Network Analysis

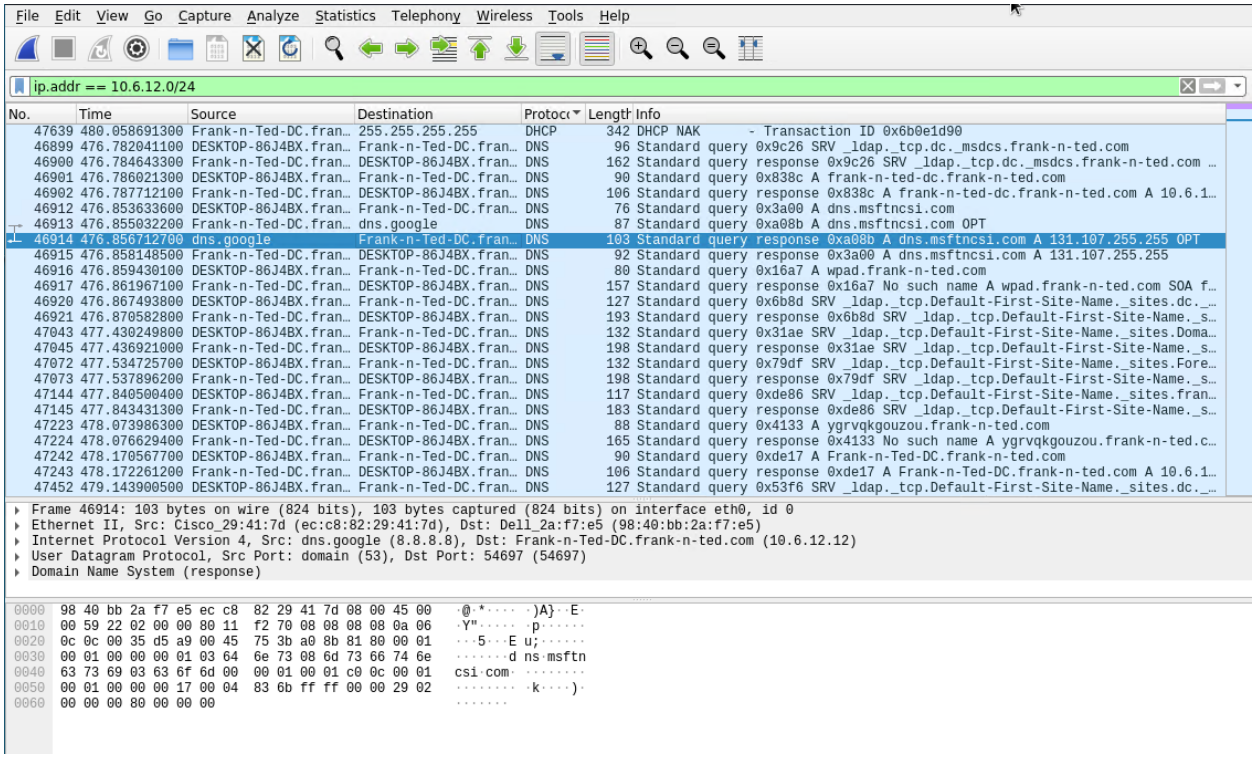
Time Thieves

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:

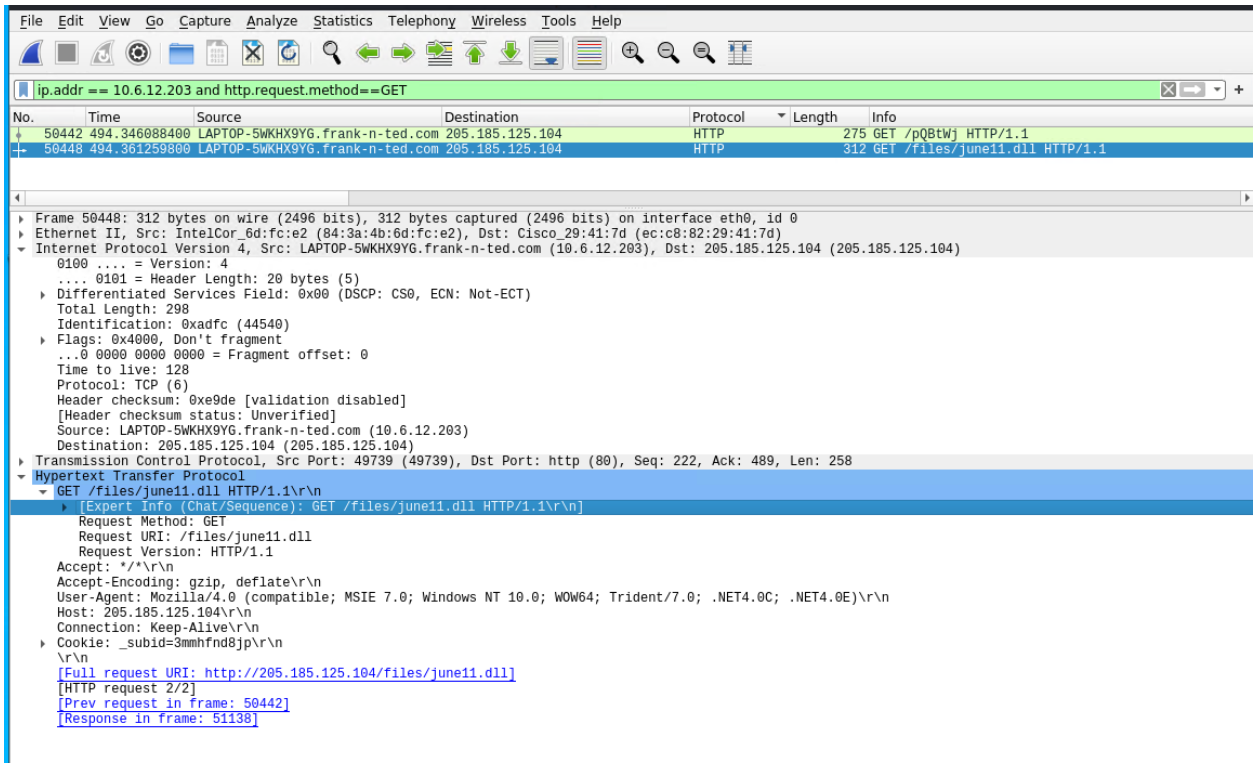
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

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

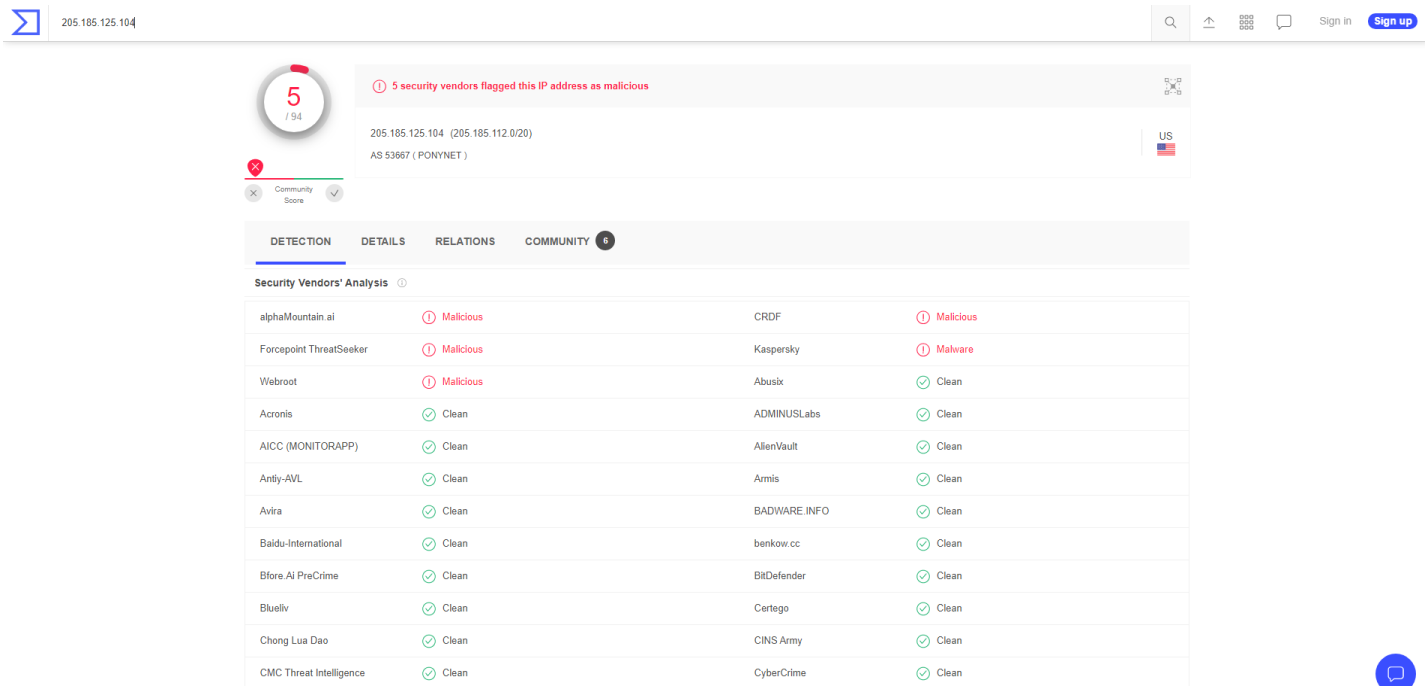
1. What is the domain name of the users' custom site?
    a. **ip.addr == 10.6.12.0/24**
    b. **Frank-n-Ted-DC.frank-n-ted.com**

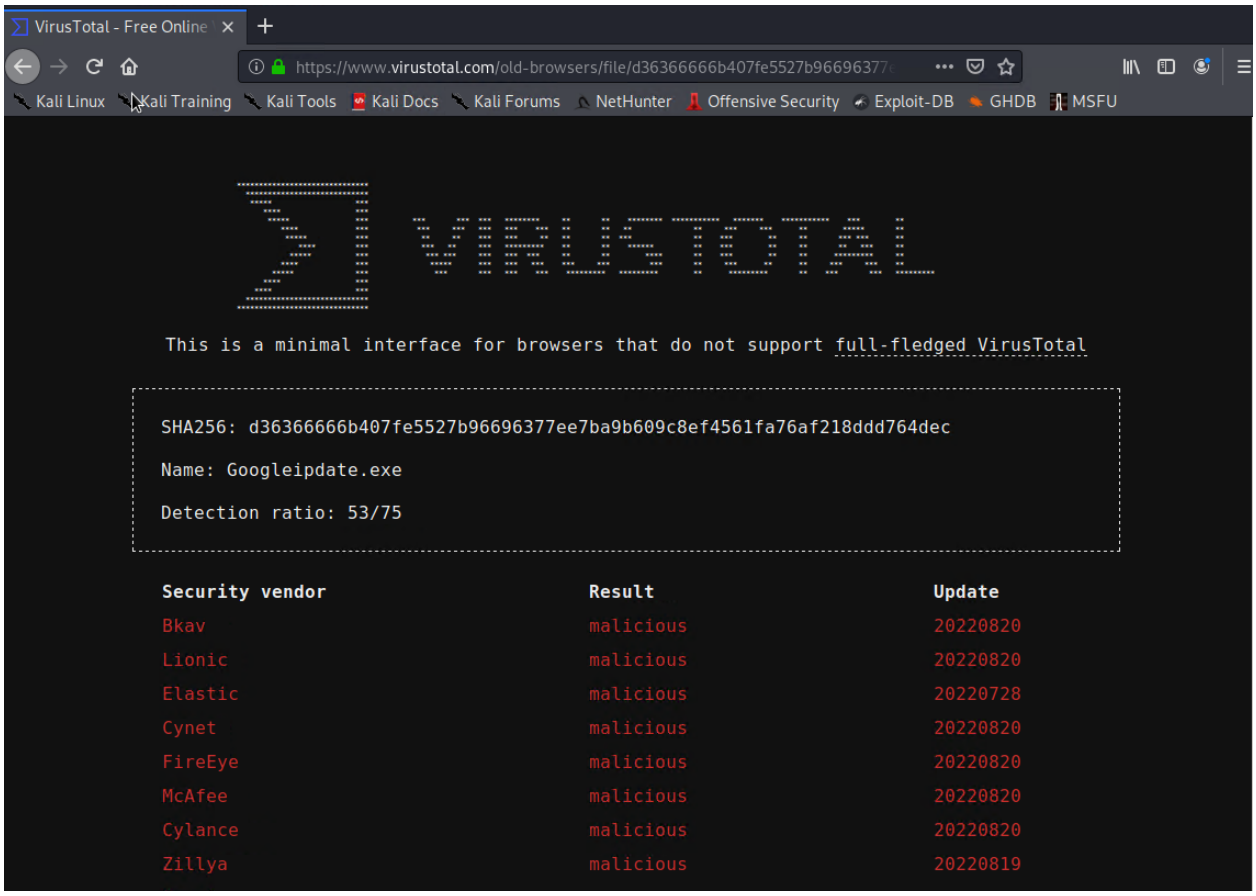


2. What is the IP address of the Domain Controller (DC) of the AD network?
    a. **IP: 10.6.12.12**
3. What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.
    a. **filter: ip.addr==10.6.12.203 and http.request.method==GET**
    b. **june11.dll**



4. Upload the file to VirusTotal.com. What kind of malware is this classified as?
    a. **alphaMountain.ai**
    b. **Forcepoint ThreatSeeker**
    c. **Webroot**
    d. **Googleipdate.exe**


205.185.125.104
Sign in
Sign up
5
/ 94
5 security vendors flagged this IP address as malicious
205.185.125.104 (205.185.112.0/20)
AS 53667 (PONYNET)
US
Community Score
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


VirusTotal - Free Online
https://www.virustotal.com/old-browsers/file/d36366666b407fe5527b96696377
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
VIRUSTOTAL
This is a minimal interface for browsers that do not support full-fledged VirusTotal
SHA256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Name: Googleipdate.exe
Detection ratio: 53/75
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

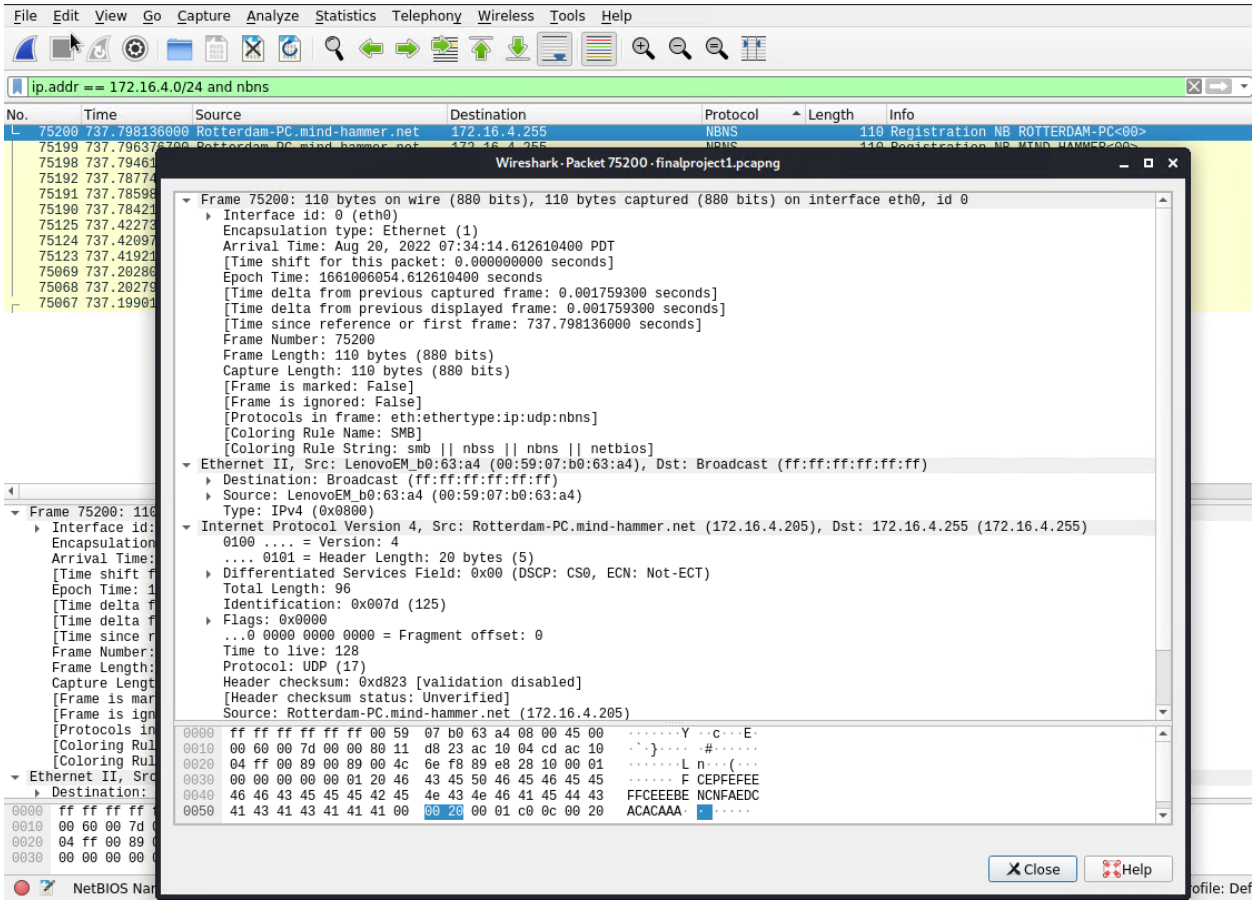
Vulnerable Windows Machines

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

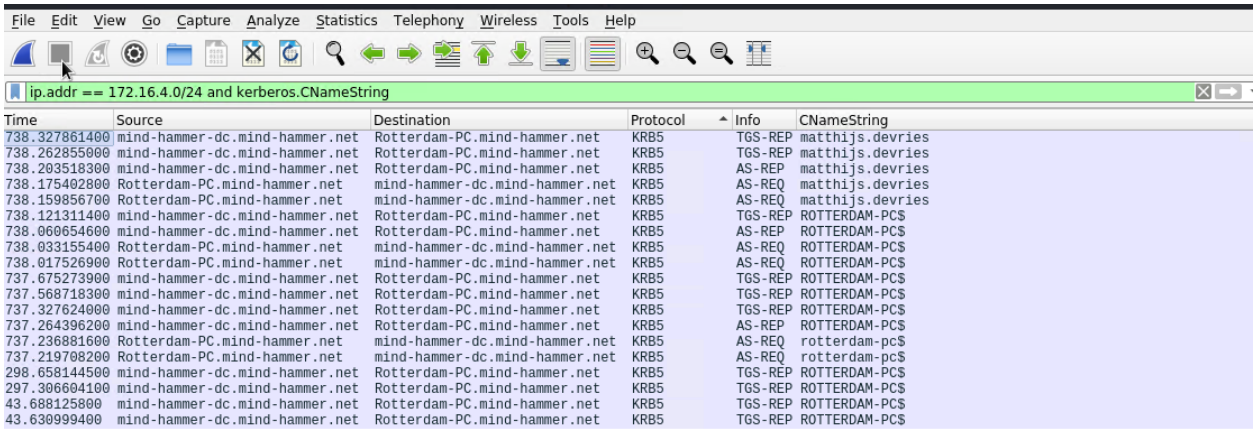
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

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**



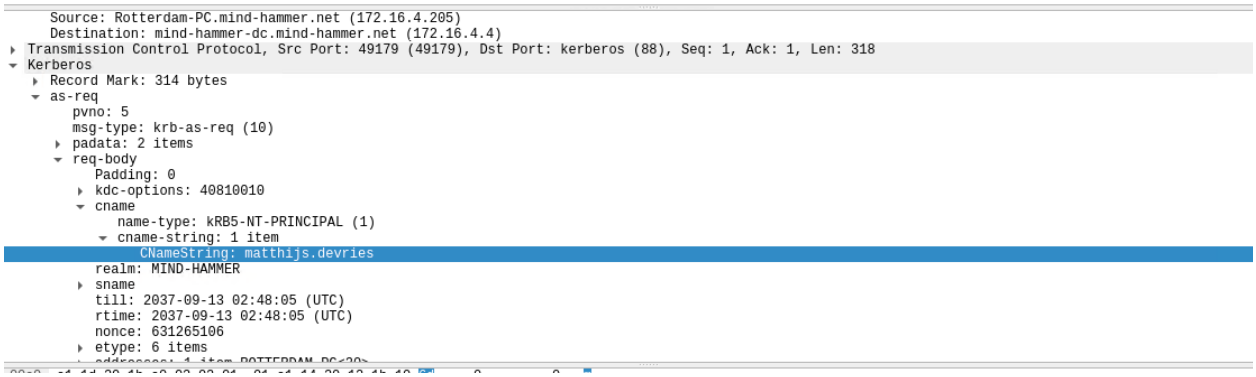
2. What is the username of the Windows user whose computer is infected?
    - **matthjs.devries**
    - **Filter: ip.addr == 172.16.4.0/24 and keberos.CNameString**



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

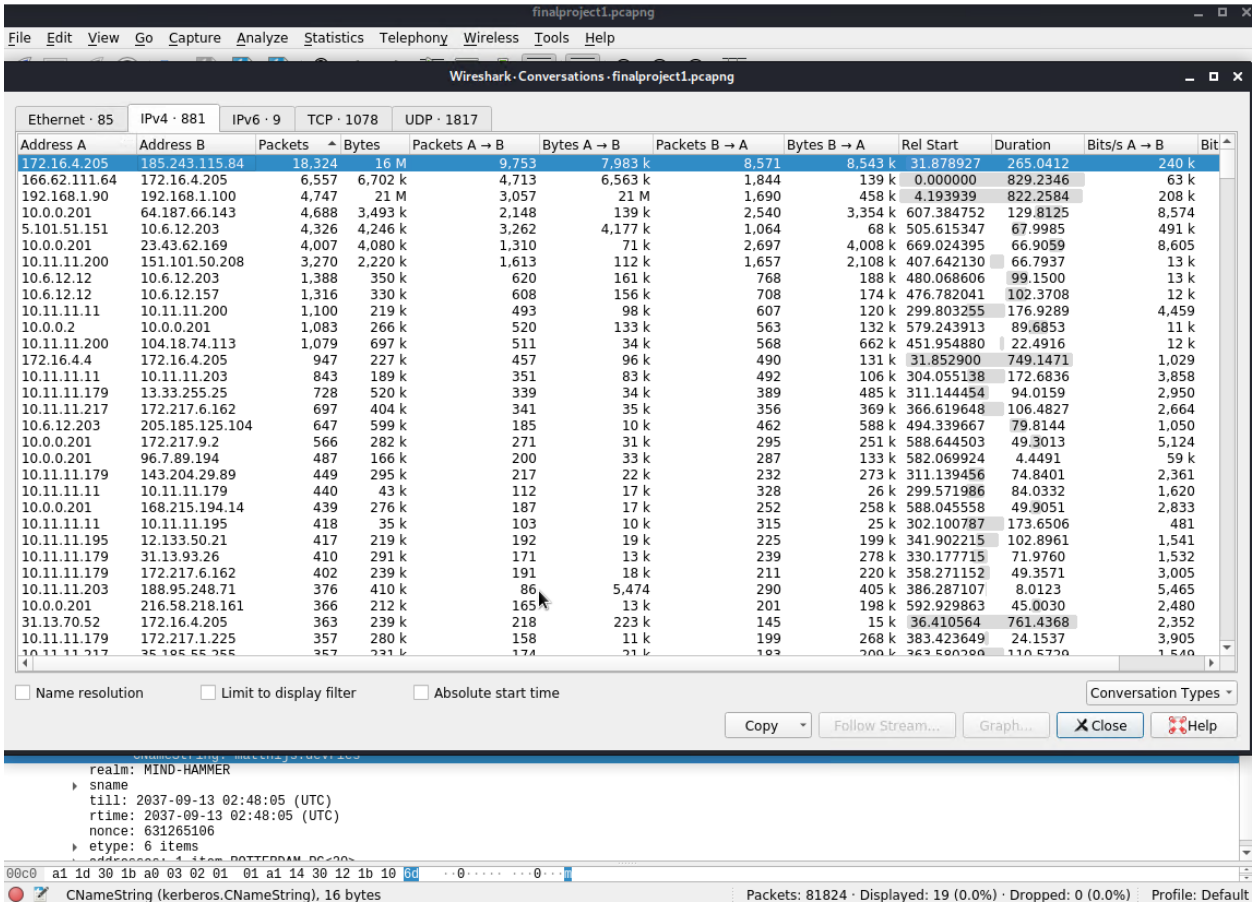
ip.addr == 172.16.4.0/24 and kerberos.CNameString

Time	Source	Destination	Protocol	Info	CNameString
738.327861400	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	matthijs.devries
738.262855000	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	matthijs.devries
738.203518300	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	AS-REP	matthijs.devries
738.175402800	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	matthijs.devries
738.159856700	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	matthijs.devries
738.121311400	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	TGS-REP	ROTTERDAM-PC$
738.060654600	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	AS-REP	ROTTERDAM-PC$
738.033155400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	AS-REQ	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$

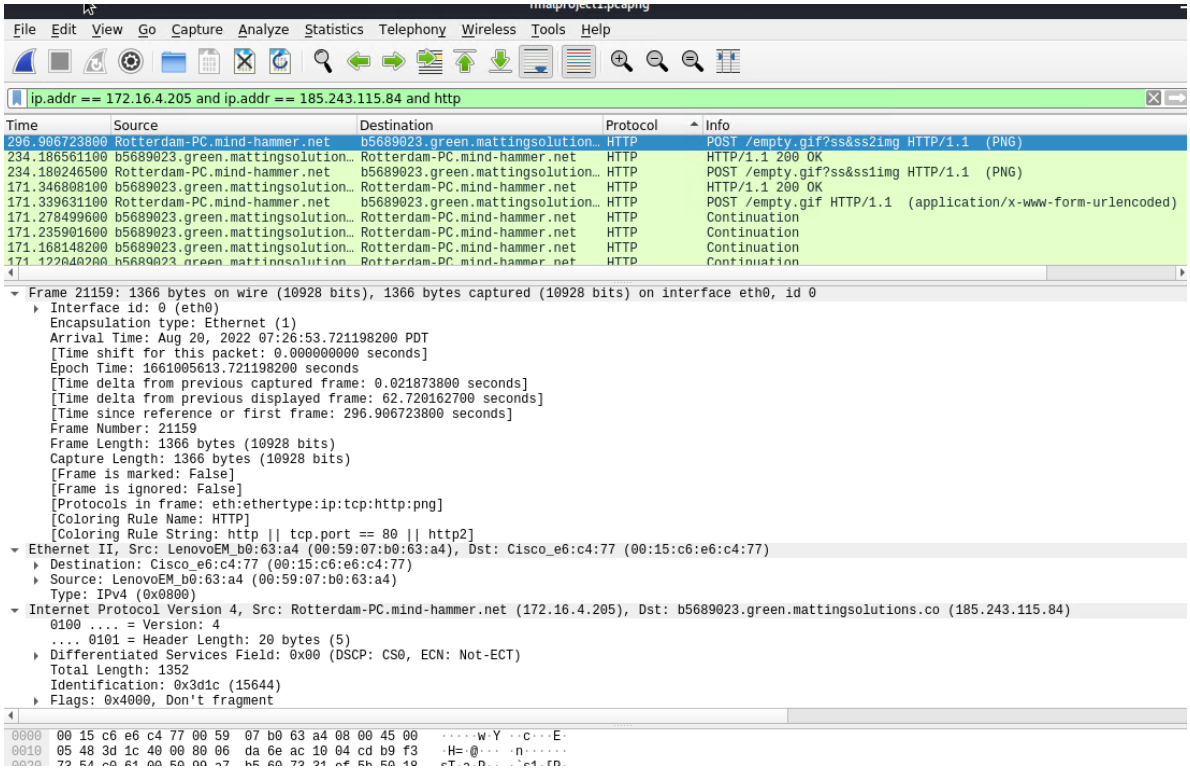


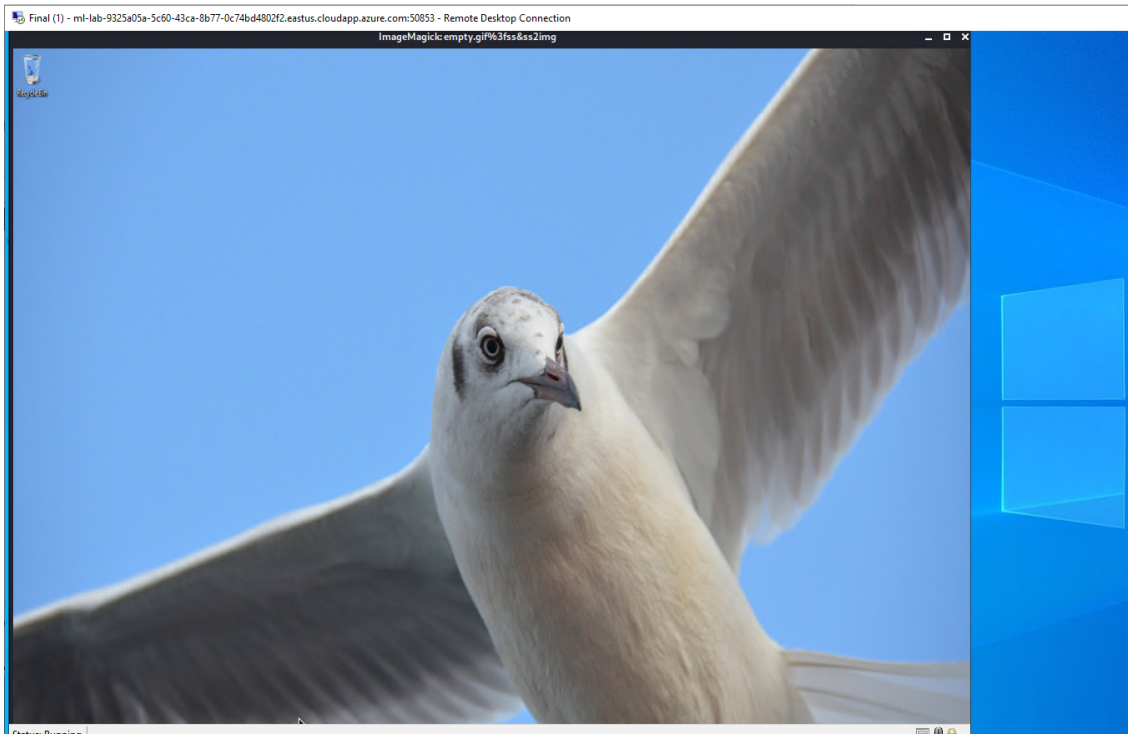
```
    Source: Rotterdam-PC.mind-hammer.net (172.16.4.205)
    Destination: mind-hammer-dc.mind-hammer.net (172.16.4.4)
▸ Transmission Control Protocol, Src Port: 49179 (49179), Dst Port: kerberos (88), Seq: 1, Ack: 1, Len: 318
▾ Kerberos
  ▸ Record Mark: 314 bytes
  ▾ as-req
      pvno: 5
      msg-type: 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**



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**


finalproject1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 172.16.4.205 and ip.addr == 185.243.115.84 and http
Time Source Destination Protocol Info
296.906723800 Rotterdam-PC.mind-hammer.net b5689023.green.mattingsolution… HTTP POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)
234.186561100 b5689023.green.mattingsolution… Rotterdam-PC.mind-hammer.net HTTP HTTP/1.1 200 OK
234.180246500 Rotterdam-PC.mind-hammer.net b5689023.green.mattingsolution… HTTP POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
171.346808100 b5689023.green.mattingsolution… Rotterdam-PC.mind-hammer.net HTTP HTTP/1.1 200 OK
171.339631100 Rotterdam-PC.mind-hammer.net b5689023.green.mattingsolution… HTTP POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
171.278499600 b5689023.green.mattingsolution… Rotterdam-PC.mind-hammer.net HTTP Continuation
171.235901600 b5689023.green.mattingsolution… Rotterdam-PC.mind-hammer.net HTTP Continuation
171.168148200 b5689023.green.mattingsolution… Rotterdam-PC.mind-hammer.net HTTP Continuation
Frame 21159: 1366 bytes on wire (10928 bits), 1366 bytes captured (10928 bits) on interface eth0, id 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Aug 20, 2022 07:26:53.721198200 PDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1661005613.721198200 seconds
[Time delta from previous captured frame: 0.021873800 seconds]
[Time delta from previous displayed frame: 62.720162700 seconds]
[Time since reference or first frame: 296.906723800 seconds]
Frame Number: 21159
Frame Length: 1366 bytes (10928 bits)
Capture Length: 1366 bytes (10928 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:png]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
Destination: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: b5689023.green.mattingsolutions.co (185.243.115.84)
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1352
Identification: 0x3d1c (15644)
Flags: 0x4000, Don't fragment
0000 00 15 c6 e6 c4 77 00 59 07 b0 63 a4 08 00 45 00
0010 05 48 3d 1c 40 00 80 06 da 6e ac 10 04 cd b9 f3


Final (1) - ml-lab-9325a05a-5c60-43ca-8b77-0c74bd4802f2.eastus.cloudapp.azure.com:50853 - Remote Desktop Connection
ImageMagick: empty.gif%3fss&ss2img
Recycle Bin

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/