Network Analysis

Time Thieves

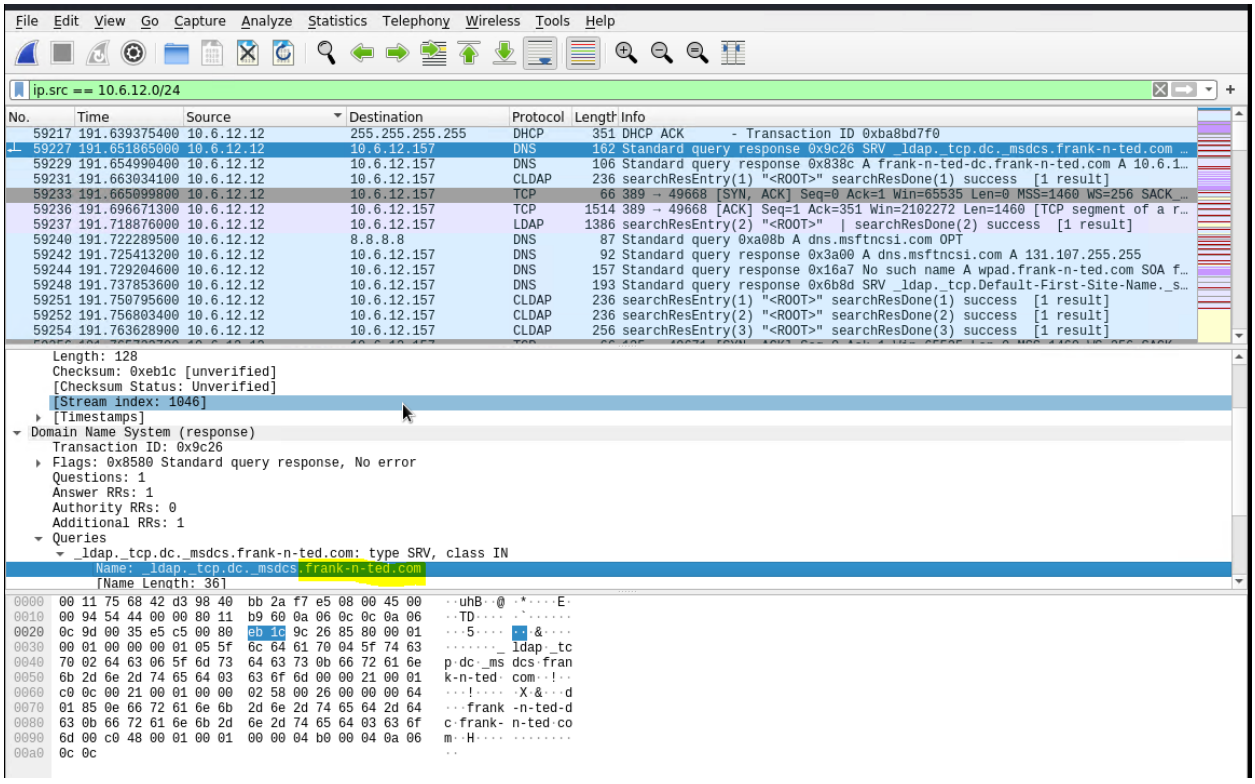
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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:

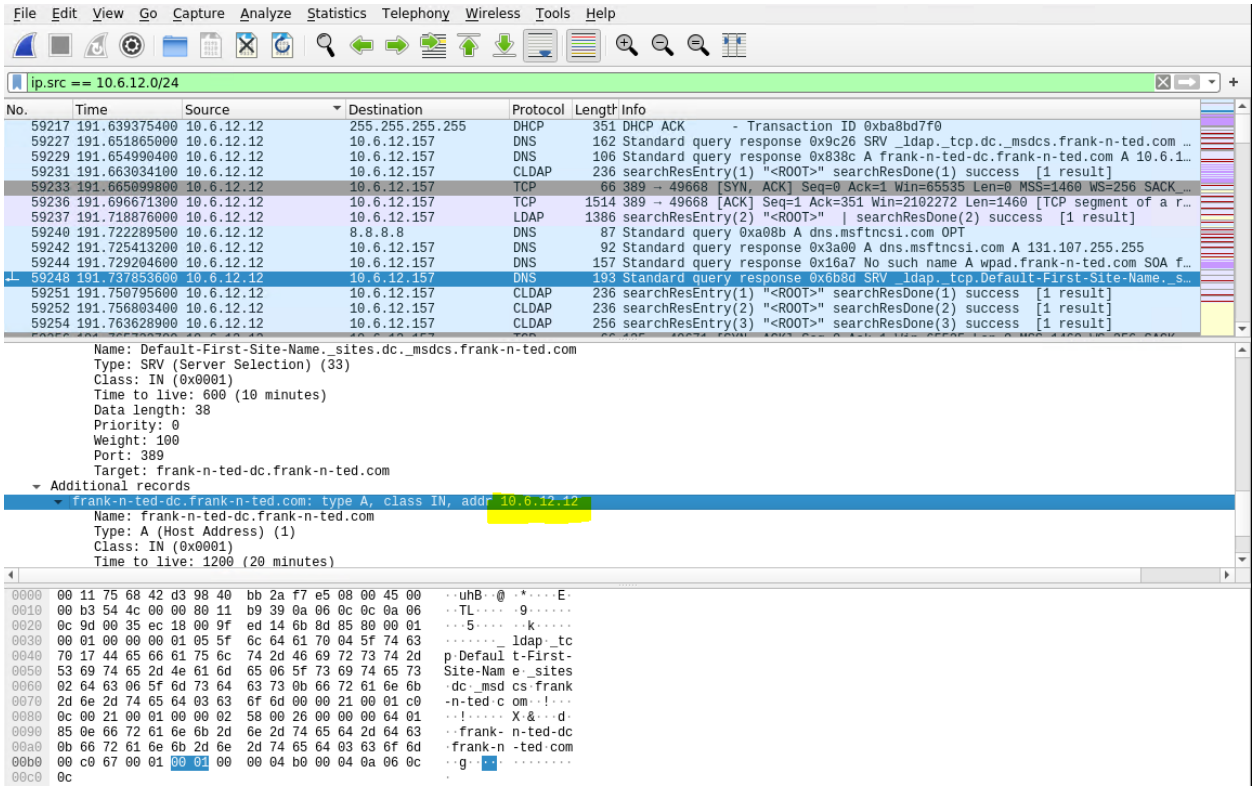
1. What is the domain name of the users' custom site?

   frank-n-ted.com

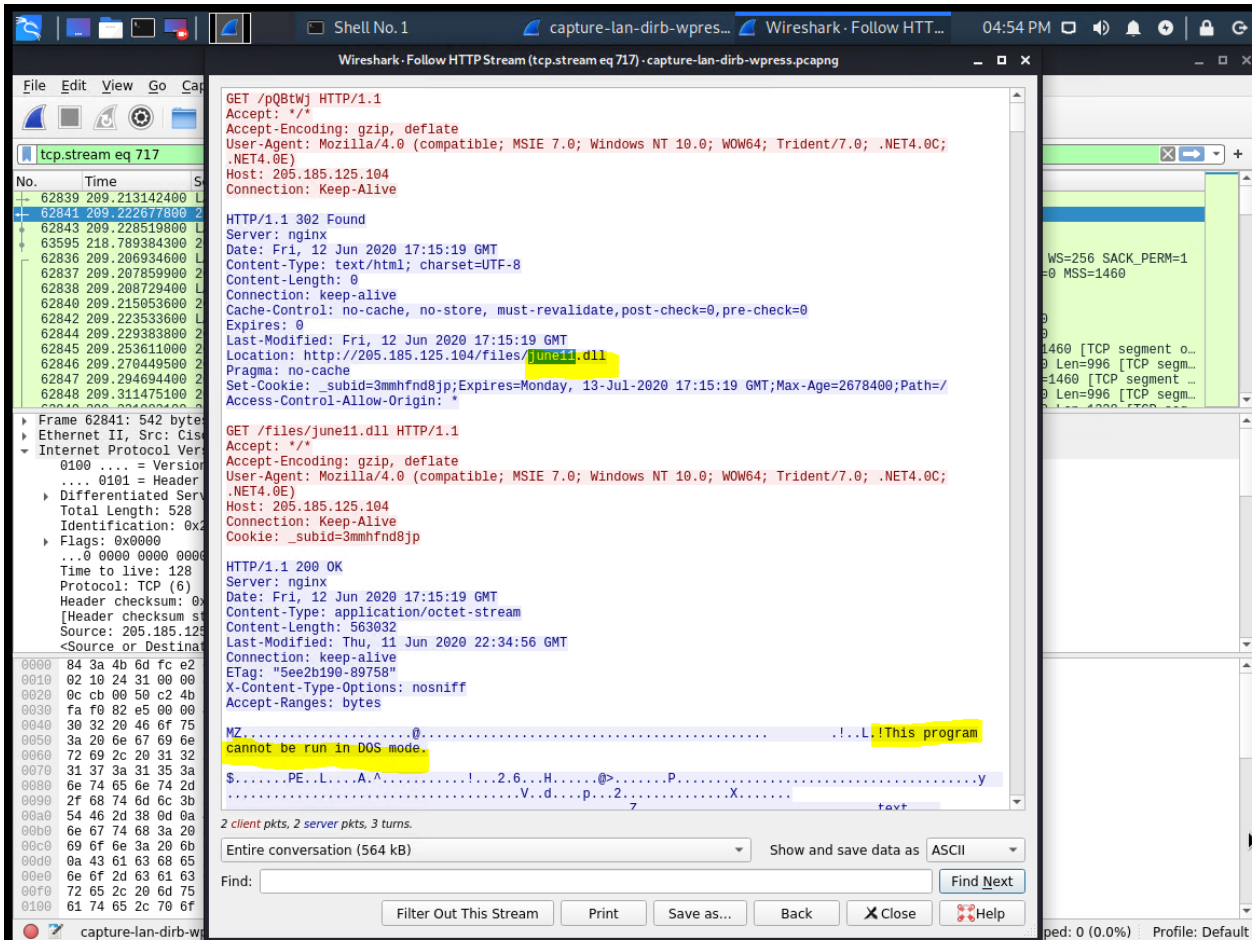


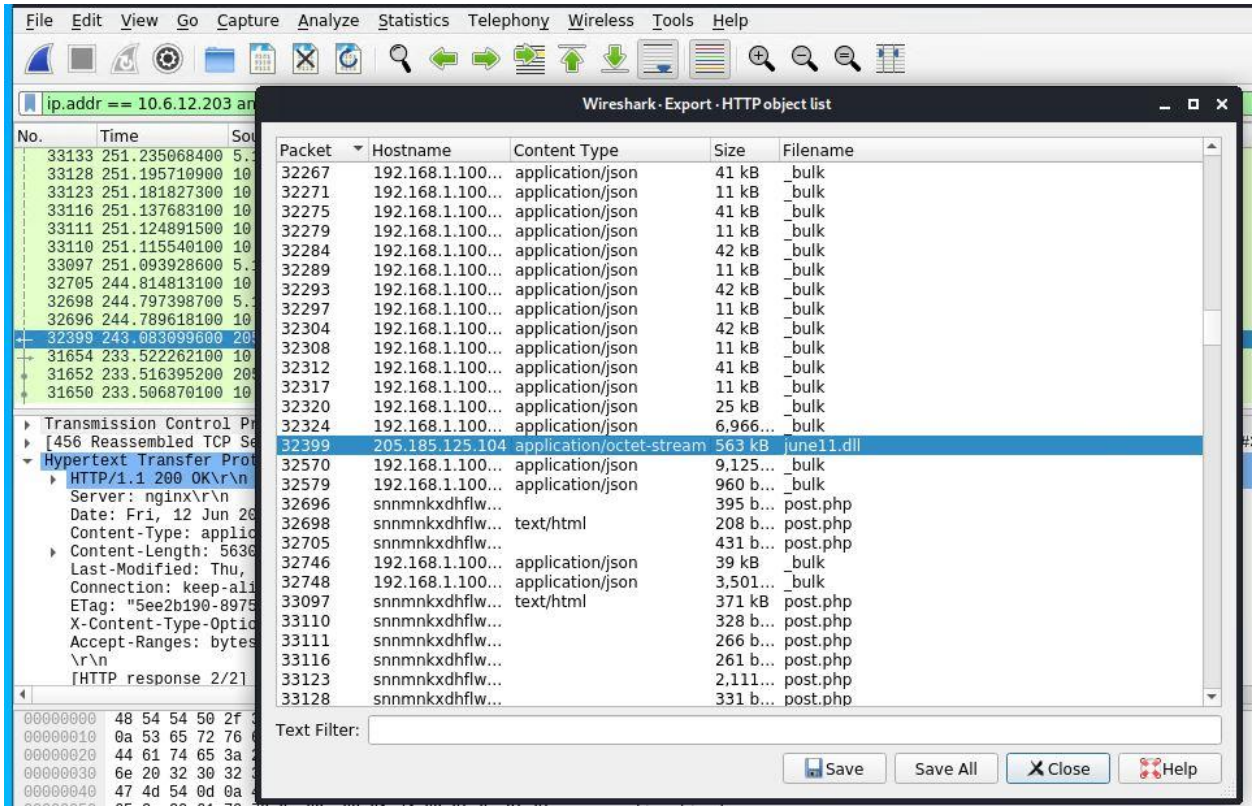
2. What is the IP address of the Domain Controller (DC) of the AD network?

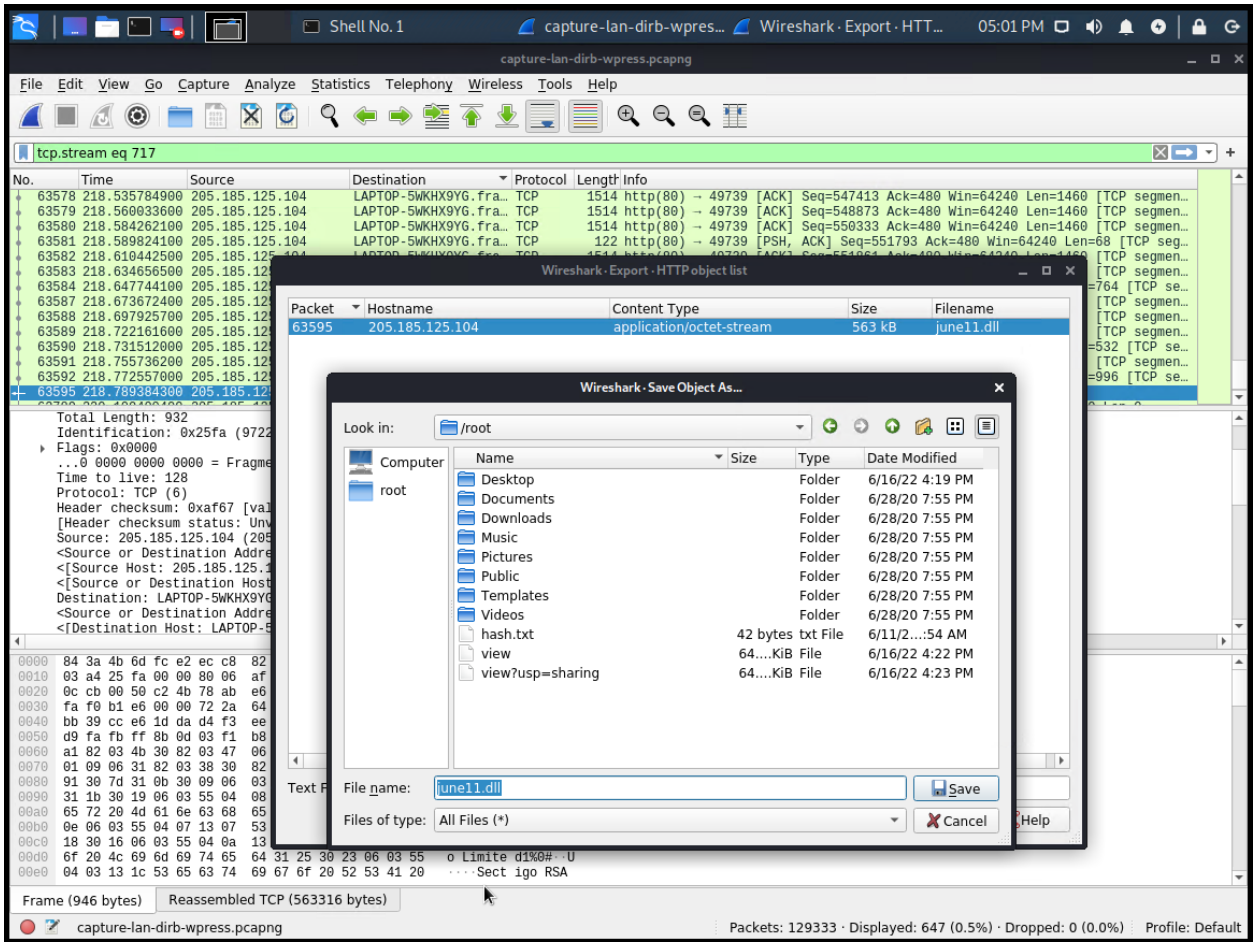
10.6.12.12



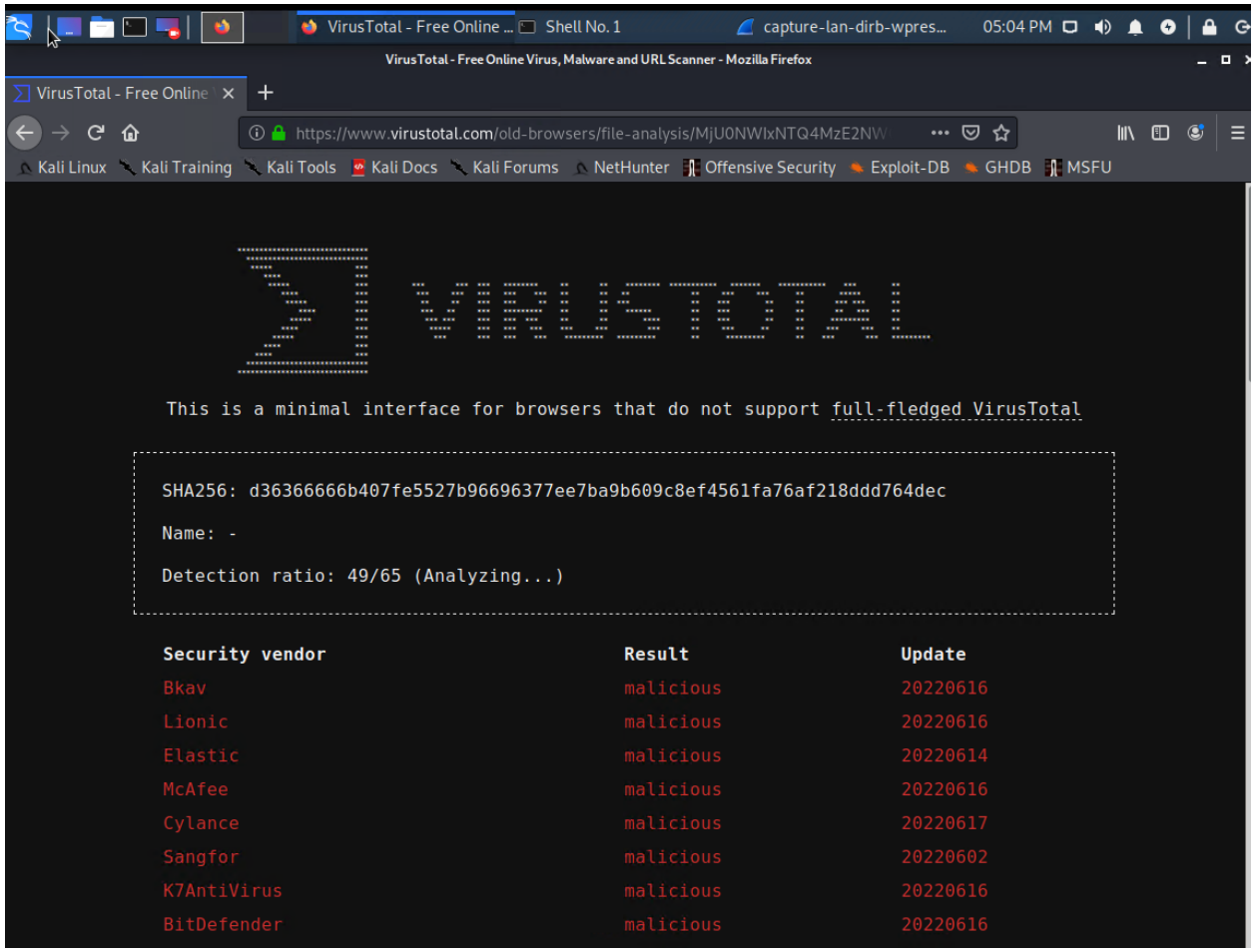
3. What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.

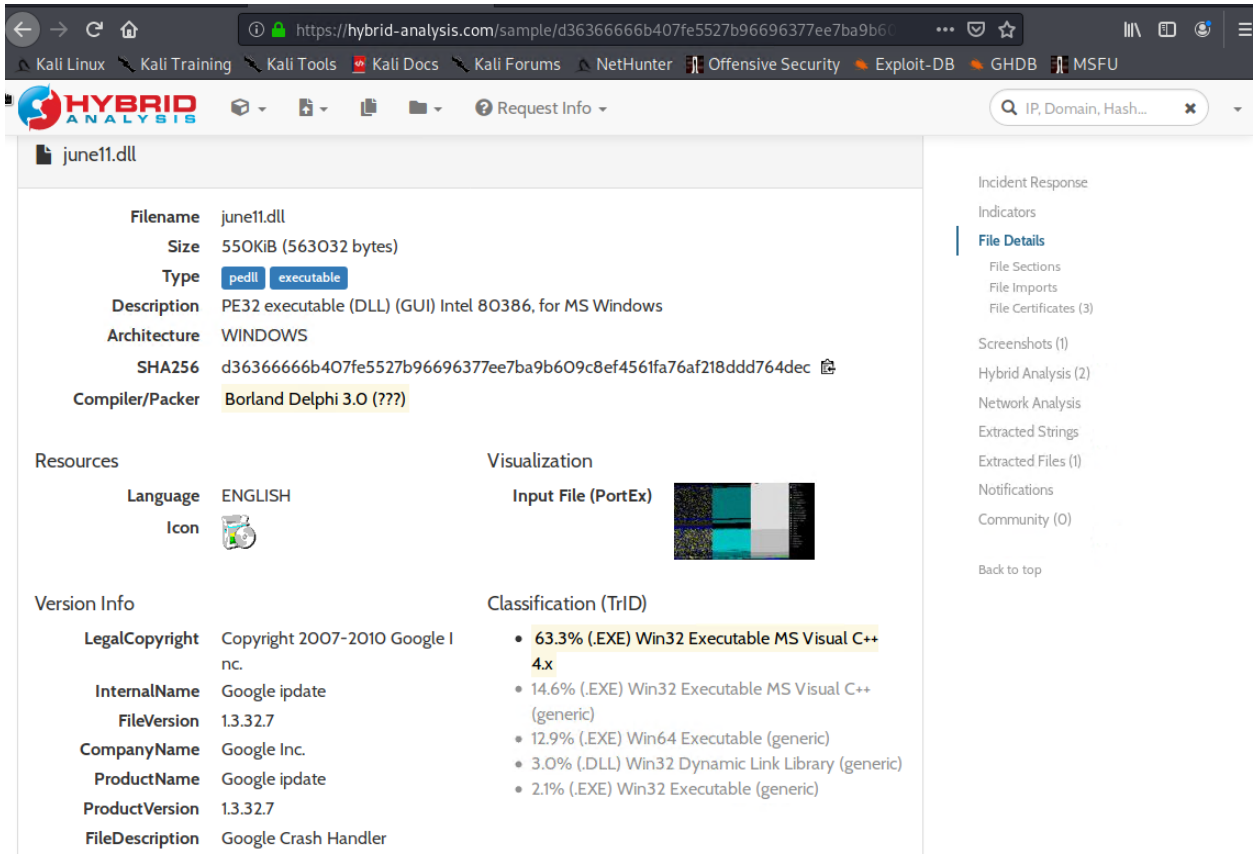

Shell No. 1
capture-lan-dirb-wpres...
Wireshark · Follow HTT...
04:54 PM
Wireshark · Follow HTTP Stream (tcp.stream eq 717) · capture-lan-dirb-wpress.pcapng
GET /pQBtWj HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
HTTP/1.1 302 Found
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-Age=2678400;Path=/
Access-Control-Allow-Origin: *
GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes
MZ.....@.....!..L.!This program cannot be run in DOS mode.
$.....PE..L....A.^.....!...2.6...H.....@>.....P.....y
2 client pkts, 2 server pkts, 3 turns.
Entire conversation (564 kB)
Show and save data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
tcp.stream eq 717
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.6.12.203 an
No. Time
33133 251.235068400
33128 251.195710900
33123 251.181827300
33116 251.137683100
33111 251.124891500
33110 251.115540100
33097 251.093928600
32705 244.814813100
32698 244.797398700
32696 244.789618100
32399 243.083099600
31654 233.522262100
31652 233.516395200
31650 233.506870100
Transmission Control Pr
[456 Reassembled TCP Se
Hypertext Transfer Prot
HTTP/1.1 200 OK\r\n
Server: nginx\r\n
Date: Fri, 12 Jun 20
Content-Type: applic
Content-Length: 5630
Last-Modified: Thu,
Connection: keep-ali
ETag: "5ee2b190-8975
X-Content-Type-Optio
Accept-Ranges: bytes
\r\n
[HTTP response 2/2]
00000000 48 54 54 50 2f
00000010 0a 53 65 72 76
00000020 44 61 74 65 3a
00000030 6e 20 32 30 32
00000040 47 4d 54 0d 0a
Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
32267 192.168.1.100... application/json 41 kB _bulk
32271 192.168.1.100... application/json 11 kB _bulk
32275 192.168.1.100... application/json 41 kB _bulk
32279 192.168.1.100... application/json 11 kB _bulk
32284 192.168.1.100... application/json 42 kB _bulk
32289 192.168.1.100... application/json 11 kB _bulk
32293 192.168.1.100... application/json 42 kB _bulk
32297 192.168.1.100... application/json 11 kB _bulk
32304 192.168.1.100... application/json 42 kB _bulk
32308 192.168.1.100... application/json 11 kB _bulk
32312 192.168.1.100... application/json 41 kB _bulk
32317 192.168.1.100... application/json 11 kB _bulk
32320 192.168.1.100... application/json 25 kB _bulk
32324 192.168.1.100... application/json 6,966... _bulk
32399 205.185.125.104 application/octet-stream 563 kB june11.dll
32570 192.168.1.100... application/json 9,125... _bulk
32579 192.168.1.100... application/json 960 b... _bulk
32696 snnmnkxdhflw... 395 b... post.php
32698 snnmnkxdhflw... text/html 208 b... post.php
32705 snnmnkxdhflw... 431 b... post.php
32746 192.168.1.100... application/json 39 kB _bulk
32748 192.168.1.100... application/json 3,501... _bulk
33097 snnmnkxdhflw... text/html 371 kB post.php
33110 snnmnkxdhflw... 328 b... post.php
33111 snnmnkxdhflw... 266 b... post.php
33116 snnmnkxdhflw... 261 b... post.php
33123 snnmnkxdhflw... 2,111... post.php
33128 snnmnkxdhflw... 331 b... post.php
Text Filter:
Save
Save All
Close
Help



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


VirusTotal - Free Online ...
Shell No. 1
capture-lan-dirb-wpres...
05:04 PM
VirusTotal - Free Online Virus, Malware and URL Scanner - Mozilla Firefox
VirusTotal - Free Online
https://www.virustotal.com/old-browsers/file-analysis/MjU0NWIxNTQ4MzE2NW
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
This is a minimal interface for browsers that do not support full-fledged VirusTotal
SHA256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Name: -
Detection ratio: 49/65 (Analyzing...)
Security vendor
Result
Update
Bkav
malicious
20220616
Lionic
malicious
20220616
Elastic
malicious
20220614
McAfee
malicious
20220616
Cylance
malicious
20220617
Sangfor
malicious
20220602
K7AntiVirus
malicious
20220616
BitDefender
malicious
20220616



File Sections

Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5
.text	5.07979261582	0x1000	0x53514	0x53600	29d65c51b29aa26a5762bb8e7efe6af6
.rdata	7.70358146765	0x55000	0x2928a	0x29400	febcaa6baae6f6ec7474b2d21df14ad4
.data	5.63882104853	0x7f000	0x7b68	0x7c00	967c79c517e45a62124fae6d48a80bd4
.rsrc	5.17616369108	0x87000	0x3288	0x3400	e1daa196fbd67864456196bdc4285f99
.reloc	5.54382274745	0x8b000	0x320	0x400	5757fa335c8c028b6e362e91a6207d43

File Imports

ADVAPI32.dll | GDI32.dll | KERNEL32.dll | USER32.dll

RegOpenKeyA

RegQueryValueExW

File Certificates

Error validating certificate: A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider. (0x800b0109)

Incident Response
Indicators
File Details
File Sections
File Imports
File Certificates (3)
Screenshots (1)
Hybrid Analysis (2)
Network Analysis
Extracted Strings
Extracted Files (1)
Notifications
Community (0)
Back to top

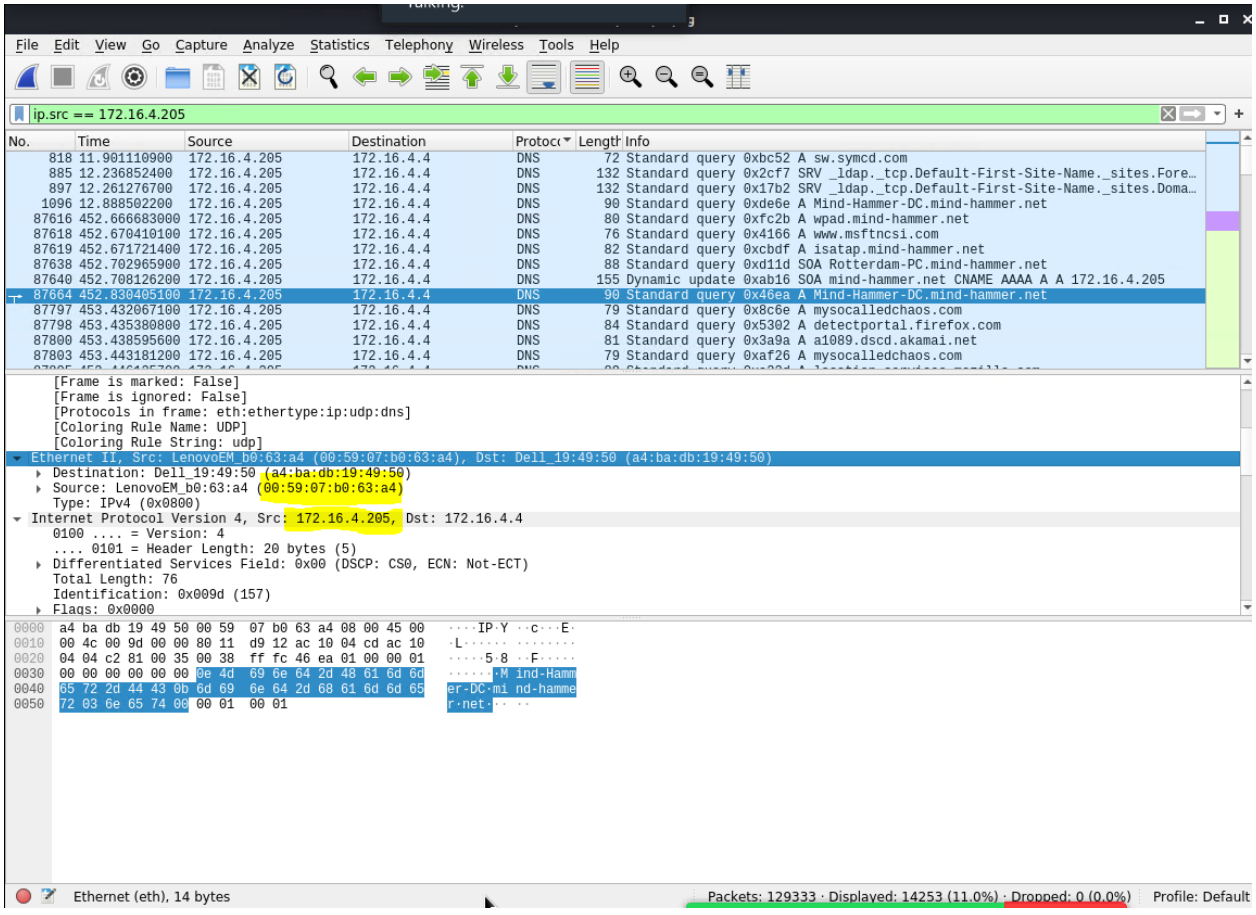
Vulnerable Windows Machines

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

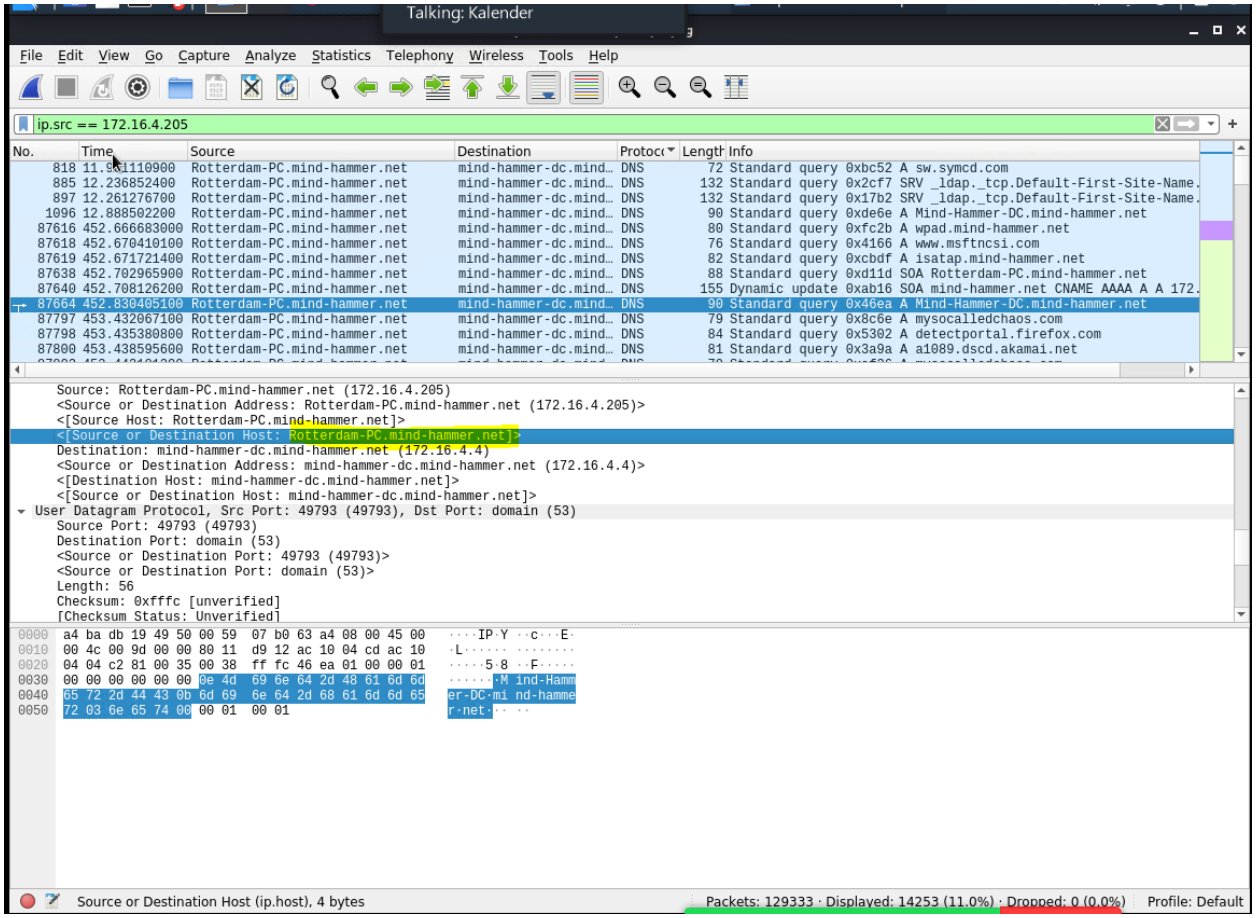
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

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

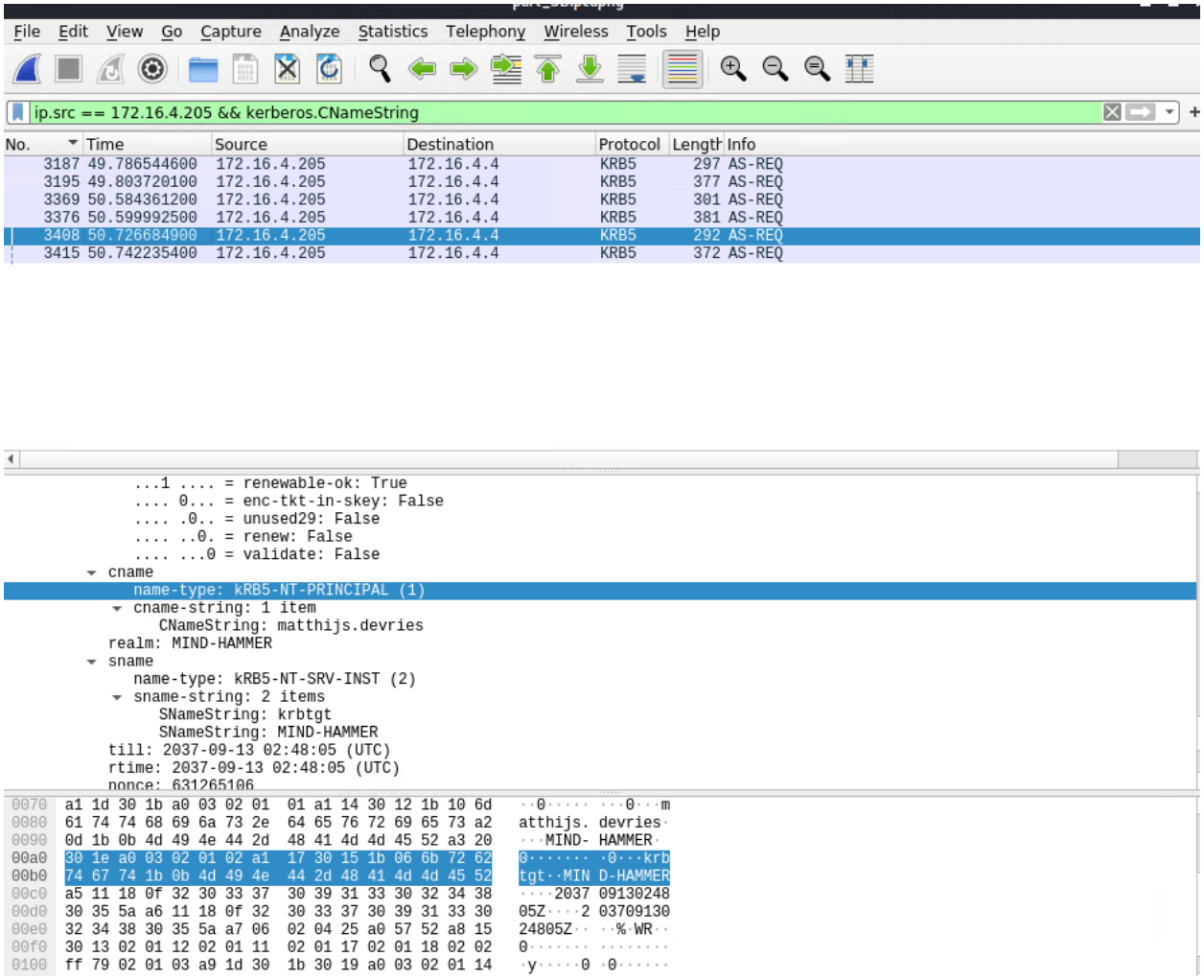


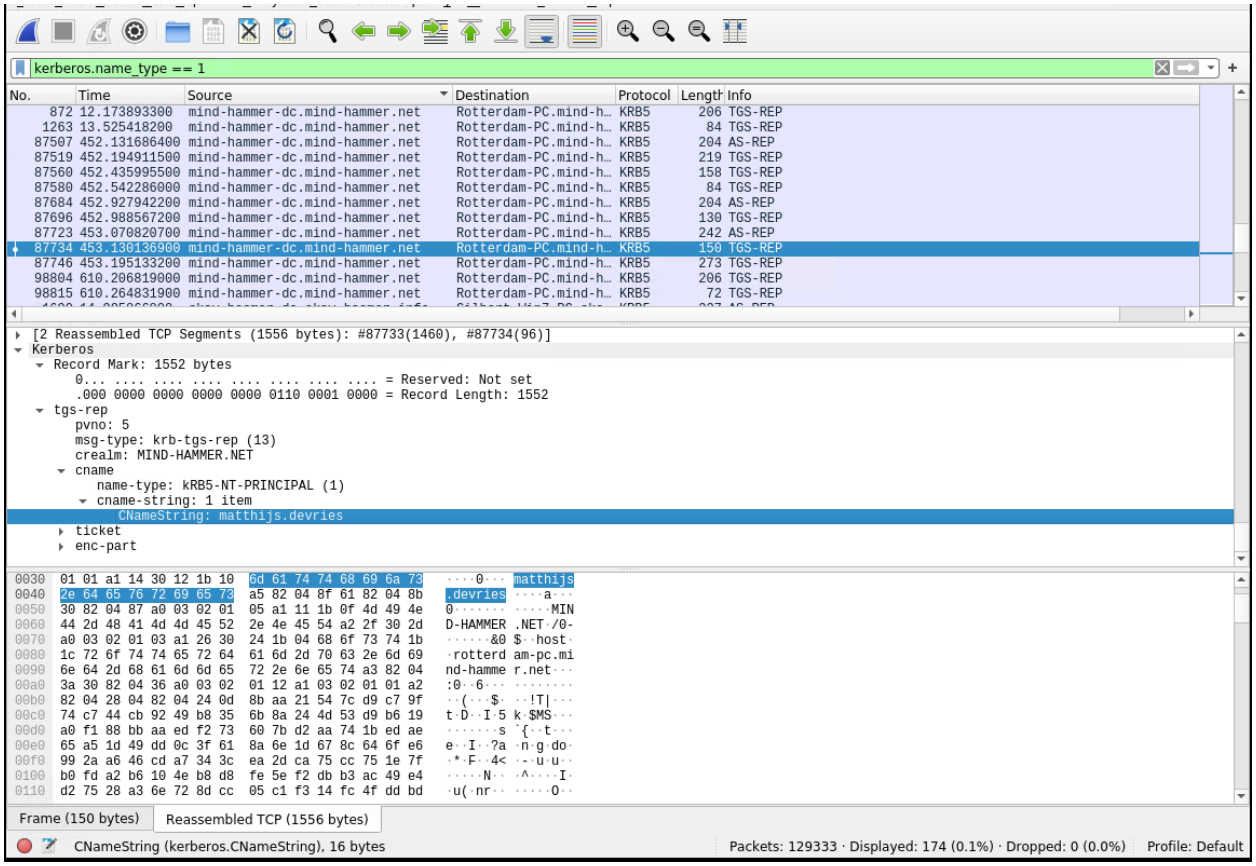
+



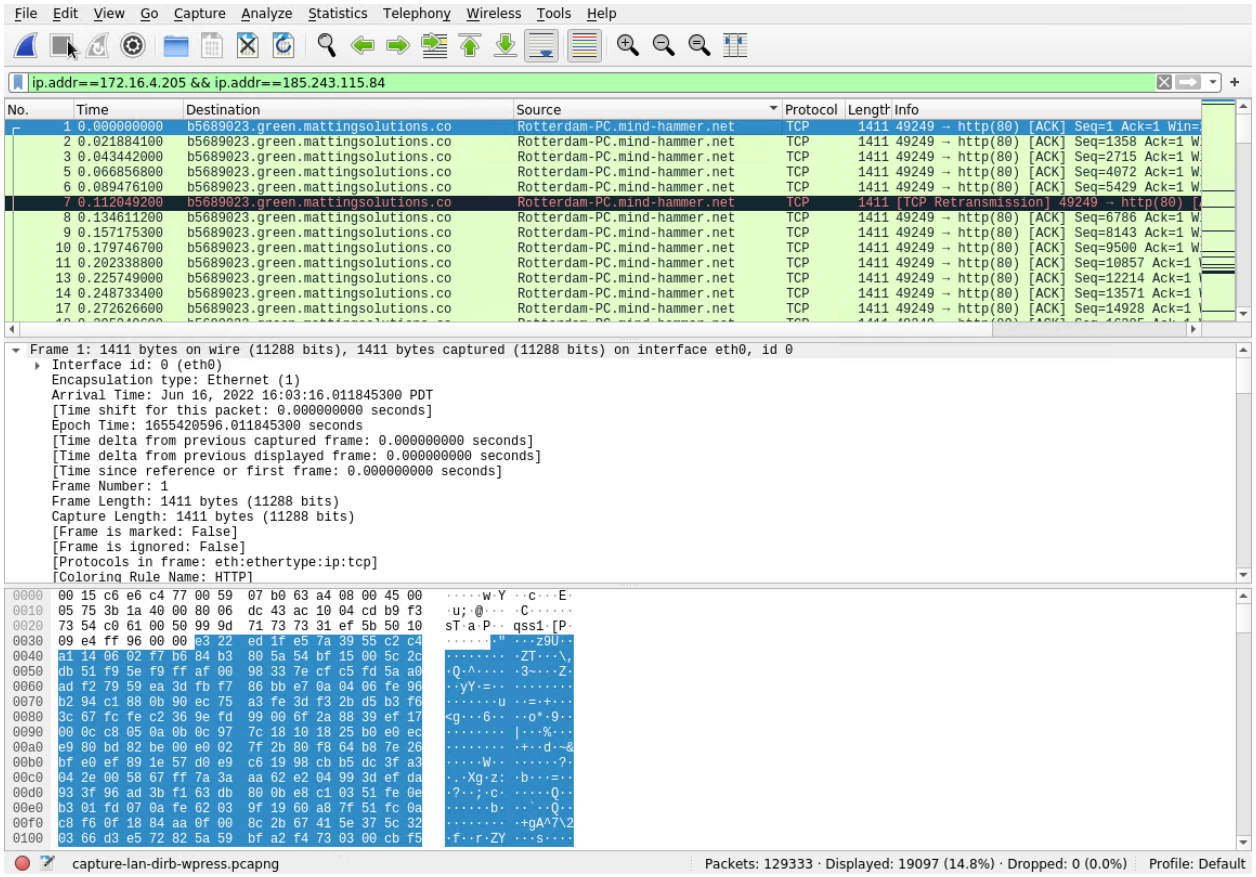
2. What is the username of the Windows user whose computer is infected?

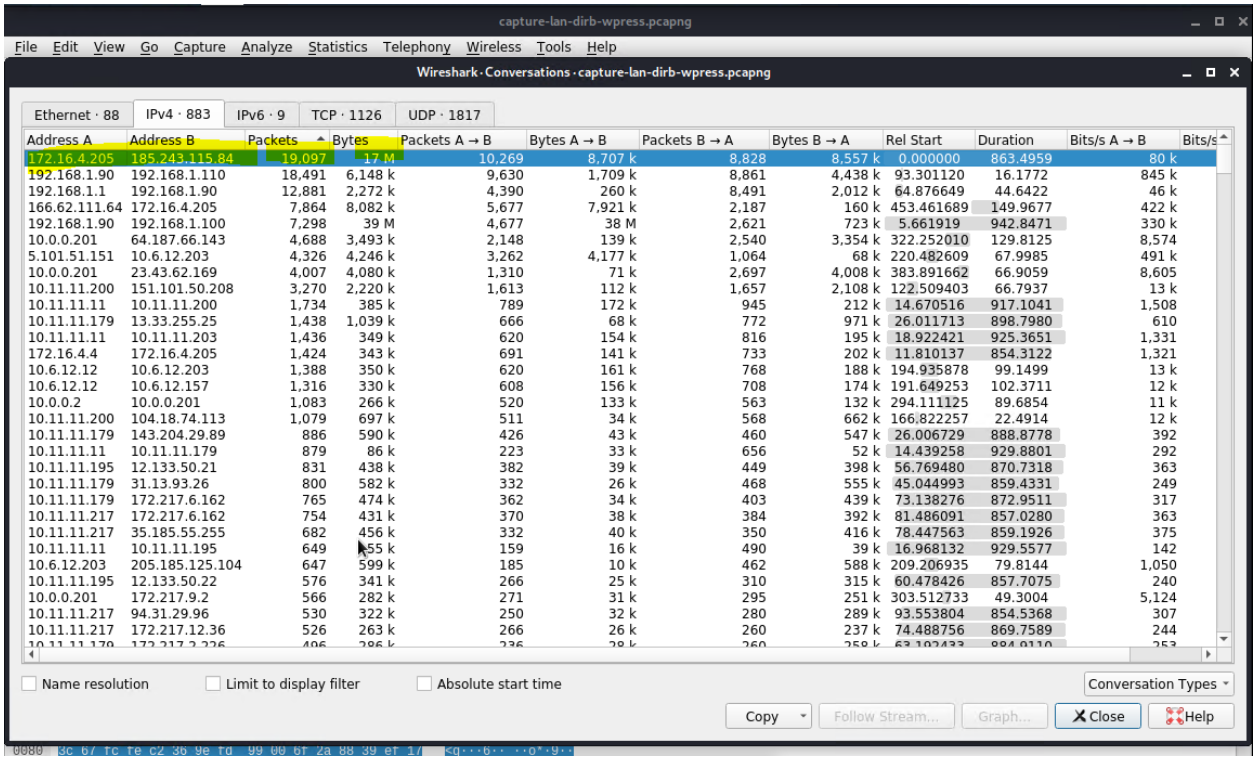
   matthijs.devries

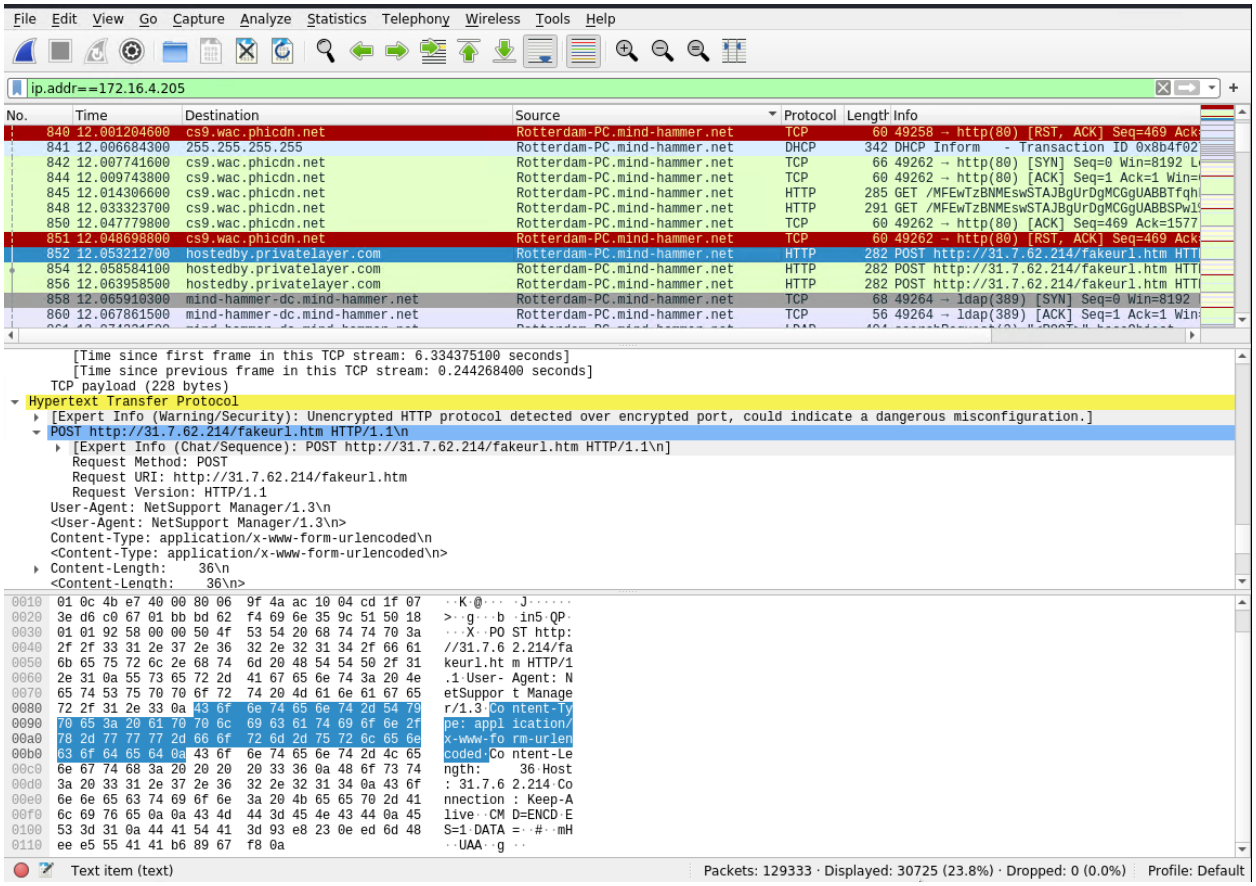

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src == 172.16.4.205 && kerberos.CNameString
No. Time Source Destination Protocol Length Info
3187 49.786544600 172.16.4.205 172.16.4.4 KRB5 297 AS-REQ
3195 49.803720100 172.16.4.205 172.16.4.4 KRB5 377 AS-REQ
3369 50.584361200 172.16.4.205 172.16.4.4 KRB5 301 AS-REQ
3376 50.599992500 172.16.4.205 172.16.4.4 KRB5 381 AS-REQ
3408 50.726684900 172.16.4.205 172.16.4.4 KRB5 292 AS-REQ
3415 50.742235400 172.16.4.205 172.16.4.4 KRB5 372 AS-REQ
...1 .... = renewable-ok: True
.... 0... = enc-tkt-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
0070 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 6d ··0····· ···0···m
0080 61 74 74 68 69 6a 73 2e 64 65 76 72 69 65 73 a2 atthijs. devries·
0090 0d 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 a3 20 ···MIND- HAMMER·
00a0 30 1e a0 03 02 01 02 a1 17 30 15 1b 06 6b 72 62 0····· ·0···krb
00b0 74 67 74 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 tgt··MIN D-HAMMER
00c0 a5 11 18 0f 32 30 33 37 30 39 31 33 30 32 34 38 ····2037 09130248
00d0 30 35 5a a6 11 18 0f 32 30 33 37 30 39 31 33 30 05Z····2 03709130
00e0 32 34 38 30 35 5a a7 06 02 04 25 a0 57 52 a8 15 24805Z·· ··%·WR··
00f0 30 13 02 01 12 02 01 11 02 01 17 02 01 18 02 02 0····· ·····
0100 ff 79 02 01 03 a9 1d 30 1b 30 19 a0 03 02 01 14 ·y·····0 ·0·····



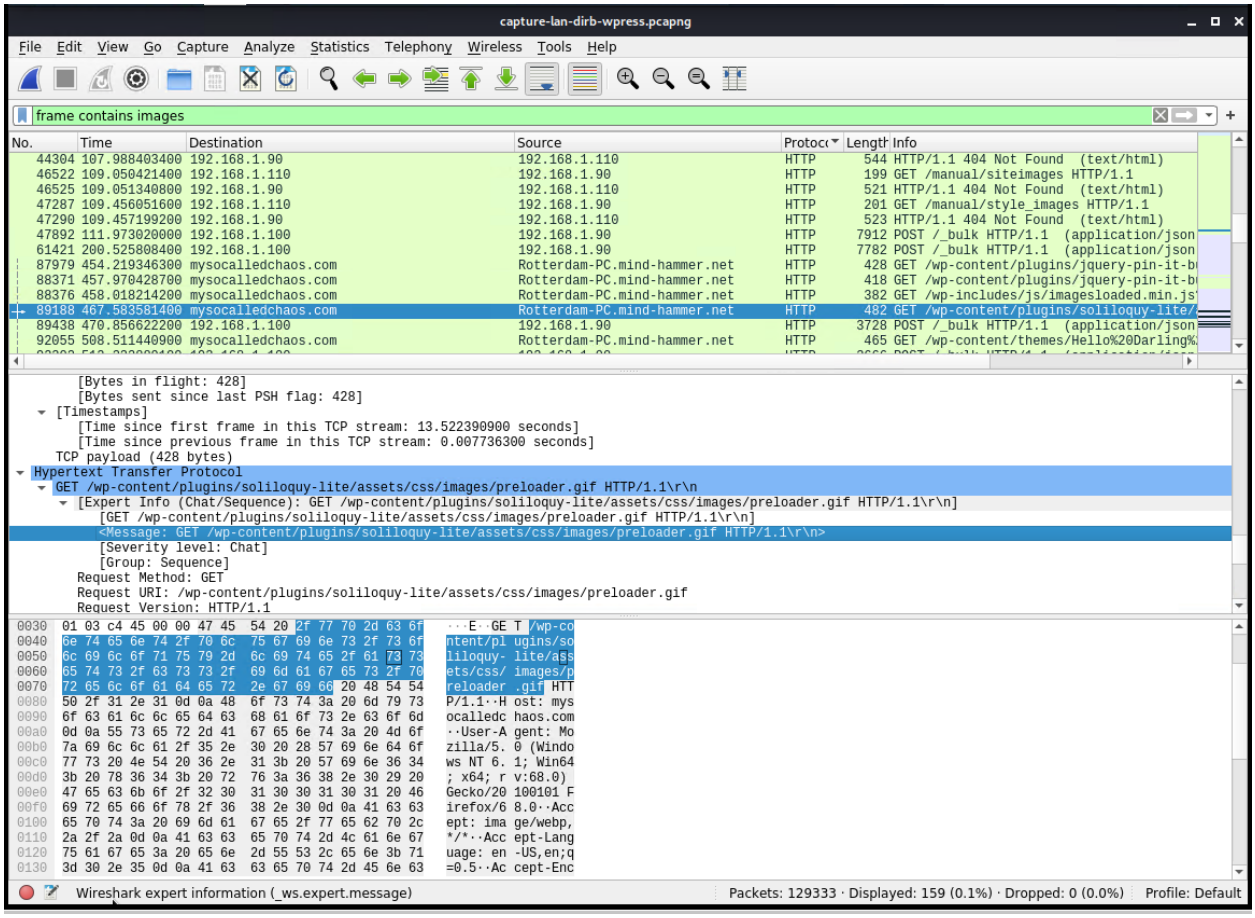
3. What are the IP addresses used in the actual infection traffic?

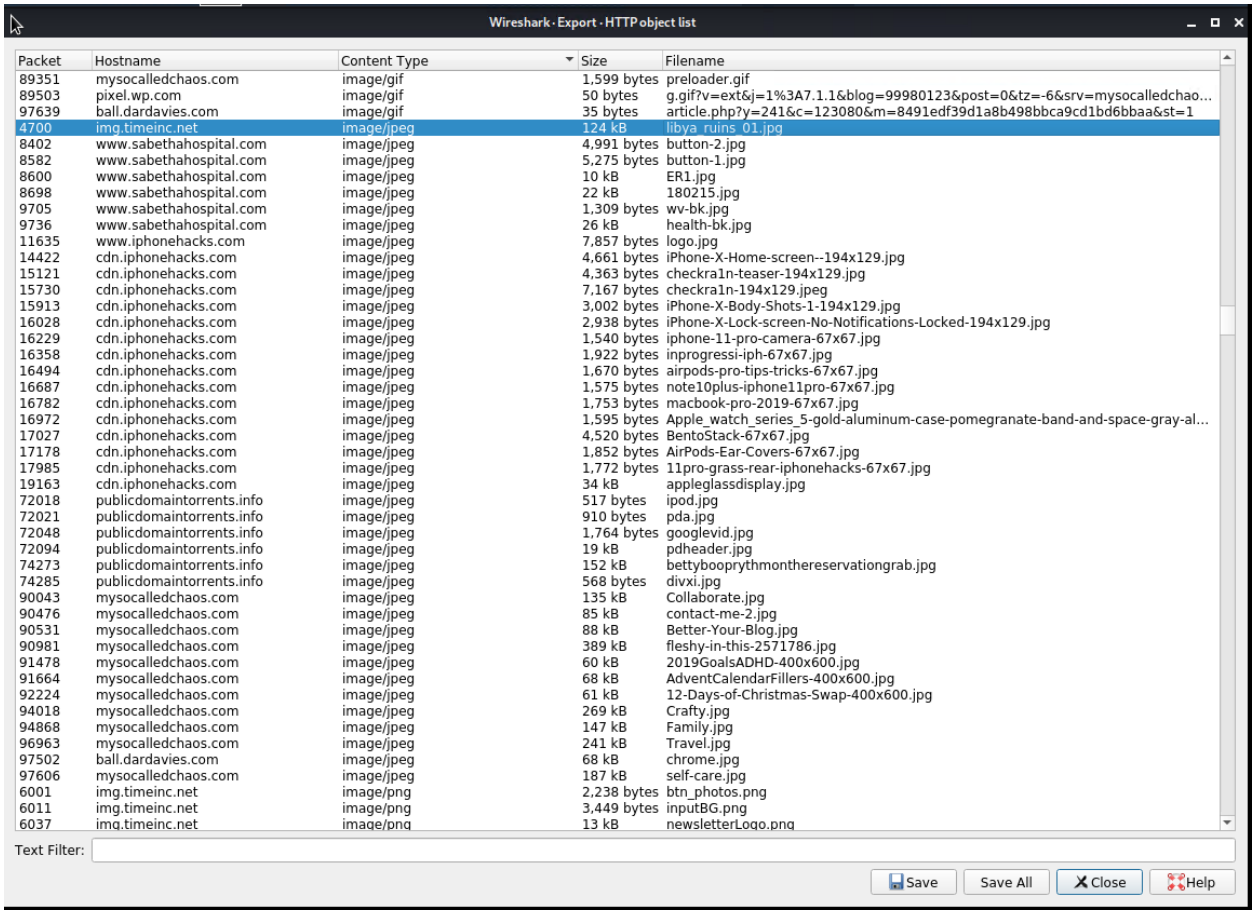

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==172.16.4.205 && ip.addr==185.243.115.84
No. Time Destination Source Protocol Length Info
1 0.000000000 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=1 Ack=1 Win=
2 0.021884100 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=1358 Ack=1 W
3 0.043442000 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=2715 Ack=1 W
5 0.066856800 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=4072 Ack=1 W
6 0.089476100 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=5429 Ack=1 W
7 0.112049200 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 [TCP Retransmission] 49249 → http(80)
8 0.134611200 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=6786 Ack=1 W
9 0.157175300 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=8143 Ack=1 W
10 0.179746700 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=9500 Ack=1 W
11 0.202338800 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=10857 Ack=1
13 0.225749000 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=12214 Ack=1
14 0.248733400 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=13571 Ack=1
17 0.272626600 b5689023.green.mattingsolutions.co Rotterdam-PC.mind-hammer.net TCP 1411 49249 → http(80) [ACK] Seq=14928 Ack=1
Frame 1: 1411 bytes on wire (11288 bits), 1411 bytes captured (11288 bits) on interface eth0, id 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 16, 2022 16:03:16.011845300 PDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1655420596.011845300 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 1411 bytes (11288 bits)
Capture Length: 1411 bytes (11288 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: HTTP]
0000 00 15 c6 e6 c4 77 00 59 07 b0 63 a4 08 00 45 00
0010 05 75 3b 1a 40 00 80 06 dc 43 ac 10 04 cd b9 f3
0020 73 54 c0 61 00 50 99 9d 71 73 73 31 ef 5b 50 10
0030 09 e4 ff 96 00 00 e3 22 ed 1f e5 7a 39 55 c2 c4
0040 a1 14 06 02 f7 b6 84 b3 80 5a 54 bf 15 00 5c 2c
0050 db 51 f9 5e f9 ff af 00 98 33 7e cf c5 fd 5a a0
0060 ad f2 79 59 ea 3d fb f7 86 bb e7 0a 04 06 fe 96
0070 b2 94 c1 88 0b 90 ec 75 a3 fe 3d f3 2b d5 b3 f6
0080 3c 67 fc fe c2 36 9e fd 99 00 6f 2a 88 39 ef 17
0090 00 0c c8 05 0a 0b 0c 97 7c 18 10 18 25 b0 e0 ec
00a0 e9 80 bd 82 be 00 e0 02 7f 2b 80 f8 64 b8 7e 26
00b0 bf e0 ef 89 1e 57 d0 e9 c6 19 98 cb b5 dc 3f a3
00c0 04 2e 00 58 67 ff 7a 3a aa 62 e2 04 99 3d ef da
00d0 93 3f 96 ad 3b f1 63 db 80 0b e8 c1 03 51 fe 0e
00e0 b3 01 fd 07 0a fe 62 03 9f 19 60 a8 7f 51 fc 0a
00f0 c8 f6 0f 18 84 aa 0f 00 8c 2b 67 41 5e 37 5c 32
0100 03 66 d3 e5 72 82 5a 59 bf a2 f4 73 03 00 cb f5
capture-lan-dirb-wpress.pcapng
Packets: 129333 · Displayed: 19097 (14.8%) · Dropped: 0 (0.0%)
Profile: Default

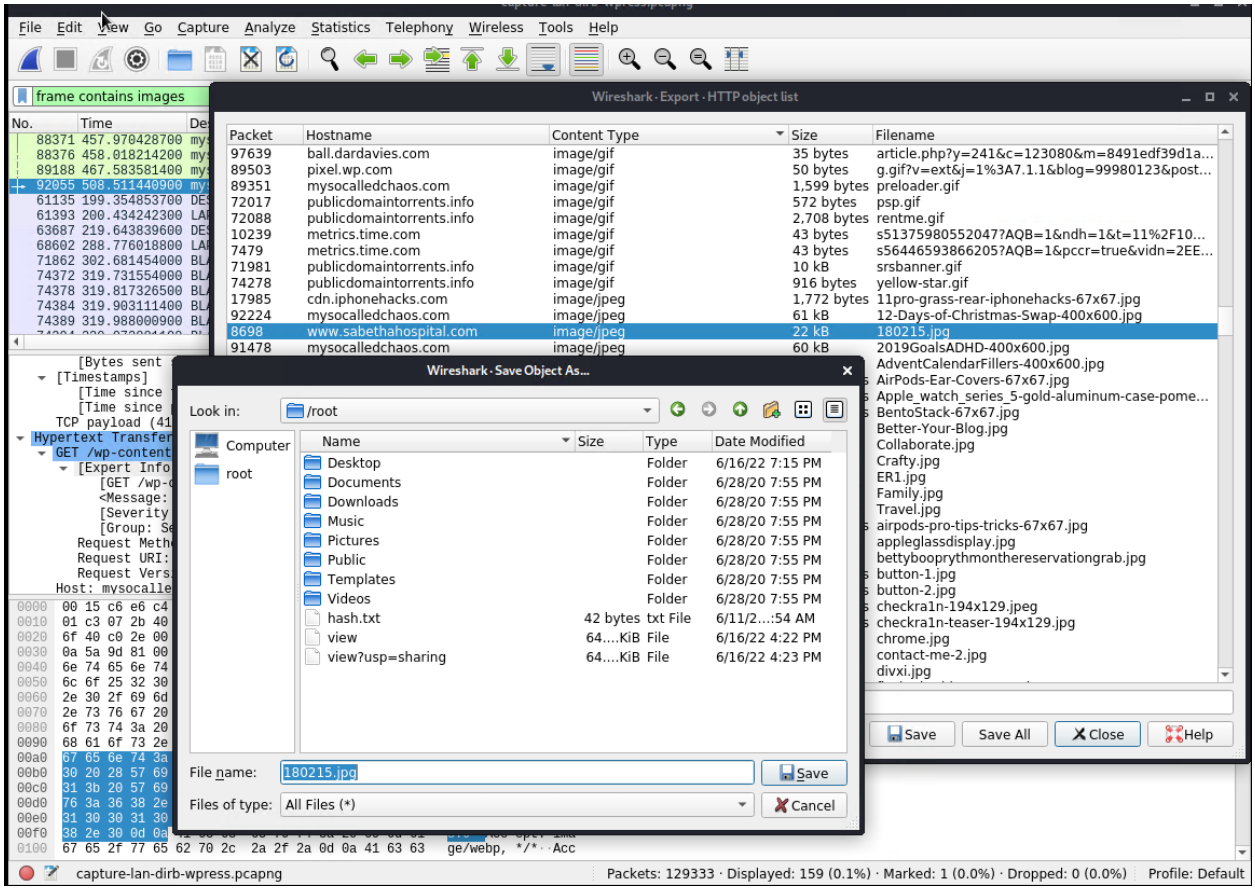

capture-lan-dirb-wpress.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · capture-lan-dirb-wpress.pcapng
Ethernet · 88
IPv4 · 883
IPv6 · 9
TCP · 1126
UDP · 1817
Address A Address B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s
172.16.4.205 185.243.115.84 19,097 17 M 10,269 8,707 k 8,828 8,557 k 0.000000 863.4959 80 k
192.168.1.90 192.168.1.110 18,491 6,148 k 9,630 1,709 k 8,861 4,438 k 93.301120 16.1772 845 k
192.168.1.1 192.168.1.90 12,881 2,272 k 4,390 260 k 8,491 2,012 k 64.876649 44.6422 46 k
166.62.111.64 172.16.4.205 7,864 8,082 k 5,677 7,921 k 2,187 160 k 453.461689 149.9677 422 k
192.168.1.90 192.168.1.100 7,298 39 M 4,677 38 M 2,621 723 k 5.661919 942.8471 330 k
10.0.0.201 64.187.66.143 4,688 3,493 k 2,148 139 k 2,540 3,354 k 322.252010 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 220.482609 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 383.891662 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 122.509403 66.7937 13 k
10.11.11.11 10.11.11.200 1,734 385 k 789 172 k 945 212 k 14.670516 917.1041 1,508
10.11.11.179 13.33.255.25 1,438 1,039 k 666 68 k 772 971 k 26.011713 898.7980 610
10.11.11.11 10.11.11.203 1,436 349 k 620 154 k 816 195 k 18.922421 925.3651 1,331
172.16.4.4 172.16.4.205 1,424 343 k 691 141 k 733 202 k 11.810137 854.3122 1,321
10.6.12.12 10.6.12.203 1,388 350 k 620 161 k 768 188 k 194.935878 99.1499 13 k
10.6.12.12 10.6.12.157 1,316 330 k 608 156 k 708 174 k 191.649253 102.3711 12 k
10.0.0.2 10.0.0.201 1,083 266 k 520 133 k 563 132 k 294.111125 89.6854 11 k
10.11.11.200 104.18.74.113 1,079 697 k 511 34 k 568 662 k 166.822257 22.4914 12 k
10.11.11.179 143.204.29.89 886 590 k 426 43 k 460 547 k 26.006729 888.8778 392
10.11.11.11 10.11.11.179 879 86 k 223 33 k 656 52 k 14.439258 929.8801 292
10.11.11.195 12.133.50.21 831 438 k 382 39 k 449 398 k 56.769480 870.7318 363
10.11.11.179 31.13.93.26 800 582 k 332 26 k 468 555 k 45.044993 859.4331 249
10.11.11.179 172.217.6.162 765 474 k 362 34 k 403 439 k 73.138276 872.9511 317
10.11.11.217 172.217.6.162 754 431 k 370 38 k 384 392 k 81.486091 857.0280 363
10.11.11.217 35.185.55.255 682 456 k 332 40 k 350 416 k 78.447563 859.1926 375
10.11.11.11 10.11.11.195 649 455 k 159 16 k 490 39 k 16.968132 929.5577 142
10.6.12.203 205.185.125.104 647 599 k 185 10 k 462 588 k 209.206935 79.8144 1,050
10.11.11.195 12.133.50.22 576 341 k 266 25 k 310 315 k 60.478426 857.7075 240
10.0.0.201 172.217.9.2 566 282 k 271 31 k 295 251 k 303.512733 49.3004 5,124
10.11.11.217 94.31.29.96 530 322 k 250 32 k 280 289 k 93.553804 854.5368 307
10.11.11.217 172.217.12.36 526 263 k 266 26 k 260 237 k 74.488756 869.7589 244
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

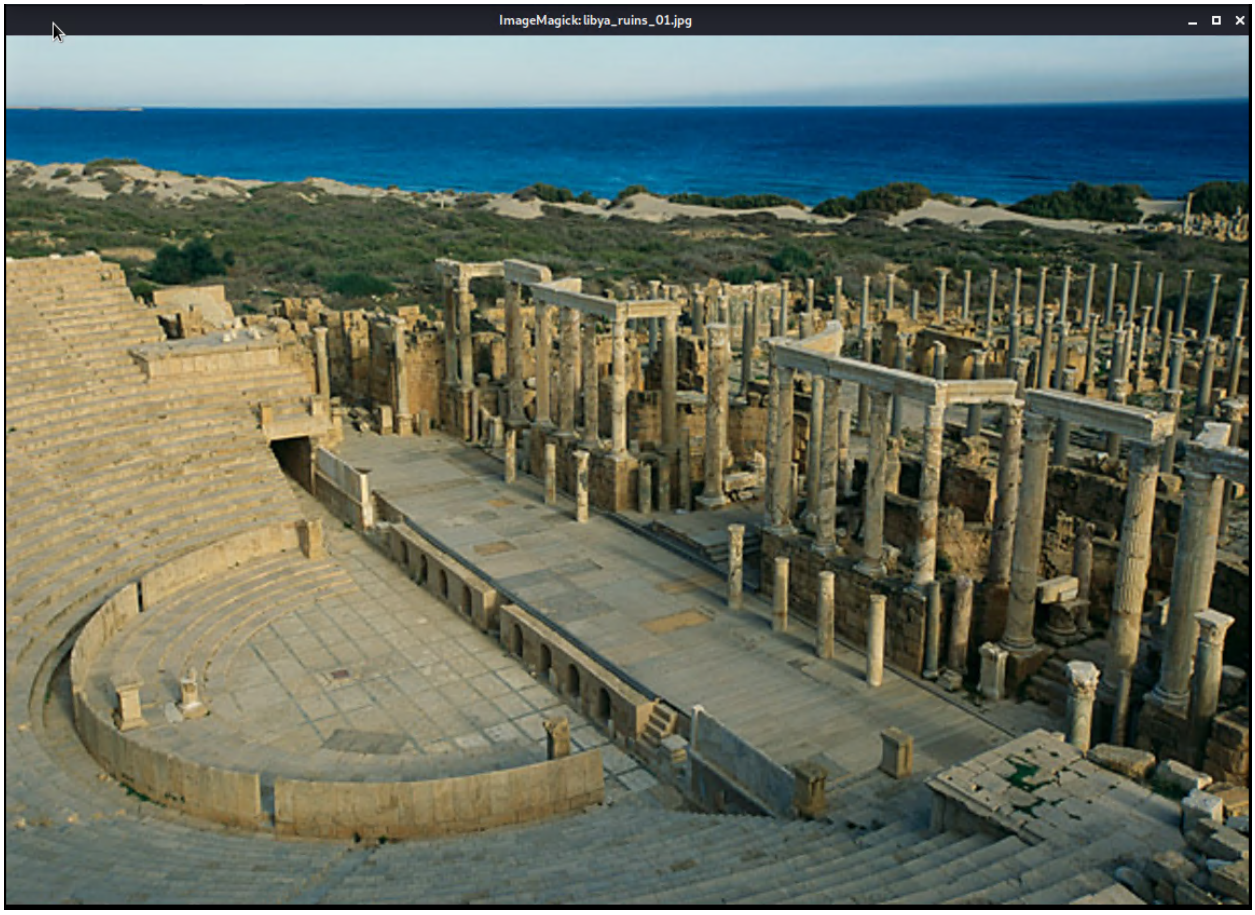


4. As a bonus, retrieve the desktop background of the Windows host.


capture-lan-dirb-wpress.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
frame contains images
No. Time Destination Source Protoc Length Info
44304 107.988403400 192.168.1.90 192.168.1.110 HTTP 544 HTTP/1.1 404 Not Found (text/html)
46522 109.050421400 192.168.1.110 192.168.1.90 HTTP 199 GET /manual/siteimages HTTP/1.1
46525 109.051340800 192.168.1.90 192.168.1.110 HTTP 521 HTTP/1.1 404 Not Found (text/html)
47287 109.456051600 192.168.1.110 192.168.1.90 HTTP 201 GET /manual/style_images HTTP/1.1
47290 109.457199200 192.168.1.90 192.168.1.110 HTTP 523 HTTP/1.1 404 Not Found (text/html)
47892 111.973020000 192.168.1.100 192.168.1.90 HTTP 7912 POST /_bulk HTTP/1.1 (application/json
61421 200.525808400 192.168.1.100 192.168.1.90 HTTP 7782 POST /_bulk HTTP/1.1 (application/json
87979 454.219346300 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 428 GET /wp-content/plugins/jquery-pin-it-b
88371 457.970428700 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 418 GET /wp-content/plugins/jquery-pin-it-b
88376 458.018214200 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 382 GET /wp-includes/js/imagesloaded.min.js
89188 467.583581400 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 482 GET /wp-content/plugins/soliloquy-lite/
89438 470.856622200 192.168.1.100 192.168.1.90 HTTP 3728 POST /_bulk HTTP/1.1 (application/json
92055 508.511440900 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 465 GET /wp-content/themes/Hello%20Darling%
[Bytes in flight: 428]
[Bytes sent since last PSH flag: 428]
[Timestamps]
[Time since first frame in this TCP stream: 13.522390900 seconds]
[Time since previous frame in this TCP stream: 0.007736300 seconds]
TCP payload (428 bytes)
Hypertext Transfer Protocol
GET /wp-content/plugins/soliloquy-lite/assets/css/images/preloader.gif HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wp-content/plugins/soliloquy-lite/assets/css/images/preloader.gif HTTP/1.1\r\n]
[GET /wp-content/plugins/soliloquy-lite/assets/css/images/preloader.gif HTTP/1.1\r\n]
<Message: GET /wp-content/plugins/soliloquy-lite/assets/css/images/preloader.gif HTTP/1.1\r\n>
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wp-content/plugins/soliloquy-lite/assets/css/images/preloader.gif
Request Version: HTTP/1.1
0030 01 03 c4 45 00 00 47 45 54 20 2f 77 70 2d 63 6f ···E··GE T /wp-co
0040 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 73 6f ntent/pl ugins/so
0050 6c 69 6c 6f 71 75 79 2d 6c 69 74 65 2f 61 73 73 liloquy- lite/ass
0060 65 74 73 2f 63 73 73 2f 69 6d 61 67 65 73 2f 70 ets/css/ images/p
0070 72 65 6c 6f 61 64 65 72 2e 67 69 66 20 48 54 54 reloader .gif HTT
0080 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6d 79 73 P/1.1··H ost: mys
0090 6f 63 61 6c 6c 65 64 63 68 61 6f 73 2e 63 6f 6d ocalledc haos.com
00a0 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ··User-A gent: Mo
00b0 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo
00c0 77 73 20 4e 54 20 36 2e 31 3b 20 57 69 6e 36 34 ws NT 6. 1; Win64
00d0 3b 20 78 36 34 3b 20 72 76 3a 36 38 2e 30 29 20 ; x64; r v:68.0)
00e0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00f0 69 72 65 66 6f 78 2f 36 38 2e 30 0d 0a 41 63 63 irefox/6 8.0··Acc
0100 65 70 74 3a 20 69 6d 61 67 65 2f 77 65 62 70 2c ept: ima ge/webp,
0110 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 */*··Acc ept-Lang
0120 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 uage: en -US,en;q
0130 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 =0.5··Ac cept-Enc
Wireshark expert information (_ws.expert.message)
Packets: 129333 · Displayed: 159 (0.1%) · Dropped: 0 (0.0%)
Profile: Default


Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
89351 mysocalledchaos.com image/gif 1,599 bytes preloader.gif
89503 pixel.wp.com image/gif 50 bytes g.gif?v=ext&j=1%3A7.1.1&blog=99980123&post=0&tz=-6&srv=mysocalledchao...
97639 ball.dardavies.com image/gif 35 bytes article.php?y=241&c=123080&m=8491edf39d1a8b498bbca9cd1bd6bbaa&st=1
4700 img.timeinc.net image/jpeg 124 kB libya_ruins_01.jpg
8402 www.sabethahospital.com image/jpeg 4,991 bytes button-2.jpg
8582 www.sabethahospital.com image/jpeg 5,275 bytes button-1.jpg
8600 www.sabethahospital.com image/jpeg 10 kB ER1.jpg
8698 www.sabethahospital.com image/jpeg 22 kB 180215.jpg
9705 www.sabethahospital.com image/jpeg 1,309 bytes wv-bk.jpg
9736 www.sabethahospital.com image/jpeg 26 kB health-bk.jpg
11635 www.iphonehacks.com image/jpeg 7,857 bytes logo.jpg
14422 cdn.iphonehacks.com image/jpeg 4,661 bytes iPhone-X-Home-screen--194x129.jpg
15121 cdn.iphonehacks.com image/jpeg 4,363 bytes checkra1n-teaser-194x129.jpg
15730 cdn.iphonehacks.com image/jpeg 7,167 bytes checkra1n-194x129.jpeg
15913 cdn.iphonehacks.com image/jpeg 3,002 bytes iPhone-X-Body-Shots-1-194x129.jpg
16028 cdn.iphonehacks.com image/jpeg 2,938 bytes iPhone-X-Lock-screen-No-Notifications-Locked-194x129.jpg
16229 cdn.iphonehacks.com image/jpeg 1,540 bytes iphone-11-pro-camera-67x67.jpg
16358 cdn.iphonehacks.com image/jpeg 1,922 bytes inprogressi-iph-67x67.jpg
16494 cdn.iphonehacks.com image/jpeg 1,670 bytes airpods-pro-tips-tricks-67x67.jpg
16687 cdn.iphonehacks.com image/jpeg 1,575 bytes note10plus-iphone11pro-67x67.jpg
16782 cdn.iphonehacks.com image/jpeg 1,753 bytes macbook-pro-2019-67x67.jpg
16972 cdn.iphonehacks.com image/jpeg 1,595 bytes Apple_watch_series_5-gold-aluminum-case-pomegranate-band-and-space-gray-al...
17027 cdn.iphonehacks.com image/jpeg 4,520 bytes BentoStack-67x67.jpg
17178 cdn.iphonehacks.com image/jpeg 1,852 bytes AirPods-Ear-Covers-67x67.jpg
17985 cdn.iphonehacks.com image/jpeg 1,772 bytes 11pro-grass-rear-iphonehacks-67x67.jpg
19163 cdn.iphonehacks.com image/jpeg 34 kB appleglassdisplay.jpg
72018 publicdomaintorrents.info image/jpeg 517 bytes ipod.jpg
72021 publicdomaintorrents.info image/jpeg 910 bytes pda.jpg
72048 publicdomaintorrents.info image/jpeg 1,764 bytes googlevid.jpg
72094 publicdomaintorrents.info image/jpeg 19 kB pdheader.jpg
74273 publicdomaintorrents.info image/jpeg 152 kB bettybooprythmonthereservationgrab.jpg
74285 publicdomaintorrents.info image/jpeg 568 bytes divxi.jpg
90043 mysocalledchaos.com image/jpeg 135 kB Collaborate.jpg
90476 mysocalledchaos.com image/jpeg 85 kB contact-me-2.jpg
90531 mysocalledchaos.com image/jpeg 88 kB Better-Your-Blog.jpg
90981 mysocalledchaos.com image/jpeg 389 kB fleshy-in-this-2571786.jpg
91478 mysocalledchaos.com image/jpeg 60 kB 2019GoalsADHD-400x600.jpg
91664 mysocalledchaos.com image/jpeg 68 kB AdventCalendarFillers-400x600.jpg
92224 mysocalledchaos.com image/jpeg 61 kB 12-Days-of-Christmas-Swap-400x600.jpg
94018 mysocalledchaos.com image/jpeg 269 kB Crafty.jpg
94868 mysocalledchaos.com image/jpeg 147 kB Family.jpg
96963 mysocalledchaos.com image/jpeg 241 kB Travel.jpg
97502 ball.dardavies.com image/jpeg 68 kB chrome.jpg
97606 mysocalledchaos.com image/jpeg 187 kB self-care.jpg
6001 img.timeinc.net image/png 2,238 bytes btn_photos.png
6011 img.timeinc.net image/png 3,449 bytes inputBG.png
6037 img.timeinc.net image/png 13 kB newsletterLogo.png
Text Filter:
Save
Save All
Close
Help


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
frame contains images
Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
97639 ball.dardavies.com image/gif 35 bytes article.php?y=241&c=123080&m=8491edf39d1a...
89503 pixel.wp.com image/gif 50 bytes g.gif?v=ext&j=1%3A7.1.1&blog=99980123&post...
89351 mysocalledchaos.com image/gif 1,599 bytes preloader.gif
72017 publicdomaintorrents.info image/gif 572 bytes psp.gif
72088 publicdomaintorrents.info image/gif 2,708 bytes rentme.gif
10239 metrics.time.com image/gif 43 bytes s51375980552047?AQB=1&ndh=1&t=11%2F10...
7479 metrics.time.com image/gif 43 bytes s564465938662O5?AQB=1&pccr=true&vidn=2EE...
71981 publicdomaintorrents.info image/gif 10 kB srsbanner.gif
74278 publicdomaintorrents.info image/gif 916 bytes yellow-star.gif
17985 cdn.iphonehacks.com image/jpeg 1,772 bytes 11pro-grass-rear-iphonehacks-67x67.jpg
92224 mysocalledchaos.com image/jpeg 61 kB 12-Days-of-Christmas-Swap-400x600.jpg
8698 www.sabethahospital.com image/jpeg 22 kB 180215.jpg
91478 mysocalledchaos.com image/jpeg 60 kB 2019GoalsADHD-400x600.jpg
AdventCalendarFillers-400x600.jpg
AirPods-Ear-Covers-67x67.jpg
Apple_watch_series_5-gold-aluminum-case-pome...
BentoStack-67x67.jpg
Better-Your-Blog.jpg
Collaborate.jpg
Crafty.jpg
ER1.jpg
Family.jpg
Travel.jpg
airpods-pro-tips-tricks-67x67.jpg
appleglassdisplay.jpg
bettybooprythmonthereservationgrab.jpg
button-1.jpg
button-2.jpg
checkra1n-194x129.jpeg
checkra1n-teaser-194x129.jpg
chrome.jpg
contact-me-2.jpg
divxi.jpg
Save Save All Close Help
Wireshark · Save Object As...
Look in: /root
Computer
root
Name Size Type Date Modified
Desktop Folder 6/16/22 7:15 PM
Documents Folder 6/28/20 7:55 PM
Downloads Folder 6/28/20 7:55 PM
Music Folder 6/28/20 7:55 PM
Pictures Folder 6/28/20 7:55 PM
Public Folder 6/28/20 7:55 PM
Templates Folder 6/28/20 7:55 PM
Videos Folder 6/28/20 7:55 PM
hash.txt 42 bytes txt File 6/11/2...:54 AM
view 64....KiB File 6/16/22 4:22 PM
view?usp=sharing 64....KiB File 6/16/22 4:23 PM
File name: 180215.jpg
Save
Files of type: All Files (*)
Cancel
capture-lan-dirb-wpress.pcapng
Packets: 129333 · Displayed: 159 (0.1%) · Marked: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default


ImageMagick: libya_ruins_01.jpg