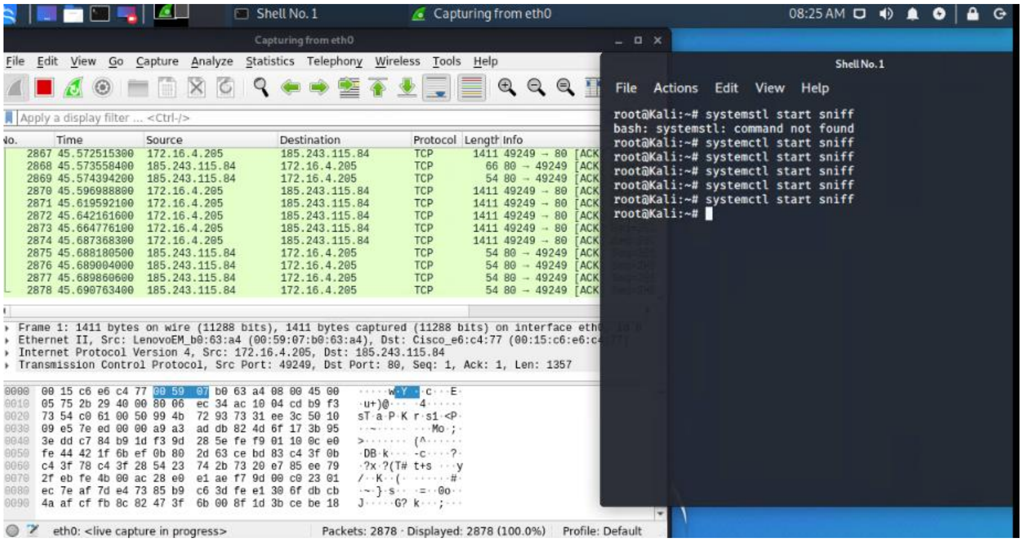
Ardavan Moghaddam

# Final Project

## Network Forensic Analysis Report (Network Template)

Opened a terminal window and run the command systemctl start sniff

Then Launched Wireshark and captured traffic on the eth0 interface.


Shell No. 1
Capturing from eth0
08:25 AM
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Shell No. 1
File Actions Edit View Help

```
No.   Time         Source          Destination     Protocol Length Info
 2867 45.572515300 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK
 2868 45.573558400 185.243.115.84  172.16.4.205    TCP        66 80 → 49249 [ACK
 2869 45.574394200 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK
 2870 45.596988800 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK
 2871 45.619592100 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK
 2872 45.642161600 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK
 2873 45.664776100 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK
 2874 45.687368300 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK
 2875 45.688180500 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK
 2876 45.689004000 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK
 2877 45.689860600 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK
 2878 45.690763400 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK
```

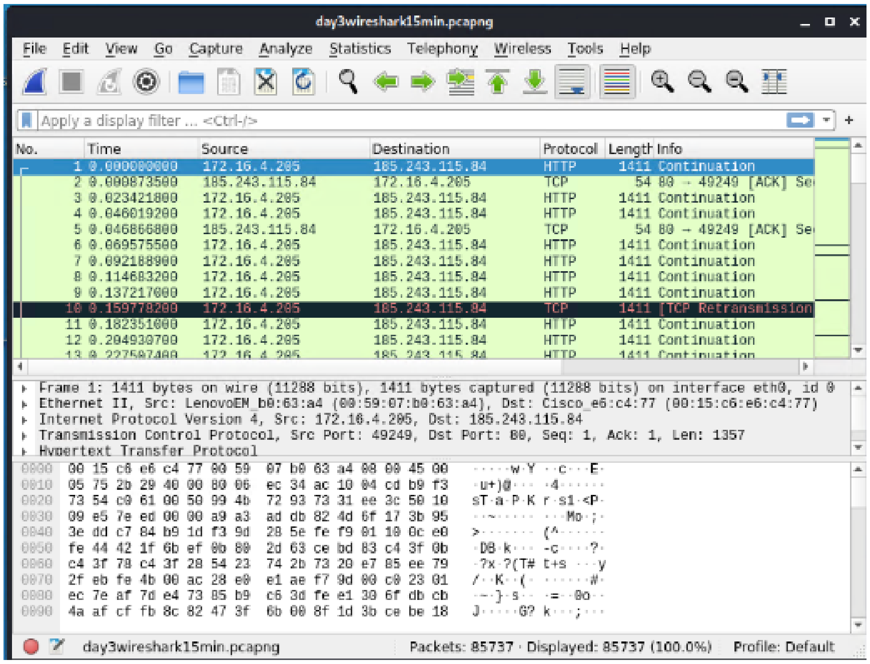
```
▸ Frame 1: 1411 bytes on wire (11288 bits), 1411 bytes captured (11288 bits) on interface eth
▸ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c
▸ Internet Protocol Version 4, Src: 172.16.4.205, Dst: 185.243.115.84
▸ Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 1, Ack: 1, Len: 1357
```

```
0000  00 15 c6 e6 c4 77 00 59  07 b0 63 a4 08 00 45 00   ·····w·Y ··c···E·
0010  05 75 2b 29 40 00 80 06  ec 34 ac 10 04 cd b9 f3   ·u+)@··· ·4······
0020  73 54 c0 61 00 50 99 4b  72 93 73 31 ee 3c 50 10   sT·a·P·K r·s1·<P·
0030  09 e5 7e ed 00 00 a9 a3  ad db 82 4d 6f 17 3b 95   ··~····· ···Mo·;·
0040  3e dd c7 84 b9 1d f3 9d  28 5e fe f9 01 10 0c e0   >······· (^······
0050  fe 44 42 1f 6b ef 0b 80  2d 63 ce bd 83 c4 3f 0b   ·DB·k··· -c····?·
0060  c4 3f 78 c4 3f 28 54 23  74 2b 73 20 e7 85 ee 79   ·?x·?(T# t+s ···y
0070  2f eb fe 4b 00 ac 28 e0  e1 ae f7 9d 00 c0 23 01   /··K··(· ······#·
0080  ec 7e af 7d e4 73 85 b9  c6 3d fe e1 30 6f db cb   ·~·}·s·· ·=··0o··
0090  4a af cf fb 8c 82 47 3f  6b 00 8f 1d 3b ce be 18   J·····G? k···;···
```

```
eth0: <live capture in progress>    Packets: 2878 · Displayed: 2878 (100.0%)    Profile: Default
```

```
root@Kali:~# systemstl start sniff
bash: systemstl: command not found
root@Kali:~# systemctl start sniff
root@Kali:~# systemctl start sniff
root@Kali:~# systemctl start sniff
root@Kali:~# systemctl start sniff
root@Kali:~# systemctl start sniff
root@Kali:~#
```

After 15 minutes run the command systemctl stop sniff to stop:


day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No. Time         Source          Destination     Protocol Length Info
  1 0.000000000  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
  2 0.000873500  185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK] Se
  3 0.023421800  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
  4 0.046019200  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
  5 0.046866800  185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK] Se
  6 0.069575500  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
  7 0.092188900  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
  8 0.114683200  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
  9 0.137217000  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
 10 0.159778200  172.16.4.205    185.243.115.84  TCP      1411 [TCP Retransmission
 11 0.182351000  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
 12 0.204930700  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
 13 0.227507400  172.16.4.205    185.243.115.84  HTTP     1411 Continuation
```

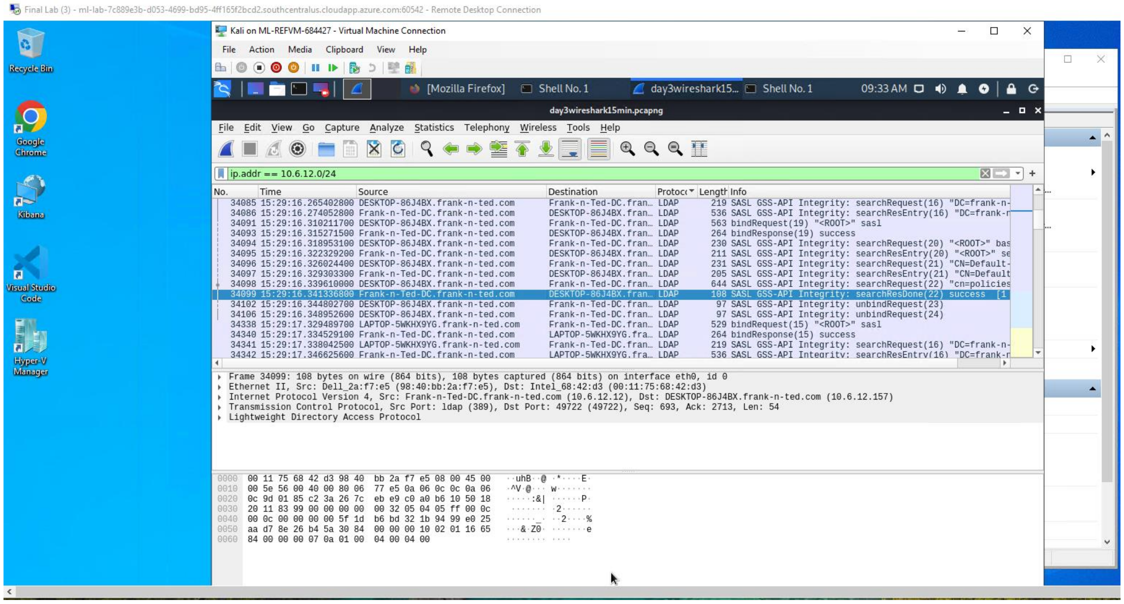
```
▸ Frame 1: 1411 bytes on wire (11288 bits), 1411 bytes captured (11288 bits) on interface eth0, id 0
▸ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
▸ Internet Protocol Version 4, Src: 172.16.4.205, Dst: 185.243.115.84
▸ Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 1, Ack: 1, Len: 1357
▸ Hypertext Transfer Protocol
```

```
0000  00 15 c6 e6 c4 77 00 59  07 b0 63 a4 08 00 45 00   ·····w·Y ··c···E·
0010  05 75 2b 29 40 00 80 06  ec 34 ac 10 04 cd b9 f3   ·u+)@··· ·4······
0020  73 54 c0 61 00 50 99 4b  72 93 73 31 ee 3c 50 10   sT·a·P·K r·s1·<P·
0030  09 e5 7e ed 00 00 a9 a3  ad db 82 4d 6f 17 3b 95   ··~····· ···Mo·;·
0040  3e dd c7 84 b9 1d f3 9d  28 5e fe f9 01 10 0c e0   >······· (^······
0050  fe 44 42 1f 6b ef 0b 80  2d 63 ce bd 83 c4 3f 0b   ·DB·k··· -c····?·
0060  c4 3f 78 c4 3f 28 54 23  74 2b 73 20 e7 85 ee 79   ·?x·?(T# t+s ···y
0070  2f eb fe 4b 00 ac 28 e0  e1 ae f7 9d 00 c0 23 01   /··K··(· ······#·
0080  ec 7e af 7d e4 73 85 b9  c6 3d fe e1 30 6f db cb   ·~·}·s·· ·=··0o··
0090  4a af cf fb 8c 82 47 3f  6b 00 8f 1d 3b ce be 18   J·····G? k···;···
```

```
day3wireshark15min.pcapng    Packets: 85737 · Displayed: 85737 (100.0%)    Profile: Default
```

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

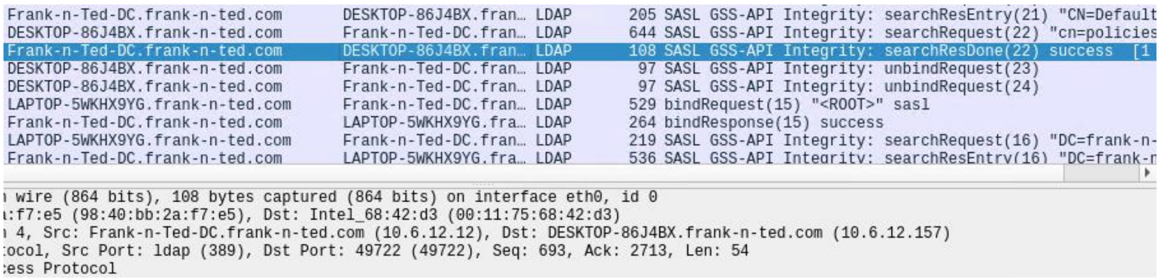
   Frank-n-ted-DC.frank-n-ted.com


Final Lab (3) - ml-lab-7c889e3b-d053-4699-bd95-4ff165f2bcd2.southcentralus.cloudapp.azure.com:60542 - Remote Desktop Connection
Recycle Bin
Google Chrome
Kibana
Visual Studio Code
Hyper-V Manager
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
[Mozilla Firefox]
Shell No. 1
day3wireshark15...
Shell No. 1
09:33 AM
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.6.12.0/24

No.   Time               Source                              Destination           Protoc Length Info
34085 15:29:16.265402800 DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP   219 SASL GSS-API Integrity: searchRequest(16) "DC=frank-n-
34086 15:29:16.274052800 Frank-n-Ted-DC.frank-n-ted.com      DESKTOP-86J4BX.fran… LDAP   536 SASL GSS-API Integrity: searchResEntry(16) "DC=frank-r
34091 15:29:16.310211700 DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP   563 bindRequest(19) "<ROOT>" sasl
34093 15:29:16.315271500 Frank-n-Ted-DC.frank-n-ted.com      DESKTOP-86J4BX.fran… LDAP   264 bindResponse(19) success
34094 15:29:16.318953100 DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP   230 SASL GSS-API Integrity: searchRequest(20) "<ROOT>" bas
34095 15:29:16.322329200 Frank-n-Ted-DC.frank-n-ted.com      DESKTOP-86J4BX.fran… LDAP   211 SASL GSS-API Integrity: searchResEntry(20) "<ROOT>" se
34096 15:29:16.326024400 DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP   231 SASL GSS-API Integrity: searchRequest(21) "CN=Default-
34097 15:29:16.329303300 Frank-n-Ted-DC.frank-n-ted.com      DESKTOP-86J4BX.fran… LDAP   205 SASL GSS-API Integrity: searchResEntry(21) "CN=Default
34098 15:29:16.339610000 DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP   644 SASL GSS-API Integrity: searchRequest(22) "cn=policies
34099 15:29:16.341336800 Frank-n-Ted-DC.frank-n-ted.com      DESKTOP-86J4BX.fran… LDAP   108 SASL GSS-API Integrity: searchResDone(22) success  [1
34102 15:29:16.344802700 DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP    97 SASL GSS-API Integrity: unbindRequest(23)
34106 15:29:16.348952600 DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP    97 SASL GSS-API Integrity: unbindRequest(24)
34338 15:29:17.329489700 LAPTOP-5WKHX9YG.frank-n-ted.com     Frank-n-Ted-DC.fran… LDAP   529 bindRequest(15) "<ROOT>" sasl
34340 15:29:17.334529100 Frank-n-Ted-DC.frank-n-ted.com      LAPTOP-5WKHX9YG.fra… LDAP   264 bindResponse(15) success
34341 15:29:17.338042500 LAPTOP-5WKHX9YG.frank-n-ted.com     Frank-n-Ted-DC.fran… LDAP   219 SASL GSS-API Integrity: searchRequest(16) "DC=frank-n-
34342 15:29:17.346625600 Frank-n-Ted-DC.frank-n-ted.com      LAPTOP-5WKHX9YG.fra… LDAP   536 SASL GSS-API Integrity: searchResEntry(16) "DC=frank-r

▸ Frame 34099: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
▸ Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel_68:42:d3 (00:11:75:68:42:d3)
▸ Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
▸ Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49722 (49722), Seq: 693, Ack: 2713, Len: 54
▸ Lightweight Directory Access Protocol

0000  00 11 75 68 42 d3 98 40  bb 2a f7 e5 08 00 45 00   ··uhB··@ ·*····E·
0010  00 5e 56 00 40 00 80 06  77 e5 0a 06 0c 0c 0a 06   ·^V·@··· w·······
0020  0c 9d 01 85 c2 3a 26 7c  eb e9 c0 a0 b6 10 50 18   ·····:&| ······P·
0030  20 11 83 99 00 00 00 00  00 32 05 04 05 ff 00 0c    ······· ·2······
0040  00 0c 00 00 00 00 5f 1d  b6 bd 32 1b 94 99 e0 25   ······_· ··2····%
0050  aa d7 8e 26 b4 5a 30 84  00 00 00 10 02 01 16 65   ···&·Z0· ·······e
0060  84 00 00 00 07 0a 01 00  04 00 04 00               ········ ····
```

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

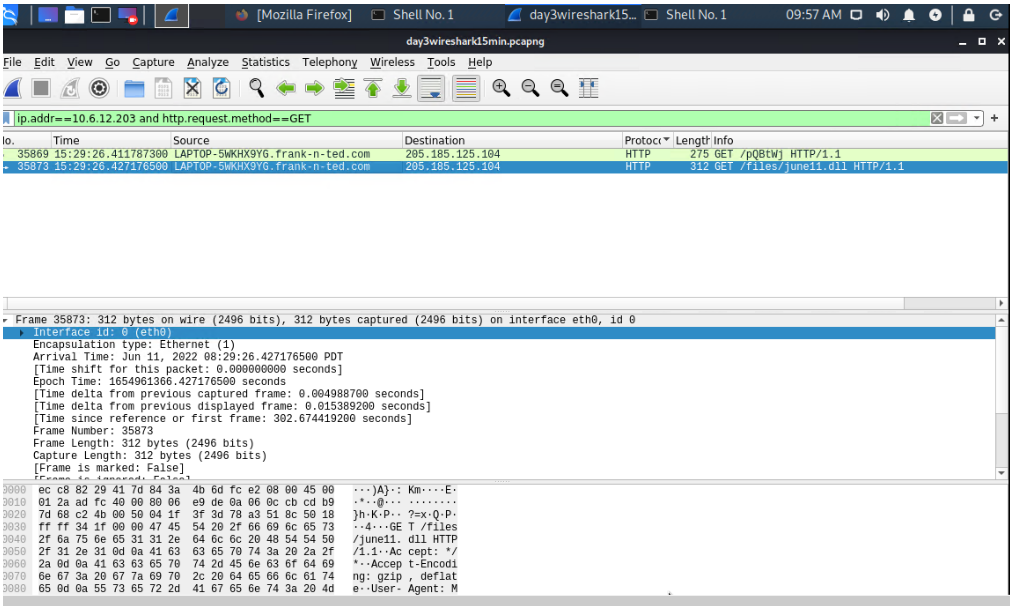
   10.6.12.157



```
Frank-n-Ted-DC.frank-n-ted.com      DESKTOP-86J4BX.fran… LDAP   205 SASL GSS-API Integrity: searchResEntry(21) "CN=Default
DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP   644 SASL GSS-API Integrity: searchRequest(22) "cn=policies
Frank-n-Ted-DC.frank-n-ted.com      DESKTOP-86J4BX.fran… LDAP   108 SASL GSS-API Integrity: searchResDone(22) success  [1
DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP    97 SASL GSS-API Integrity: unbindRequest(23)
DESKTOP-86J4BX.frank-n-ted.com      Frank-n-Ted-DC.fran… LDAP    97 SASL GSS-API Integrity: unbindRequest(24)
LAPTOP-5WKHX9YG.frank-n-ted.com     Frank-n-Ted-DC.fran… LDAP   529 bindRequest(15) "<ROOT>" sasl
Frank-n-Ted-DC.frank-n-ted.com      LAPTOP-5WKHX9YG.fra… LDAP   264 bindResponse(15) success
LAPTOP-5WKHX9YG.frank-n-ted.com     Frank-n-Ted-DC.fran… LDAP   219 SASL GSS-API Integrity: searchRequest(16) "DC=frank-n-
Frank-n-Ted-DC.frank-n-ted.com      LAPTOP-5WKHX9YG.fra… LDAP   536 SASL GSS-API Integrity: searchResEntry(16) "DC=frank-r

 wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel_68:42:d3 (00:11:75:68:42:d3)
 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
tocol, Src Port: ldap (389), Dst Port: 49722 (49722), Seq: 693, Ack: 2713, Len: 54
cess Protocol
```

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

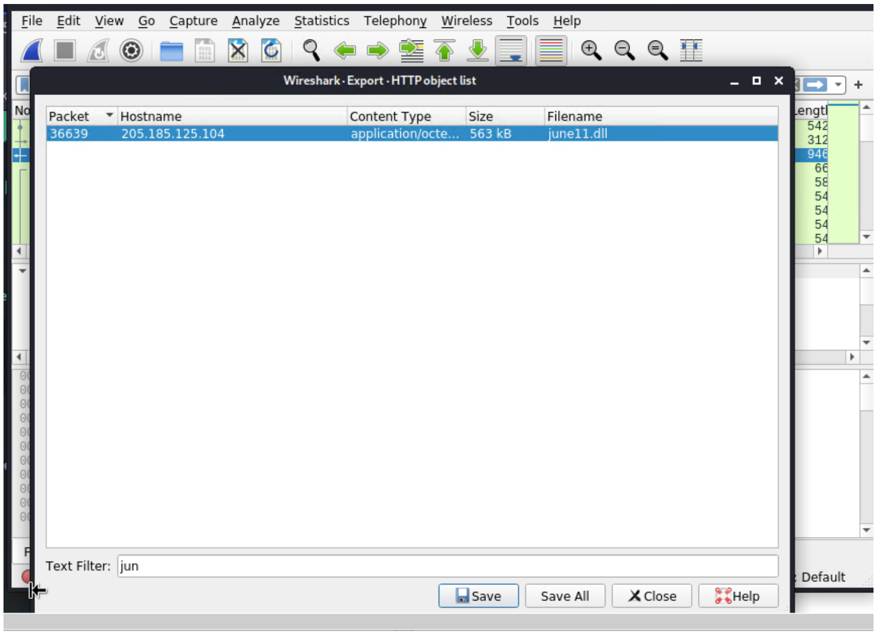

[Mozilla Firefox]
Shell No. 1
day3wireshark15...
Shell No. 1
09:57 AM
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==10.6.12.203 and http.request.method==GET
```

```
lo.   Time               Source                          Destination       Protoco Length Info
35869 15:29:26.411787300 LAPTOP-5WKHX9YG.frank-n-ted.com 205.185.125.104   HTTP    275 GET /pQBtWj HTTP/1.1
35873 15:29:26.427176500 LAPTOP-5WKHX9YG.frank-n-ted.com 205.185.125.104   HTTP    312 GET /files/june11.dll HTTP/1.1
```

```
Frame 35873: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
  Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Jun 11, 2022 08:29:26.427176500 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1654961366.427176500 seconds
  [Time delta from previous captured frame: 0.004988700 seconds]
  [Time delta from previous displayed frame: 0.015389200 seconds]
  [Time since reference or first frame: 302.674419200 seconds]
  Frame Number: 35873
  Frame Length: 312 bytes (2496 bits)
  Capture Length: 312 bytes (2496 bits)
  [Frame is marked: False]
```

```
0000  ec c8 82 29 41 7d 84 3a  4b 6d fc e2 08 00 45 00   ···)A}·: Km····E·
0010  01 2a ad fc 40 00 80 06  e9 de 0a 06 0c cb cd b9   ·*··@··· ········
0020  7d 68 c2 4b 00 50 04 1f  3f 3d 78 a3 51 8c 50 18   }h·K·P·· ?=x·Q·P·
0030  ff ff 34 1f 00 00 47 45  54 20 2f 66 69 6c 65 73   ··4···GE T /files
0040  2f 6a 75 6e 65 31 31 2e  64 6c 6c 20 48 54 54 50   /june11. dll HTTP
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
0070  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0080  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
```

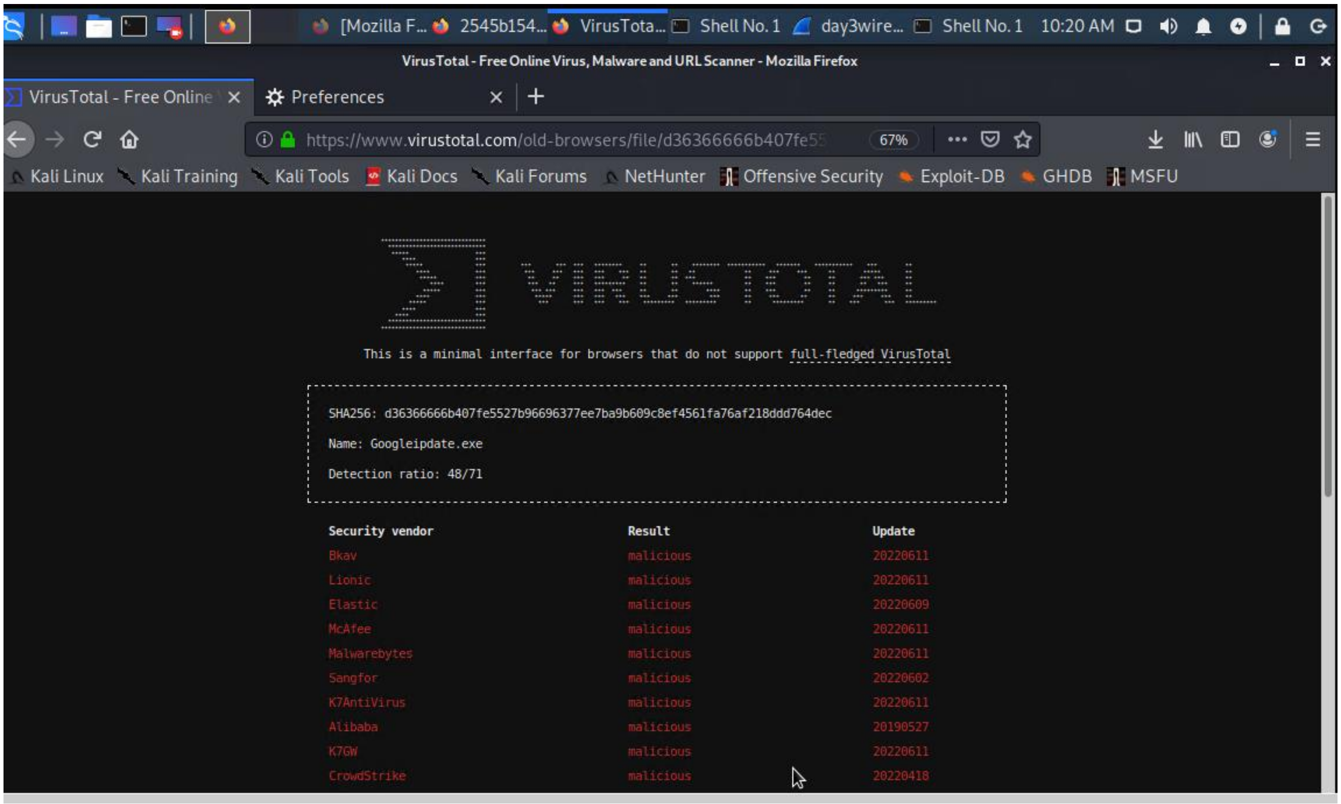

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Export · HTTP object list
Save
Save All
Close
Help
Default

| Packet | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 36639 | 205.185.125.104 | application/octe... | 563 kB | june11.dll |

Text Filter: jun

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

   Googleipdate.exe



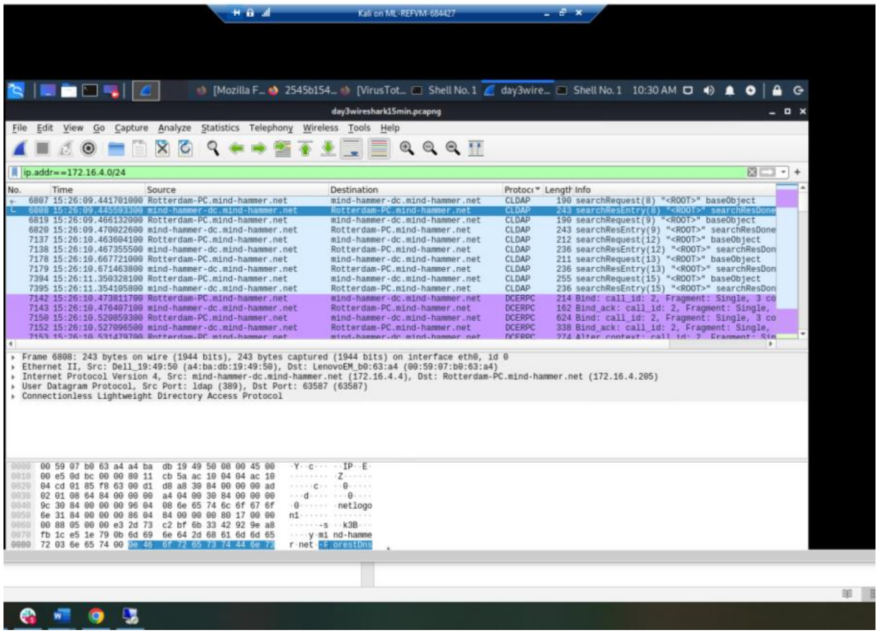
This is a minimal interface for browsers that do not support full-fledged VirusTotal

```
SHA256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Name: Googleipdate.exe

Detection ratio: 48/71
```

| Security vendor | Result | Update |
|---|---|---|
| Bkav | malicious | 20220611 |
| Lionic | malicious | 20220611 |
| Elastic | malicious | 20220609 |
| McAfee | malicious | 20220611 |
| Malwarebytes | malicious | 20220611 |
| Sangfor | malicious | 20220602 |
| K7AntiVirus | malicious | 20220611 |
| Alibaba | malicious | 20190527 |
| K7GW | malicious | 20220611 |
| CrowdStrike | malicious | 20220418 |

Vulnerable windows Machines

1. Find the following information about the infected Windows machine:
    - Host name: Rotterdam-pc.mindhammer.net
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4

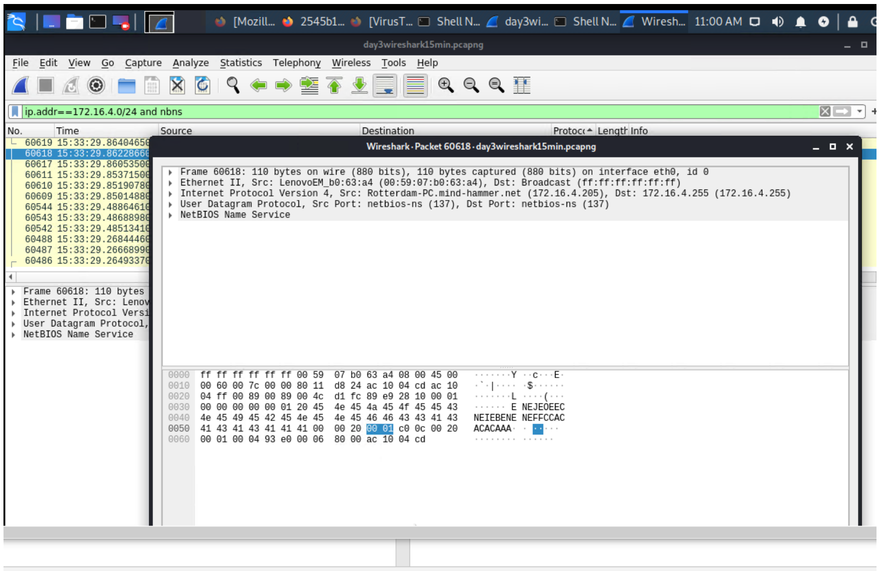


ip.addr==172.16.4.0/24

```
No.   Time               Source                           Destination                      Protocol Length Info
 6807 15:26:09.441701000 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   CLDAP    190 searchRequest(8) "<ROOT>" baseObject
 6808 15:26:09.445593300 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     CLDAP    243 searchResEntry(8) "<ROOT>" searchResDone
 6819 15:26:09.466132000 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   CLDAP    190 searchRequest(9) "<ROOT>" baseObject
 6820 15:26:09.470022600 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     CLDAP    243 searchResEntry(9) "<ROOT>" searchResDone
 7137 15:26:10.463604100 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   CLDAP    212 searchRequest(12) "<ROOT>" baseObject
 7138 15:26:10.467355500 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     CLDAP    236 searchResEntry(12) "<ROOT>" searchResDon
 7178 15:26:10.667721000 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   CLDAP    211 searchRequest(13) "<ROOT>" baseObject
 7179 15:26:10.671463800 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     CLDAP    236 searchResEntry(13) "<ROOT>" searchResDon
 7394 15:26:11.350328100 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   CLDAP    255 searchRequest(15) "<ROOT>" baseObject
 7395 15:26:11.354105800 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     CLDAP    236 searchResEntry(15) "<ROOT>" searchResDon
 7142 15:26:10.473811700 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   DCERPC   214 Bind: call_id: 2, Fragment: Single, 3 co
 7143 15:26:10.476407100 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     DCERPC   162 Bind_ack: call_id: 2, Fragment: Single,
 7150 15:26:10.520859300 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   DCERPC   624 Bind: call_id: 2, Fragment: Single, 3 co
 7152 15:26:10.527096500 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     DCERPC   338 Bind_ack: call_id: 2, Fragment: Single,
 7153 15:26:10.531479700 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   DCERPC   274 Alter context: call_id: 2, Fragment: Sin
```

```
Frame 6808: 243 bytes on wire (1944 bits), 243 bytes captured (1944 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: mind-hammer-dc.mind-hammer.net (172.16.4.4), Dst: Rotterdam-PC.mind-hammer.net (172.16.4.205)
User Datagram Protocol, Src Port: ldap (389), Dst Port: 63587 (63587)
Connectionless Lightweight Directory Access Protocol
```

```
0000  00 59 07 b0 63 a4 a4 ba  db 19 49 50 08 00 45 00   ·Y··c··· ··IP··E·
0010  00 e5 0d bc 00 00 80 11  cb 5a ac 10 04 04 ac 10   ········ ·Z······
0020  04 cd 01 85 f8 63 00 d1  d8 a8 30 84 00 00 00 ad   ·····c·· ··0·····
0030  02 01 08 64 84 00 00 00  a4 04 00 30 84 00 00 00   ···d···· ···0····
0040  9c 30 84 00 00 00 96 04  08 6e 65 74 6c 6f 67 6f   ·0······ ·netlogo
0050  6e 31 84 00 00 00 86 04  84 00 00 00 80 17 00 00   n1······ ········
0060  00 88 05 00 00 e3 2d 73  c2 bf 6b 33 42 92 9e a8   ······-s ··k3B···
0070  fb 1c e5 1e 79 0b 6d 69  6e 64 2d 68 61 6d 6d 65   ····y·mi nd-hamme
0080  72 03 6e 65 74 00 0e 46  6f 72 65 73 74 44 6e 73   r·net··F orestDns
```



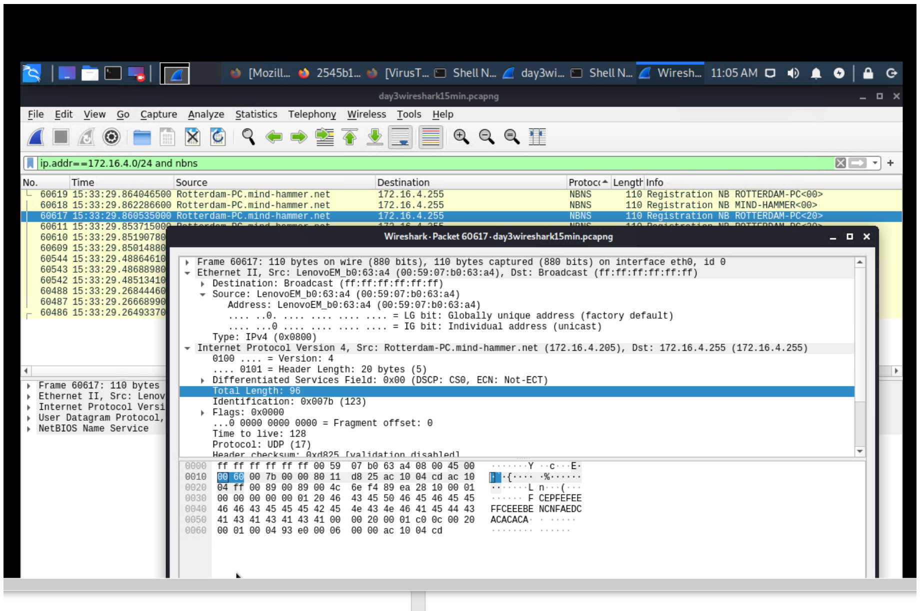
ip.addr==172.16.4.0/24 and nbns

```
No.   Time
60619 15:33:29.86404650
60618 15:33:29.86228660
60617 15:33:29.86053500
60611 15:33:29.85371500
60610 15:33:29.85190780
60609 15:33:29.85014880
60544 15:33:29.48864610
60543 15:33:29.48688980
60542 15:33:29.48513410
60488 15:33:29.26844460
60487 15:33:29.26668990
60486 15:33:29.26493370
```

Wireshark · Packet 60618 · day3wireshark15min.pcapng

```
Frame 60618: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 172.16.4.255 (172.16.4.255)
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff 00 59  07 b0 63 a4 08 00 45 00   ·······Y ··c···E·
0010  00 60 00 7c 00 00 80 11  d8 24 ac 10 04 cd ac 10   ·`·|···· ·$······
0020  04 ff 00 89 00 89 00 4c  d1 fc 89 e9 28 10 00 01   ·······L ····(···
0030  00 00 00 00 00 01 20 45  4e 45 4a 45 4f 45 45 43   ······ E NEJEOEEC
0040  4e 45 49 45 42 45 4e 45  4e 45 46 46 43 43 41 43   NEIEBENE NEFFCCAC
0050  41 43 41 43 41 41 41 00  00 20 00 01 c0 0c 00 20   ACACAAA· · ······
0060  00 01 00 04 93 e0 00 06  80 00 ac 10 04 cd         ········ ······
```


[Mozill... 2545b1... [VirusT... Shell N... day3wi... Shell N... Wiresh... 11:05 AM
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 60617 · day3wireshark15min.pcapng

```
ip.addr==172.16.4.0/24 and nbns
```

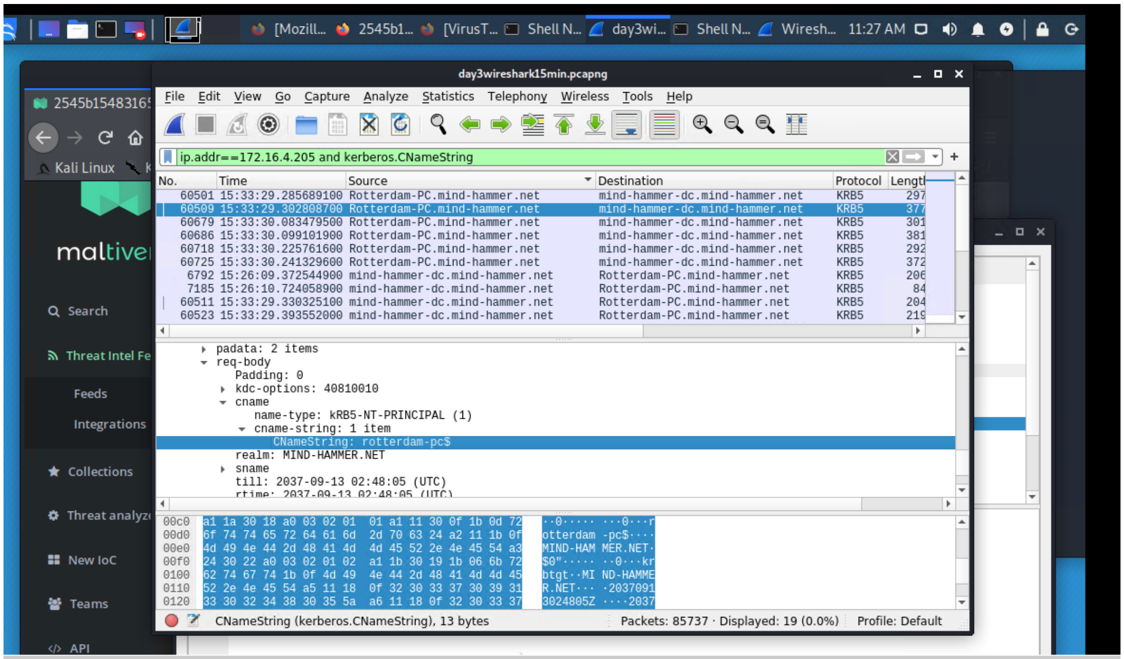
```
No.   Time               Source                       Destination    Protoco Length Info
60619 15:33:29.864046500 Rotterdam-PC.mind-hammer.net 172.16.4.255   NBNS    110 Registration NB ROTTERDAM-PC<00>
60618 15:33:29.862286600 Rotterdam-PC.mind-hammer.net 172.16.4.255   NBNS    110 Registration NB MIND-HAMMER<00>
60617 15:33:29.860535000 Rotterdam-PC.mind-hammer.net 172.16.4.255   NBNS    110 Registration NB ROTTERDAM-PC<20>
60611 15:33:29.853715000
60610 15:33:29.85190780
60609 15:33:29.85014880
60544 15:33:29.48864610
60543 15:33:29.48688980
60542 15:33:29.48513410
60488 15:33:29.26844460
60487 15:33:29.26668990
60486 15:33:29.26493370

Frame 60617: 110 bytes
Ethernet II, Src: Lenov
Internet Protocol Versi
User Datagram Protocol,
NetBIOS Name Service
```

```
Frame 60617: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
    Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 172.16.4.255 (172.16.4.255)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 96
  Identification: 0x007b (123)
  Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0xd825 [validation disabled]
```

```
0000  ff ff ff ff ff ff 00 59  07 b0 63 a4 08 00 45 00   ·······Y ··c···E·
0010  00 60 00 7b 00 00 80 11  d8 25 ac 10 04 cd ac 10   ·`·{···· ·%······
0020  04 ff 00 89 00 89 00 4c  6e f4 89 ea 28 10 00 01   ·······L n···(···
0030  00 00 00 00 00 01 20 46  43 45 50 46 45 46 45 45   ······ F CEPFEFEE
0040  46 46 43 45 45 45 42 45  4e 43 4e 46 41 45 44 43   FFCEEEBE NCNFAEDC
0050  41 43 41 43 41 43 41 00  00 20 00 01 c0 0c 00 20   ACACACA· · ······
0060  00 01 00 04 93 e0 00 06  00 00 ac 10 04 cd         ········ ······
```

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

Rotterdam-pc$


[Mozill... 2545b1... [VirusT... Shell N... day3wi... Shell N... Wiresh... 11:27 AM
2545b1548316
Kali Linux
maltive
Search
Threat Intel Fe
Feeds
Integrations
Collections
Threat analyz
New IoC
Teams
API
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==172.16.4.205 and kerberos.CNameString
```

```
No.   Time               Source                           Destination                      Protocol Length
60501 15:33:29.285689100 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   KRB5     297
60509 15:33:29.302808700 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   KRB5     377
60679 15:33:30.083479500 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   KRB5     301
60686 15:33:30.099101900 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   KRB5     381
60718 15:33:30.225761600 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   KRB5     292
60725 15:33:30.241329600 Rotterdam-PC.mind-hammer.net     mind-hammer-dc.mind-hammer.net   KRB5     372
 6792 15:26:09.372544900 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     KRB5     206
 7185 15:26:10.724058900 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     KRB5      84
60511 15:33:29.330325100 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     KRB5     204
60523 15:33:29.393552000 mind-hammer-dc.mind-hammer.net   Rotterdam-PC.mind-hammer.net     KRB5     219
```

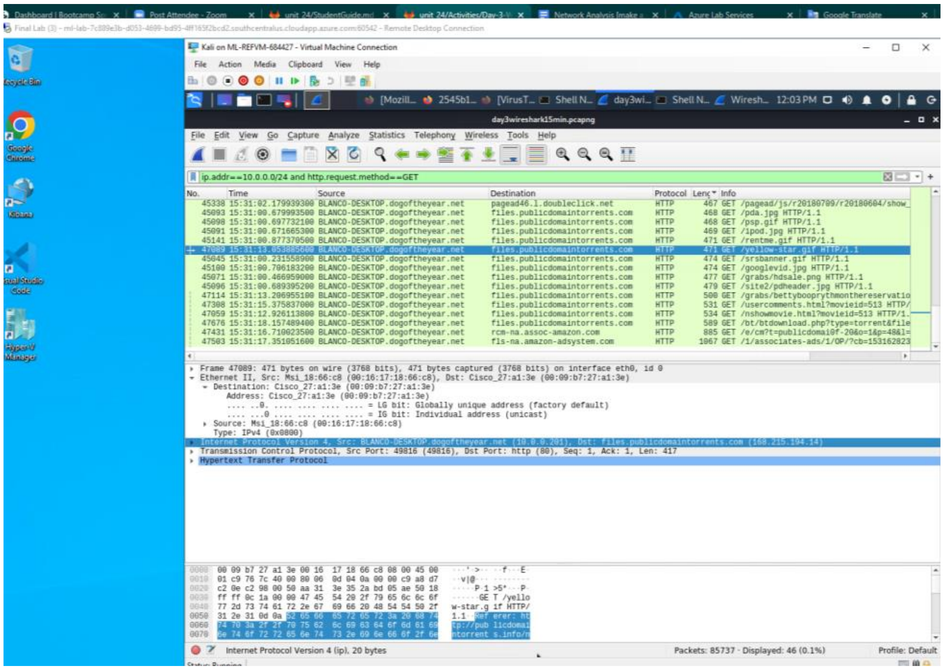
```
padata: 2 items
req-body
  Padding: 0
  kdc-options: 40810010
  cname
    name-type: kRB5-NT-PRINCIPAL (1)
    cname-string: 1 item
      CNameString: rotterdam-pc$
  realm: MIND-HAMMER.NET
  sname
  till: 2037-09-13 02:48:05 (UTC)
  rtime: 2037-09-13 02:48:05 (UTC)
```

```
00c0  a1 1a 30 18 a0 03 02 01  01 a1 11 30 0f 1b 0d 72   ··0····· ···0···r
00d0  6f 74 74 65 72 64 61 6d  2d 70 63 24 a2 11 1b 0f   otterdam -pc$····
00e0  4d 49 4e 44 2d 48 41 4d  4d 45 52 2e 4e 45 54 a3   MIND-HAM MER.NET·
00f0  24 30 22 a0 03 02 01 02  a1 1b 30 19 1b 06 6b 72   $0"····· ··0···kr
0100  62 74 67 74 1b 0f 4d 49  4e 44 2d 48 41 4d 4d 45   btgt··MI ND-HAMME
0110  52 2e 4e 45 54 a5 11 18  0f 32 30 33 37 30 39 31   R.NET··· ·2037091
0120  33 30 32 34 38 30 35 5a  a6 11 18 0f 32 30 33 37   3024805Z ····2037
```

CNameString (kerberos.CNameString), 13 bytes    Packets: 85737 · Displayed: 19 (0.0%)    Profile: Default

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

166.62.111.64


Dashboard | Bootcamp Sp
Post Attendee - Zoom
unit 24/StudentGuide.md
unit 24/Activities/Day-3-V
Network Analysis Imake
Azure Lab Services
Google Translate
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
[Mozill... 2545b1... [VirusT... Shell N... day3wi... Shell N... Wiresh... 12:03 PM
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Recycle Bin
Google Chrome
Kibana
Visual Studio Code
Hyper-V Manager

ip.addr==10.0.0.0/24 and http.request.method==GET

```
No.   Time               Source                        Destination                      Protocol Lenc Info
45338 15:31:02.179939300 BLANCO-DESKTOP.dogoftheyear.net pagead46.l.doubleclick.net       HTTP     467 GET /pagead/js/r20180709/r20180604/show_
45093 15:31:00.679993500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     468 GET /pda.jpg HTTP/1.1
45098 15:31:00.697732100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     468 GET /psp.gif HTTP/1.1
45091 15:31:00.671665300 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     469 GET /ipod.jpg HTTP/1.1
45141 15:31:00.877370500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     471 GET /rentme.gif HTTP/1.1
47089 15:31:13.053885600 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     471 GET /yellow-star.gif HTTP/1.1
45045 15:31:00.231558900 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     474 GET /srsbanner.gif HTTP/1.1
45100 15:31:00.706183200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     474 GET /googlevid.jpg HTTP/1.1
45071 15:31:00.466959000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     477 GET /grabs/hdsale.png HTTP/1.1
45096 15:31:00.689395200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     479 GET /site2/pdheader.jpg HTTP/1.1
47114 15:31:13.206955100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     500 GET /grabs/bettybooprythmonthereservatio
47308 15:31:15.375837000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     531 GET /usercomments.html?movieid=513 HTTP/
47059 15:31:12.926113800 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     534 GET /nshowmovie.html?movieid=513 HTTP/1.
47676 15:31:18.157489400 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP     589 GET /bt/btdownload.php?type=torrent&file
47431 15:31:16.710023500 BLANCO-DESKTOP.dogoftheyear.net rcm-na.assoc-amazon.com          HTTP     885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=
47503 15:31:17.351051600 BLANCO-DESKTOP.dogoftheyear.net fls-na.amazon-adsystem.com       HTTP    1067 GET /1/associates-ads/1/OP/?cb=153162823
```

```
▸ Frame 47089: 471 bytes on wire (3768 bits), 471 bytes captured (3768 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)
      Address: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▸ Source: Msi_18:66:c8 (00:16:17:18:66:c8)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
▸ Transmission Control Protocol, Src Port: 49816 (49816), Dst Port: http (80), Seq: 1, Ack: 1, Len: 417
▸ Hypertext Transfer Protocol
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  01 c9 76 7c 40 00 80 06  0d 04 0a 00 00 c9 a8 d7   ··v|@··· ········
0020  c2 0e c2 98 00 50 aa 31  3e 35 2a bd 05 ae 50 18   ·····P·1 >5*···P·
0030  ff ff 0c 1a 00 00 47 45  54 20 2f 79 65 6c 6c 6f   ······GE T /yello
0040  77 2d 73 74 61 72 2e 67  69 66 20 48 54 54 50 2f   w-star.g if HTTP/
0050  31 2e 31 0d 0a 52 65 66  65 72 65 72 3a 20 68 74   1.1··Ref erer: ht
0060  74 70 3a 2f 2f 70 75 62  6c 69 63 64 6f 6d 61 69   tp://pub licdomai
0070  6e 74 6f 72 72 65 6e 74  73 2e 69 6e 66 6f 2f 6e   ntorrent s.info/n
```

Internet Protocol Version 4 (ip), 20 bytes

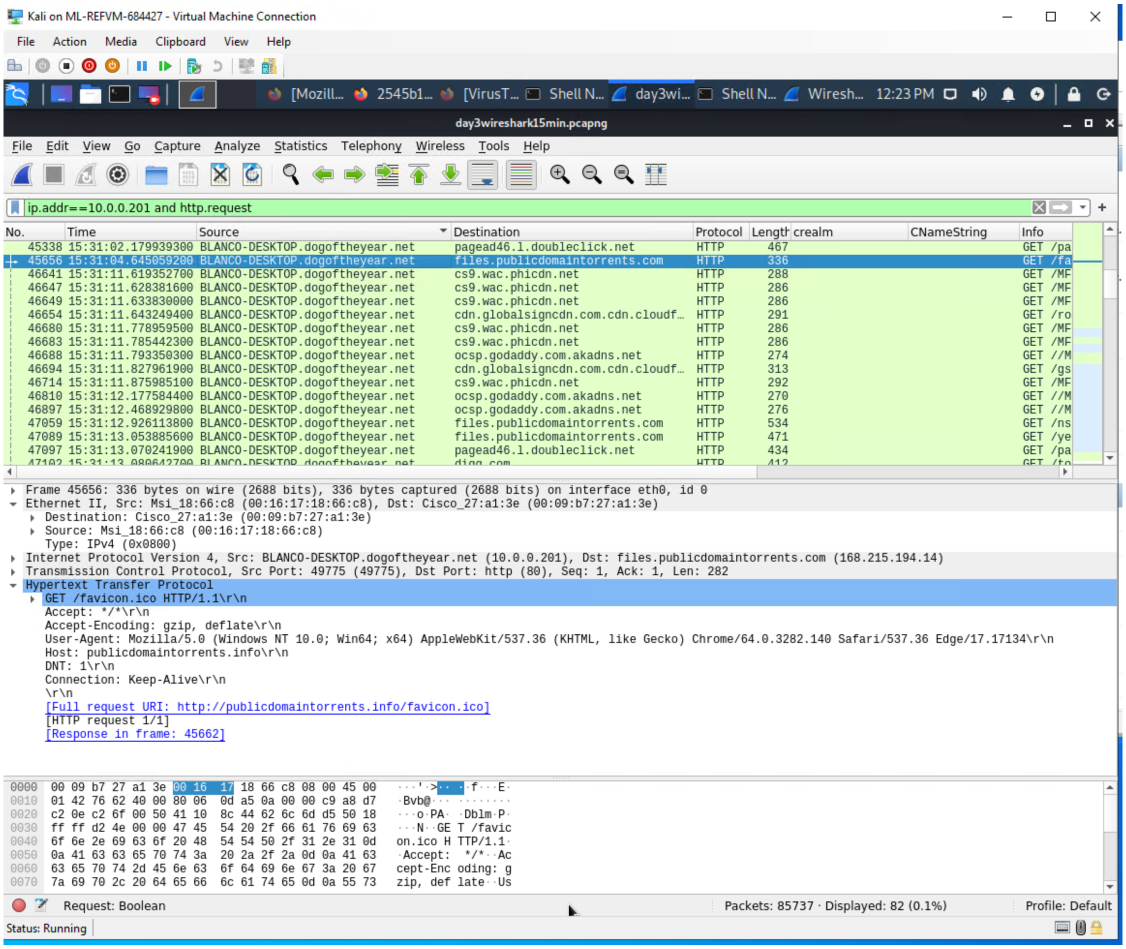
Packets: 85737 · Displayed: 46 (0.1%)

Profile: Default

Status: Running

# Illegal Downloads

1. 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
   - OS version : Windows NT 10.0



Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
[Mozill... 2545b1... [VirusT... Shell N... day3wi... Shell N... Wiresh... 12:23 PM
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.0.201 and http.request

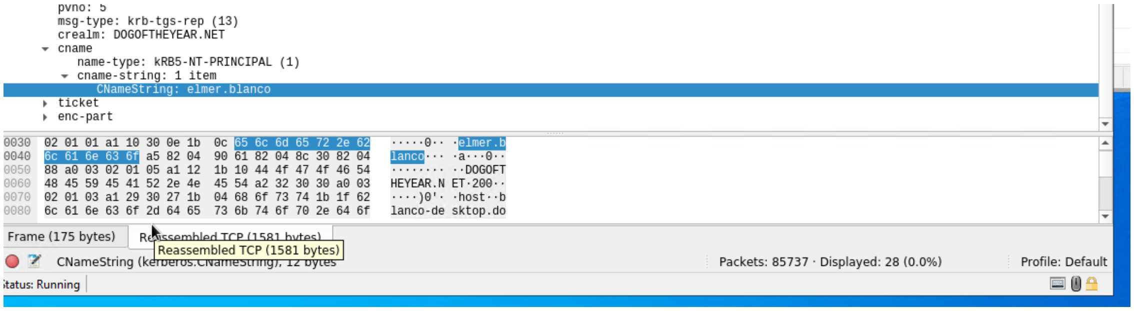
```
No.    Time               Source                            Destination                          Protocol Length crealm CNameString Info
 45338 15:31:02.179939300 BLANCO-DESKTOP.dogoftheyear.net  pagead46.l.doubleclick.net           HTTP     467                        GET /pa
 45656 15:31:04.645059200 BLANCO-DESKTOP.dogoftheyear.net  files.publicdomaintorrents.com       HTTP     336                        GET /fa
 46641 15:31:11.619352700 BLANCO-DESKTOP.dogoftheyear.net  cs9.wac.phicdn.net                   HTTP     288                        GET /MF
 46647 15:31:11.628381600 BLANCO-DESKTOP.dogoftheyear.net  cs9.wac.phicdn.net                   HTTP     286                        GET /MF
 46649 15:31:11.633830000 BLANCO-DESKTOP.dogoftheyear.net  cs9.wac.phicdn.net                   HTTP     286                        GET /MF
 46654 15:31:11.643249400 BLANCO-DESKTOP.dogoftheyear.net  cdn.globalsigncdn.com.cdn.cloudf…    HTTP     291                        GET /ro
 46680 15:31:11.778959500 BLANCO-DESKTOP.dogoftheyear.net  cs9.wac.phicdn.net                   HTTP     286                        GET /MF
 46683 15:31:11.785442300 BLANCO-DESKTOP.dogoftheyear.net  cs9.wac.phicdn.net                   HTTP     286                        GET /MF
 46688 15:31:11.793350300 BLANCO-DESKTOP.dogoftheyear.net  ocsp.godaddy.com.akadns.net          HTTP     274                        GET //M
 46694 15:31:11.827961900 BLANCO-DESKTOP.dogoftheyear.net  cdn.globalsigncdn.com.cdn.cloudf…    HTTP     313                        GET /gs
 46714 15:31:11.875985100 BLANCO-DESKTOP.dogoftheyear.net  cs9.wac.phicdn.net                   HTTP     292                        GET /MF
 46810 15:31:12.177584400 BLANCO-DESKTOP.dogoftheyear.net  ocsp.godaddy.com.akadns.net          HTTP     270                        GET //M
 46897 15:31:12.468929800 BLANCO-DESKTOP.dogoftheyear.net  ocsp.godaddy.com.akadns.net          HTTP     276                        GET //M
 47059 15:31:12.926113800 BLANCO-DESKTOP.dogoftheyear.net  files.publicdomaintorrents.com       HTTP     534                        GET /ns
 47089 15:31:13.053885600 BLANCO-DESKTOP.dogoftheyear.net  files.publicdomaintorrents.com       HTTP     471                        GET /ye
 47097 15:31:13.070241900 BLANCO-DESKTOP.dogoftheyear.net  pagead46.l.doubleclick.net           HTTP     434                        GET /pa
 47102 15:31:13.080642700 BLANCO-DESKTOP.dogoftheyear.net  digg.com                             HTTP     412                        GET /to
```

```
Frame 45656: 336 bytes on wire (2688 bits), 336 bytes captured (2688 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: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
Transmission Control Protocol, Src Port: 49775 (49775), Dst Port: http (80), Seq: 1, Ack: 1, Len: 282
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
  Accept: */*\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/537.36 Edge/17.17134\r\n
  Host: publicdomaintorrents.info\r\n
  DNT: 1\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://publicdomaintorrents.info/favicon.ico]
  [HTTP request 1/1]
  [Response in frame: 45662]
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  01 42 76 62 40 00 80 06  0d a5 0a 00 00 c9 a8 d7   ·Bvb@··· ········
0020  c2 0e c2 6f 00 50 41 10  8c 44 62 6c 6d d5 50 18   ···o·PA· ·Dblm·P·
0030  ff ff d2 4e 00 00 47 45  54 20 2f 66 61 76 69 63   ···N··GE T /favic
0040  6f 6e 2e 69 63 6f 20 48  54 54 50 2f 31 2e 31 0d   on.ico H TTP/1.1·
0050  0a 41 63 63 65 70 74 3a  20 2a 2f 2a 0d 0a 41 63   ·Accept:  */*··Ac
0060  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0070  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 55 73   zip, def late··Us
```

Request: Boolean    Packets: 85737 · Displayed: 82 (0.1%)    Profile: Default

Status: Running



```
  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
```

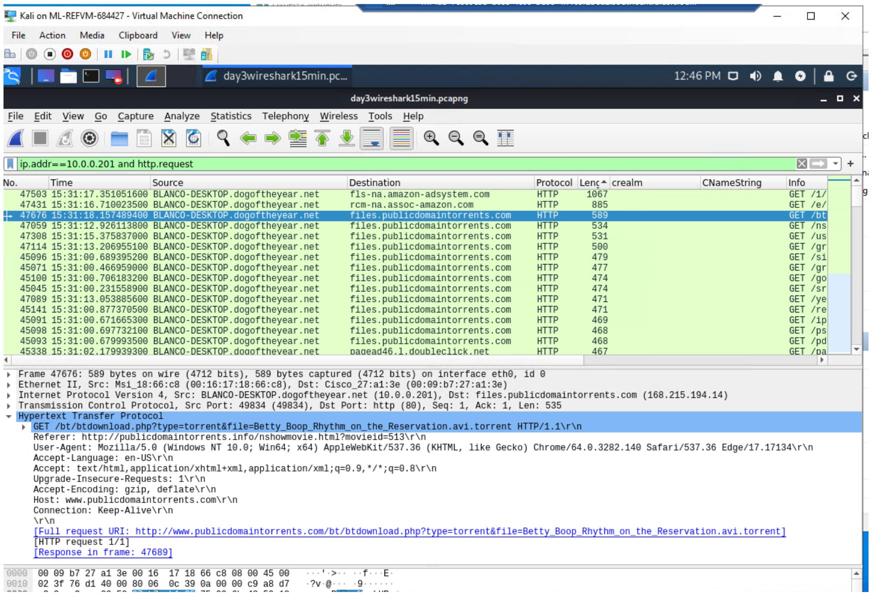
```
0030  02 01 01 a1 10 30 0e 1b  0c 65 6c 6d 65 72 2e 62   ·····0·· ·elmer.b
0040  6c 61 6e 63 6f a5 82 04  90 61 82 04 8c 30 82 04   lanco··· ·a···0··
0050  88 a0 03 02 01 05 a1 12  1b 10 44 4f 47 4f 46 54   ········ ··DOGOFT
0060  48 45 59 45 41 52 2e 4e  45 54 a2 32 30 30 a0 03   HEYEAR.N ET·200··
0070  02 01 03 a1 29 30 27 1b  04 68 6f 73 74 1b 1f 62   ····)0'· ·host··b
0080  6c 61 6e 63 6f 2d 64 65  73 6b 74 6f 70 2e 64 6f   lanco-de sktop.do
```

Frame (175 bytes)    Reassembled TCP (1581 bytes)

Reassembled TCP (1581 bytes)

CNameString (kerberos.CNameString), 12 bytes    Packets: 85737 · Displayed: 28 (0.0%)    Profile: Default

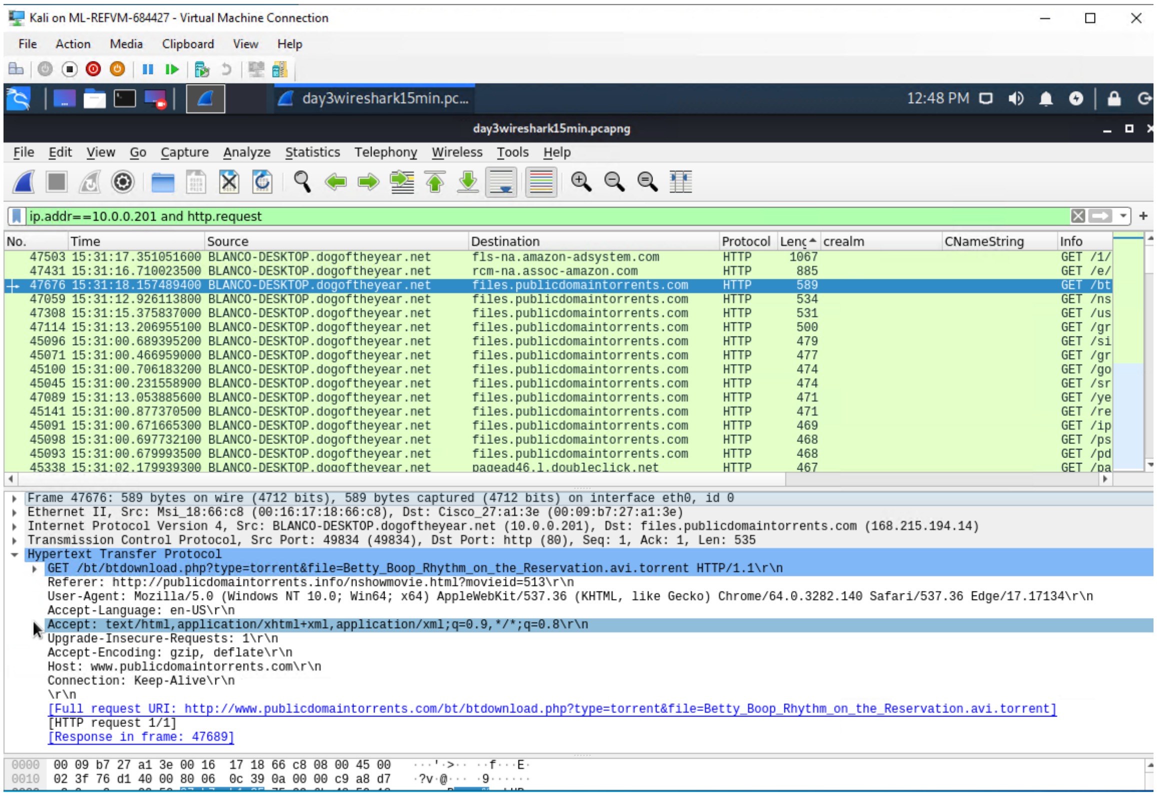
Status: Running


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
day3wireshark15min.pc...
12:46 PM
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==10.0.0.201 and http.request

No.   Time               Source                          Destination                      Protocol Leng crealm  CNameString  Info
47503 15:31:17.351051600 BLANCO-DESKTOP.dogoftheyear.net fls-na.amazon-adsystem.com       HTTP     1067                      GET /1/
47431 15:31:16.710023500 BLANCO-DESKTOP.dogoftheyear.net rcm-na.assoc-amazon.com          HTTP      885                      GET /e/
47676 15:31:18.157489400 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      589                      GET /bt
47059 15:31:12.926113800 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      534                      GET /ns
47308 15:31:15.375837000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      531                      GET /us
47114 15:31:13.206955100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      500                      GET /gr
45096 15:31:00.689395200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      479                      GET /si
45071 15:31:00.466959000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      477                      GET /gr
45100 15:31:00.706183200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      474                      GET /go
45045 15:31:00.231558900 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      474                      GET /sr
47089 15:31:13.053885600 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      471                      GET /ye
45141 15:31:00.877370500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      471                      GET /re
45091 15:31:00.671665300 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      469                      GET /ip
45098 15:31:00.697732100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      468                      GET /ps
45093 15:31:00.679993500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      468                      GET /pd
45338 15:31:02.179939300 BLANCO-DESKTOP.dogoftheyear.net pagead46.l.doubleclick.net       HTTP      467                      GET /pa

Frame 47676: 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)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (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
  Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\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/537.36 Edge/17.17134\r\n
  Accept-Language: en-US\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: www.publicdomaintorrents.com\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
  [HTTP request 1/1]
  [Response in frame: 47689]

0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  02 3f 76 d1 40 00 80 06  0c 39 0a 00 00 c9 a8 d7   ·?v·@··· ·9······
```

2.Which torrent file did the user download?

Betty_Boop_Rhythm_On_The_Reservation.avi.torrent


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
day3wireshark15min.pc...
12:48 PM
day3wireshark15min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==10.0.0.201 and http.request

No.   Time               Source                          Destination                      Protocol Leng crealm  CNameString  Info
47503 15:31:17.351051600 BLANCO-DESKTOP.dogoftheyear.net fls-na.amazon-adsystem.com       HTTP     1067                      GET /1/
47431 15:31:16.710023500 BLANCO-DESKTOP.dogoftheyear.net rcm-na.assoc-amazon.com          HTTP      885                      GET /e/
47676 15:31:18.157489400 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      589                      GET /bt
47059 15:31:12.926113800 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      534                      GET /ns
47308 15:31:15.375837000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      531                      GET /us
47114 15:31:13.206955100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      500                      GET /gr
45096 15:31:00.689395200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      479                      GET /si
45071 15:31:00.466959000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      477                      GET /gr
45100 15:31:00.706183200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      474                      GET /go
45045 15:31:00.231558900 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      474                      GET /sr
47089 15:31:13.053885600 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      471                      GET /ye
45141 15:31:00.877370500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      471                      GET /re
45091 15:31:00.671665300 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      469                      GET /ip
45098 15:31:00.697732100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      468                      GET /ps
45093 15:31:00.679993500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com   HTTP      468                      GET /pd
45338 15:31:02.179939300 BLANCO-DESKTOP.dogoftheyear.net pagead46.l.doubleclick.net       HTTP      467                      GET /pa

Frame 47676: 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)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (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
  Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\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/537.36 Edge/17.17134\r\n
  Accept-Language: en-US\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: www.publicdomaintorrents.com\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
  [HTTP request 1/1]
  [Response in frame: 47689]

0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  02 3f 76 d1 40 00 80 06  0c 39 0a 00 00 c9 a8 d7   ·?v·@··· ·9······
```