	2021-12-03 09:05:15.715493700	10.6.12.12	10.6.12.203	KRB5	248	88	49709	frank.brokowski	AS
65135	2021-12-03 09:05:15.776656500	10.6.12.12	10.6.12.203	KRB5	185	88	49710	frank.brokowski	TC
65177	2021-12-03 09:05:15.910064600	10.6.12.12	10.6.12.203	KRB5	307	88	49714	frank.brokowski	TC
65235	2021-12-03 09:05:16.173257600	10.6.12.12	10.6.12.203	KRB5	257	88	49716	frank.brokowski	TC
65247	2021-12-03 09:05:16.232731100	10.6.12.12	10.6.12.203	KRB5	132	88	49717	frank.brokowski	TC
38516	2021-12-03 09:02:11.018185300	10.11.11.200	10.11.11.11	KRB5	302	49159	88	gilbert-win7-nc\$	AS

[Time since previous frame in this TCP stream: 0.004857700 seconds]	
TCP payload (249 bytes)	
[PDU Size: 1709]	
TCP segment data (249 bytes)	
[2 Reassembled TCP Segments (1709 bytes): #75793(1460), #75794(249)]	
Kerberos	
Record Mark: 1705 bytes	
0... .. = Reserved: Not set	
.000 0000 0000 0000 0110 1010 1001 = Record Length: 1705	
tgs-rep	
pvno: 5	
msg-type: krb-tgs-rep (13)	
crealm: DOGOFtheyear.NET	
cname	
name-type: kRB5-NT-PRINCIPAL (1)	
cname-string: 1 item	
CNameString: elmer.blanco	
ticket	
enc-part	

Mac Address:00:16:17:18:66:c8



No.	Time	Source	Destination	Protocol	Length	src port	Dst port
75794	2021-12-03 09:06:58.189594600	10.0.0.2	10.0.0.201	KRB5	303	88	49749
65113	2021-12-03 09:05:15.671706400	10.6.12.203	10.6.12.12	KRB5	291	49708	88
65121	2021-12-03 09:05:15.687291700	10.6.12.203	10.6.12.12	KRB5	371	49709	88
65123	2021-12-03 09:05:15.715493700	10.6.12.12	10.6.12.203	KRB5	248	88	49709
65135	2021-12-03 09:05:15.776656500	10.6.12.12	10.6.12.203	KRB5	185	88	49710
65177	2021-12-03 09:05:15.910064600	10.6.12.12	10.6.12.203	KRB5	307	88	49714
65235	2021-12-03 09:05:16.173257600	10.6.12.12	10.6.12.203	KRB5	257	88	49716
65247	2021-12-03 09:05:16.232731100	10.6.12.12	10.6.12.203	KRB5	132	88	49717
38516	2021-12-03 09:02:11.018185300	10.11.11.200	10.11.11.11	KRB5	302	49159	88

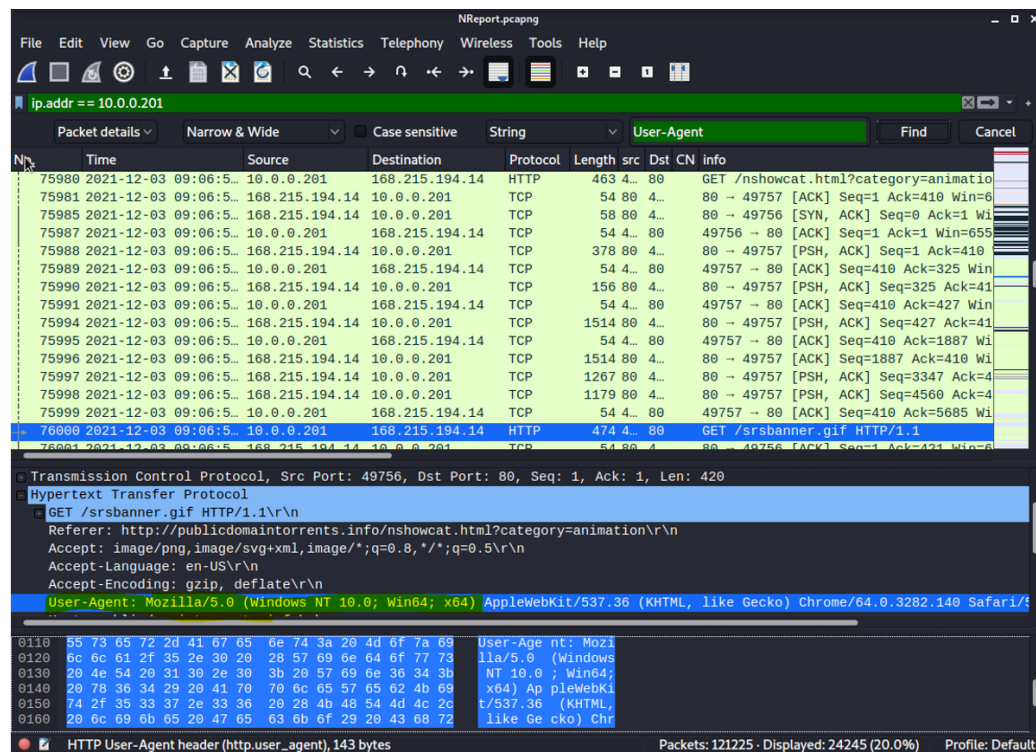
[Time since reference or first frame: 806.022995300 seconds]

Frame Number: 75794
Frame Length: 303 bytes (2424 bits)
Capture Length: 303 bytes (2424 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_f4:3b:96 (00:12:3f:f4:3b:96), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)

- Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
Address: Msi_18:66:c8 (00:16:17:18:66:c8)
... ..0. = LG bit: Globally unique address (factory default)
... ..0. = IG bit: Individual address (unicast)
- Source: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
Address: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
... ..0. = LG bit: Globally unique address (factory default)
... ..0. = IG bit: Individual address (unicast)

OS version: Windows NT 10.0



No.	Time	Source	Destination	Protocol	Length	src	Dst	CN	info
75980	2021-12-03 09:06:5...	10.0.0.201	168.215.194.14	HTTP	463	4...	80		GET /nshowcat.html?category=animation
75981	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	54	80	4...	80	→ 49757 [ACK] Seq=1 Ack=410 Win=6
75985	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	58	80	4...	80	→ 49756 [SYN, ACK] Seq=0 Ack=1 Wi
75987	2021-12-03 09:06:5...	10.0.0.201	168.215.194.14	TCP	54	4...	80	49756	→ 80 [ACK] Seq=1 Ack=1 Win=655
75988	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	378	80	4...	80	→ 49757 [PSH, ACK] Seq=1 Ack=410
75989	2021-12-03 09:06:5...	10.0.0.201	168.215.194.14	TCP	54	4...	80	49757	→ 80 [ACK] Seq=410 Ack=325 Win
75990	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	156	80	4...	80	→ 49757 [PSH, ACK] Seq=325 Ack=41
75991	2021-12-03 09:06:5...	10.0.0.201	168.215.194.14	TCP	54	4...	80	49757	→ 80 [ACK] Seq=410 Ack=427 Win
75994	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	1514	80	4...	80	→ 49757 [PSH, ACK] Seq=427 Ack=41
75995	2021-12-03 09:06:5...	10.0.0.201	168.215.194.14	TCP	54	4...	80	49757	→ 80 [ACK] Seq=410 Ack=1887 Wi
75996	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	1514	80	4...	80	→ 49757 [ACK] Seq=1887 Ack=410 Wi
75997	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	1267	80	4...	80	→ 49757 [PSH, ACK] Seq=3347 Ack=4
75998	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	1179	80	4...	80	→ 49757 [PSH, ACK] Seq=4560 Ack=4
75999	2021-12-03 09:06:5...	10.0.0.201	168.215.194.14	TCP	54	4...	80	49757	→ 80 [ACK] Seq=410 Ack=5685 Wi
76000	2021-12-03 09:06:5...	10.0.0.201	168.215.194.14	HTTP	474	4...	80		GET /srsbanner.gif HTTP/1.1
76001	2021-12-03 09:06:5...	168.215.194.14	10.0.0.201	TCP	54	80	4...	80	→ 49756 [ACK] Seq=1 Ack=410 Min=0

Transmission Control Protocol, Src Port: 49756, Dst Port: 80, Seq: 1, Ack: 1, Len: 420

Hypertext Transfer Protocol

- GET /srsbanner.gif HTTP/1.1\r\n
- Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\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/4

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/4

HTTP User-Agent header (http.user_agent), 143 bytes

Packets: 121225 - Displayed: 24245 (20.0%) Profile: Default

2. Which torrent file did the user download?

Betty Boop -Rhythm on the reservation

