

# 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?

a. **ip.addr == 10.6.12.0/24**

b. **Frank-n-Ted-DC.frank-n-ted.com**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

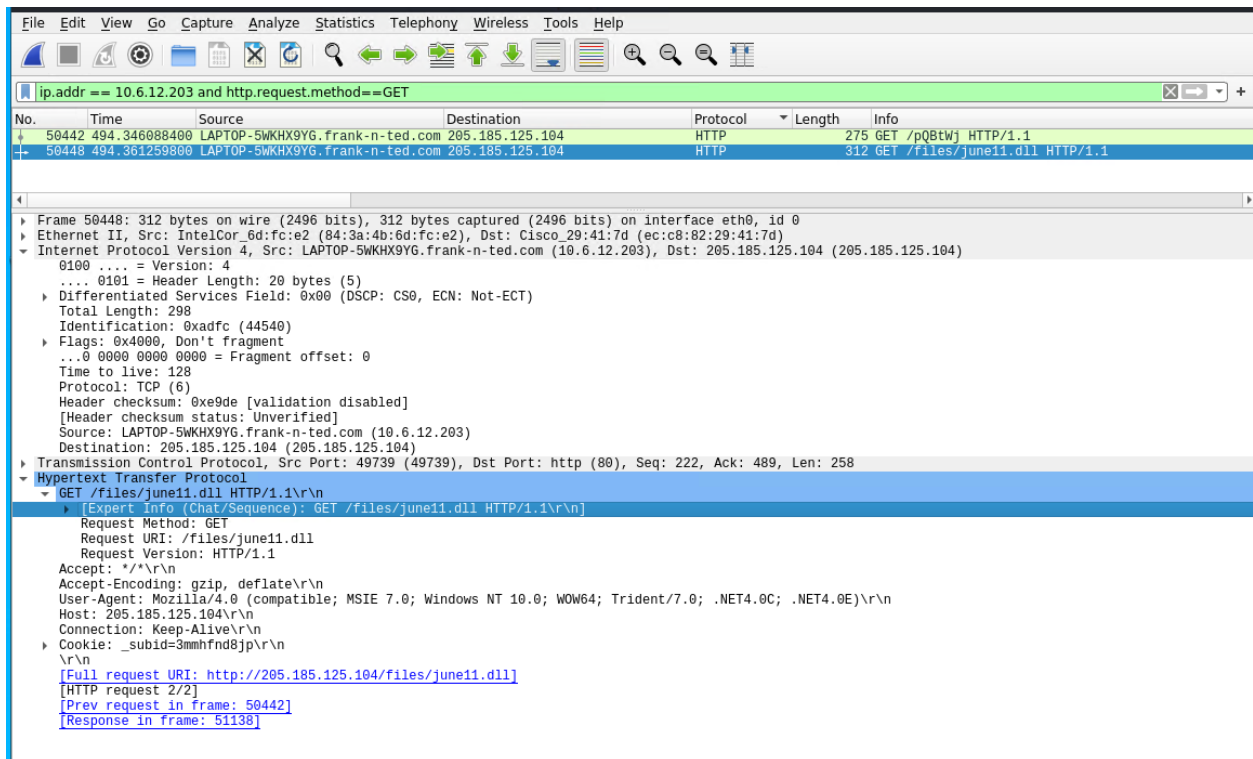
ip.addr == 10.6.12.0/24

No.	Time	Source	Destination	Protocol	Length	Info
47639	480.058691300	Frank-n-Ted-DC.fran...	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x6b0e1d90
46899	476.782041100	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
46900	476.784643300	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com ...
46901	476.786021300	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
46902	476.787712100	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1...
46912	476.853633000	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	76	Standard query 0x3a00 A dns.msftncsi.com
46913	476.855032200	Frank-n-Ted-DC.fran...	dns.google	DNS	87	Standard query 0xa08b A dns.msftncsi.com OPT
46914	476.856714200	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	103	Standard query response 0xa08b A dns.msftncsi.com A 131.107.255.255 OPT
46915	476.858148500	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	92	Standard query response 0x3a00 A dns.msftncsi.com A 131.107.255.255
46916	476.859430100	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	80	Standard query 0x16a7 A wpad.frank-n-ted.com
46917	476.861967100	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	157	Standard query response 0x16a7 No such name A wpad.frank-n-ted.com SOA f...
46920	476.867493800	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	127	Standard query 0x6b8d SRV _ldap._tcp.Default-First-Site-Name._sites.dc._...
46921	476.870582800	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	193	Standard query response 0x6b8d SRV _ldap._tcp.Default-First-Site-Name._sites.dc._...
47043	477.430249800	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	132	Standard query 0x31ae SRV _ldap._tcp.Default-First-Site-Name._sites.Doma...
47045	477.436921000	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	198	Standard query response 0x31ae SRV _ldap._tcp.Default-First-Site-Name._sites.Doma...
47072	477.534725700	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	132	Standard query 0x79df SRV _ldap._tcp.Default-First-Site-Name._sites.Fore...
47073	477.537896200	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	198	Standard query response 0x79df SRV _ldap._tcp.Default-First-Site-Name._sites.Fore...
47144	477.840500400	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	117	Standard query 0xde86 SRV _ldap._tcp.Default-First-Site-Name._sites.fran...
47145	477.843431300	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	183	Standard query response 0xde86 SRV _ldap._tcp.Default-First-Site-Name._sites.fran...
47223	478.073986300	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	88	Standard query 0x4133 A ygrvqkgouzou.frank-n-ted.com
47224	478.076629400	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	165	Standard query response 0x4133 No such name A ygrvqkgouzou.frank-n-ted.c...
47242	478.170567700	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	90	Standard query 0xde17 A Frank-n-Ted-DC.frank-n-ted.com
47243	478.172261200	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	106	Standard query response 0xde17 A Frank-n-Ted-DC.frank-n-ted.com A 10.6.1...
47452	479.143900500	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	127	Standard query 0x53f6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._...

Frame 46914: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface eth0, id 0  
Ethernet II, Src: Cisco 29:41:7d (ec:c8:82:29:41:7d), Dst: Dell 2a:f7:e5 (98:40:bb:2a:f7:e5)  
Internet Protocol Version 4, Src: dns.google (8.8.8.8), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)  
User Datagram Protocol, Src Port: domain (53), Dst Port: 54697 (54697)  
Domain Name System (response)

```
0000  98 40 bb 2a f7 e5 ec c8 82 29 41 7d 08 00 45 00  .@.*....)A}..E.  
0010  00 59 22 02 00 00 80 11 f2 70 08 08 08 0a 06    Y"....p.....  
0020  0c 0c 00 35 d5 a9 00 45 75 3b a0 8b 81 80 00 01  ...5....E u;....  
0030  00 01 00 00 00 01 03 64 6e 73 08 0d 73 66 74 6e  ....d ns.msftn  
0040  63 73 69 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01  cs1.com.....  
0050  00 01 00 00 00 17 00 04 83 60 ff ff 00 00 29 02    .....k.....  
0060  00 00 00 00 00 00 00 00
```

2. What is the IP address of the Domain Controller (DC) of the AD network?
  - a. **IP: 10.6.12.12**
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.
  - a. **filter: ip.addr==10.6.12.203 and http.request.method==GET**
  - b. **june11.dll**



4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?
  - a. **alphaMountain.ai**
  - b. **Forcepoint ThreatSeeker**
  - c. **Webroot**
  - d. **Googleipdate.exe**



205.185.125.104 (205.185.112.0/20)  
AS 53667 ( PONYNET )

US 

## DETECTION   DETAILS   RELATIONS   COMMUNITY 6

### Security Vendors' Analysis

alphaMountain.ai	🚩 Malicious	CRDF	🚩 Malicious
Forcepoint ThreatSeeker	🚩 Malicious	Kaspersky	🚩 Malware
Webroot	🚩 Malicious	Abusix	✅ Clean
Acronis	✅ Clean	ADMINUSLabs	✅ Clean
AICC (MONITORAPP)	✅ Clean	AlienVault	✅ Clean
Antiy-AVL	✅ Clean	Armis	✅ Clean
Avira	✅ Clean	BADWARE.INFO	✅ Clean
Baidu-International	✅ Clean	benkow.cc	✅ Clean
Bfore AI PreCrime	✅ Clean	BitDefender	✅ Clean
Blueliv	✅ Clean	Certego	✅ Clean
Chong Lua Dao	✅ Clean	CINS Army	✅ Clean
CMC Threat Intelligence	✅ Clean	CyberCrime	✅ Clean



The screenshot shows the VirusTotal web interface for the file `d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`. The file name is `Googleipdate.exe`, and its SHA256 hash is displayed at the top. Below the header, there are two tabs: "Details" (selected) and "Comments". Under the "Details" tab, the "Scans" section shows a table of detection results from various security vendors.

Security vendor	Result	Update
Bkav	malicious	20220820
Lionic	malicious	20220820
Elastic	malicious	20220728
Cynet	malicious	20220820
FireEye	malicious	20220820
McAfee	malicious	20220820
Cylance	malicious	20220820
Zillya	malicious	20220819

# Vulnerable Windows Machines

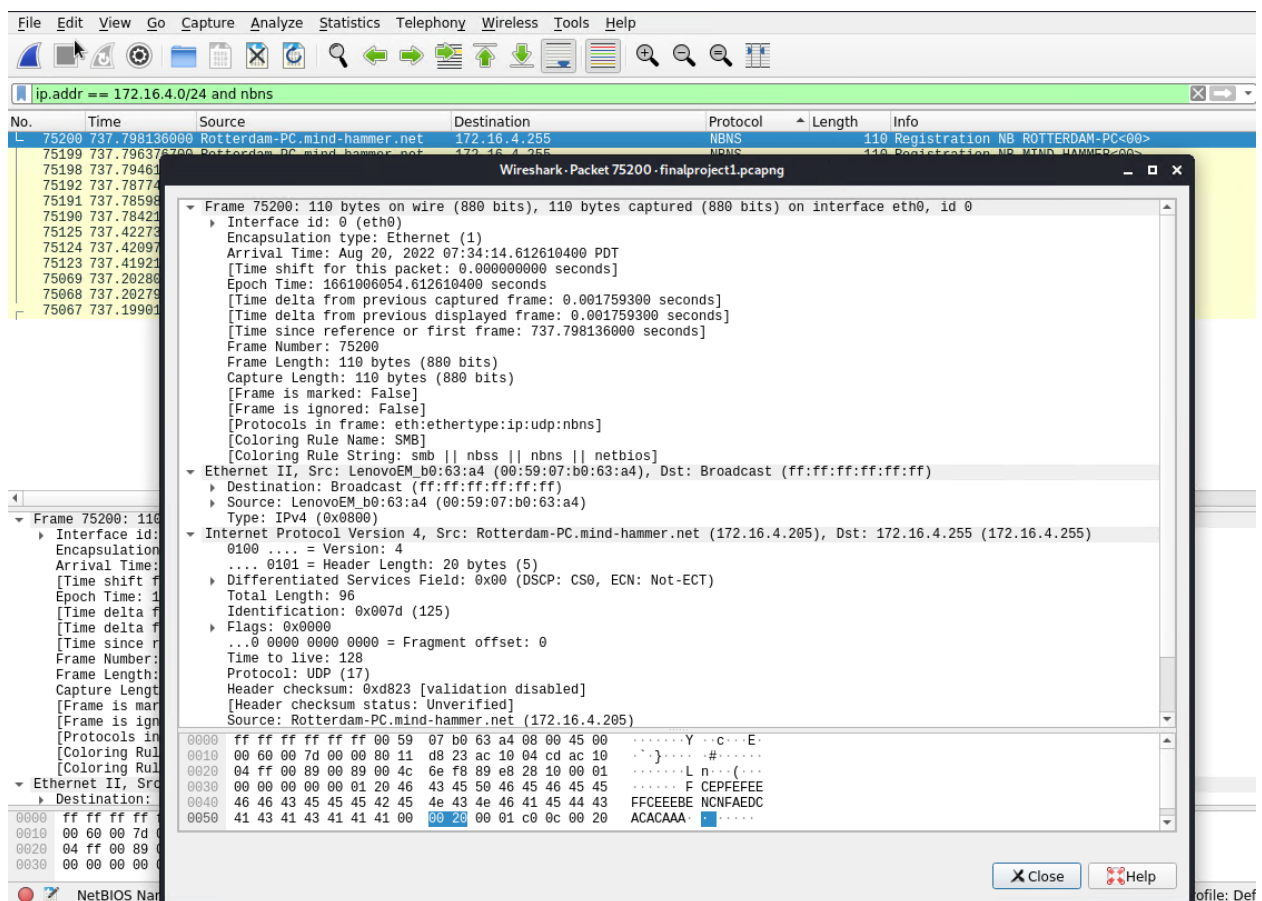
The Security team received reports of an infected Windows host on the network. They know the following:

- 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: **172.16.4.205**
- MAC address: **00:59:07:b0:63:a4**



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

- **matthijs.devries**
- **Filter: ip.addr == 172.16.4.0/24 and kerberos.CNameString**

Wireshark packet capture showing Kerberos traffic. The top pane displays a list of packets filtered by the expression `ip.addr == 172.16.4.0/24 and kerberos.CNameString`. The bottom pane shows the details of a selected Kerberos AS-REQ packet, highlighting the `CNameString: matthijs.devries` field.

Time	Source	Destination	Protocol	Info	CNameString
738.327861400	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	matthijs.devries
738.262855900	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	matthijs.devries
738.293518300	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	AS-REP	matthijs.devries
738.159856700	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	matthijs.devries
738.121311400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	matthijs.devries
738.060654600	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$
738.033155400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REP	ROTTERDAM-PC\$
738.017526900	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	ROTTERDAM-PC\$
737.675273900	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$
737.568718300	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$
737.327624000	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$
737.264396200	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	AS-REP	ROTTERDAM-PC\$
737.236881600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	rotterdam-pc\$
737.219708200	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	rotterdam-pc\$
298.658144500	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$
297.306604100	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$
43.688125800	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$
43.630999400	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC\$

Source: Rotterdam-PC.mind-hammer.net (172.16.4.205)  
Destination: mind-hammer-dc.mind-hammer.net (172.16.4.4)  
Transmission Control Protocol, Src Port: 49179 (49179), Dst Port: kerberos (88), Seq: 1, Ack: 1, Len: 318

▼ Kerberos

- Record Mark: 314 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: matthijs.devries
    - realm: MIND-HAMMER
    - sname
    - till: 2037-09-13 02:48:05 (UTC)
    - rtime: 2037-09-13 02:48:05 (UTC)
    - nonce: 631265106
    - etype: 6 items

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

- **Address A: 172.16.4.205**
- **Address B: 185.243.115.84**
- **Packets: 18,324**

finalproject1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark - Conversations - finalproject1.pcapng

Ethernet · 85IPv4 · 881IPv6 · 9TCP · 1078UDP · 1817

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	18,324	16 M	9,753	7,983 k	8,571	8,543 k	31.878927	265.0412	240 k	
166.62.111.64	172.16.4.205	6,557	6,702 k	4,713	6,563 k	1,844	139 k	0.000000	829.2346	63 k	
192.168.1.90	192.168.1.100	4,747	21 M	3,057	21 M	1,690	458 k	4.193939	822.2584	208 k	
10.0.0.201	64.187.66.143	4,688	3,493 k	2,148	139 k	2,540	3,354 k	607.384752	129.8125	8,574	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	505.615347	67.9985	491 k	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	669.024395	66.9059	8,605	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	407.642130	66.7937	13 k	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	480.068606	99.1500	13 k	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	476.782041	102.3708	12 k	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	299.803255	176.9289	4,459	
10.0.0.2	10.0.0.201	1,083	266 k	520	133 k	563	132 k	579.243913	89.6853	11 k	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	451.954880	22.4916	12 k	
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	31.852900	749.1471	1,029	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	304.055138	172.6836	3,858	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	311.144454	94.0159	2,950	
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	366.619648	106.4827	2,664	
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	494.339667	79.8144	1,050	
10.0.0.201	172.217.9.2	566	282 k	271	31 k	295	251 k	588.644503	49.3013	5,124	
10.0.0.201	96.7.89.194	487	166 k	200	33 k	287	133 k	582.069924	4.4491	59 k	
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	311.139456	74.8401	2,361	
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	299.571986	84.0332	1,620	
10.0.0.201	168.215.194.14	439	276 k	187	17 k	252	258 k	588.045558	49.9051	2,833	
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	302.100787	173.6506	481	
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	341.902215	102.8961	1,541	
10.11.11.179	31.13.93.26	410	291 k	171	13 k	239	278 k	330.177715	71.9760	1,532	
10.11.11.179	172.217.6.162	402	239 k	191	18 k	211	220 k	358.271152	49.3571	3,005	
10.11.11.203	188.95.248.71	376	410 k	86	5,474	290	405 k	386.287107	8.0123	5,465	
10.0.0.201	216.58.218.161	366	212 k	165	13 k	201	198 k	592.929863	45.0030	2,480	
31.13.70.52	172.16.4.205	363	239 k	218	223 k	145	15 k	36.410564	761.4368	2,352	
10.11.11.179	172.217.1.225	357	280 k	158	11 k	199	268 k	383.423649	24.1537	3,905	
10.11.11.217	35.165.65.265	357	231 k	174	21 k	183	208 k	363.580388	110.6738	1,540	

☐ Name resolution☐ Limit to display filter☐ Absolute start time

CopyFollow Stream...Graph...CloseHelp

Conversation Types

realm: MIND-HAMMER  
 sname  
 till: 2037-09-13 02:48:05 (UTC)  
 rtime: 2037-09-13 02:48:05 (UTC)  
 nonce: 631265106  
 etype: 6 items

00c0 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 60 ...0...0...0...

CNameString (kerberos.CNameString), 16 bytes

Packets: 81824 · Displayed: 19 (0.0%) · Dropped: 0 (0.0%) · Profile: Default

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

- **ip.addr == 172.16.4.205 and ip.addr == 185.243.115.84 and http**
- **POST \empty.gif**



File

Edit

View

Go

Capture

Analyze

Statistics

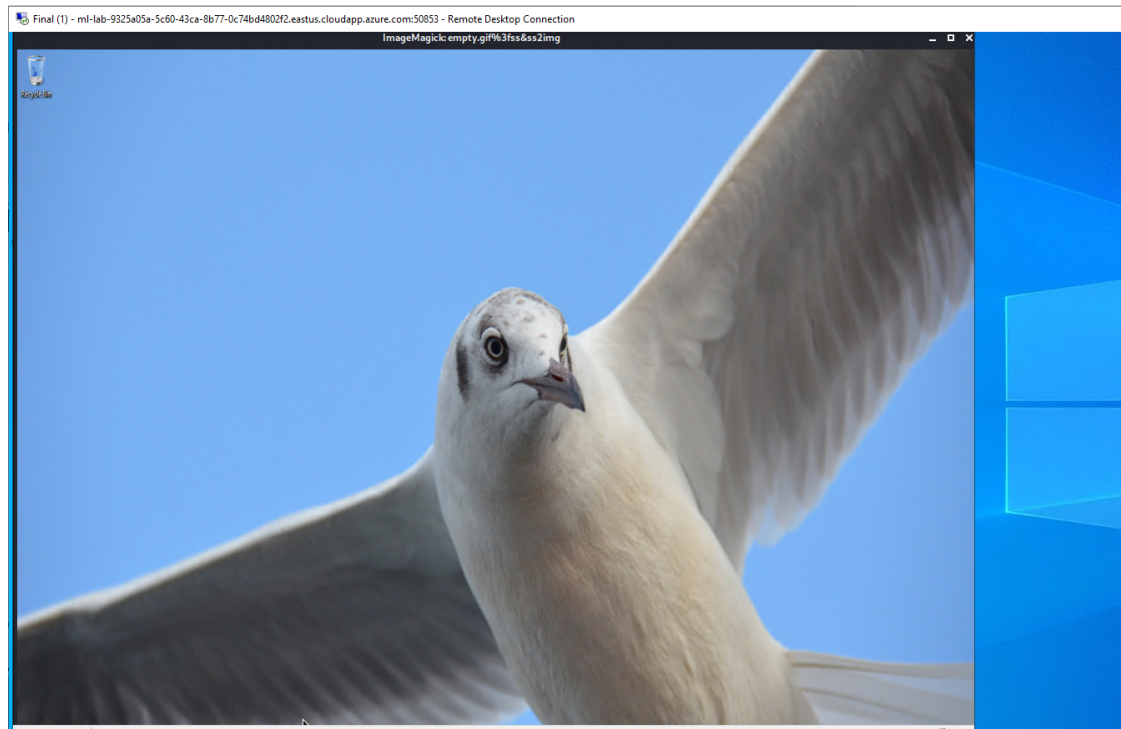
Telephony

Wireless

Tools

Help

</



## References

Duncan, B. (2019, March 29). *Wireshark Tutorial: Identifying Hosts and Users*. Palo Alto Networks Unit 42. Retrieved August 24, 2022, from <https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/>