MALWARE TRAFFIC ANALYSIS

ANGGOTA KELOMPOK

2501963822 - Josua Abraham
2501991536 - Vaustin
2502001441 - Ayubi Sholahudin
2502009412 - Ramadhana Khalaf Sandhyakala
2502018480 - Carlson King

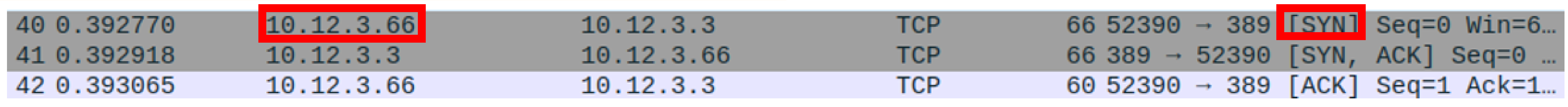
FILE PCAP 2021-12-ISC-FORENSIC-CHALLENGE.PCAP

- 2021-12-22 -- ISC Diary - December 2021 Forensic Contest: Answers and Analysis

PERTANYAAN

1. What was the IP address of the infected Windows computer?
2. What was the host name of the infected Windows computer?
3. What was the user account names from the infected Windows computer? (should be "name" not "names")
4. What was the date and time the infection activity began?
5. What was the family of malware that caused this infection?

WHAT WAS THE IP ADDRESS OF THE INFECTED WINDOWS COMPUTER?

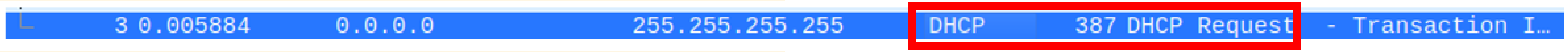


```
40 0.392770   10.12.3.66    10.12.3.3     TCP    66 52390 → 389 [SYN] Seq=0 Win=6…
41 0.392918   10.12.3.3     10.12.3.66    TCP    66 389 → 52390 [SYN, ACK] Seq=0 …
42 0.393065   10.12.3.66    10.12.3.3     TCP    60 52390 → 389 [ACK] Seq=1 Ack=1…
```

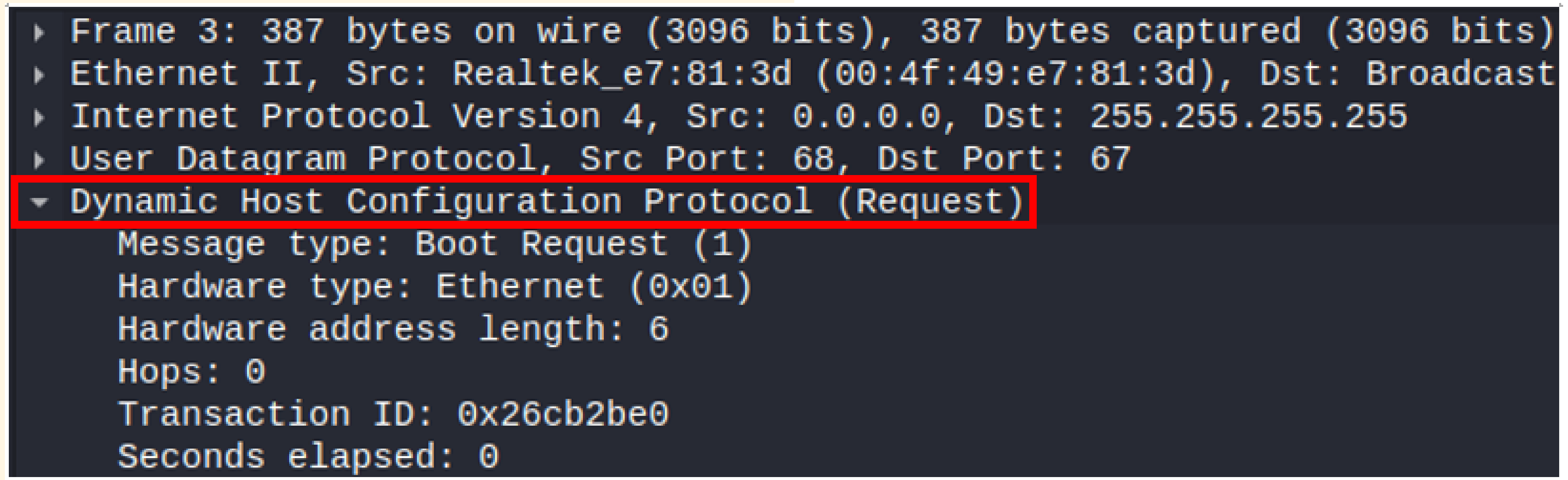
Jawaban: 10.12.3.66

Dari three-way handshake tersebut, dapat dilihat bahwa IP client adalah 10.12.3.66, karena IP tersebut mengirim SYN ke IP 10.12.3.3, dimana SYN merupakan proses client meminta server untuk membuka koneksi untuk client.

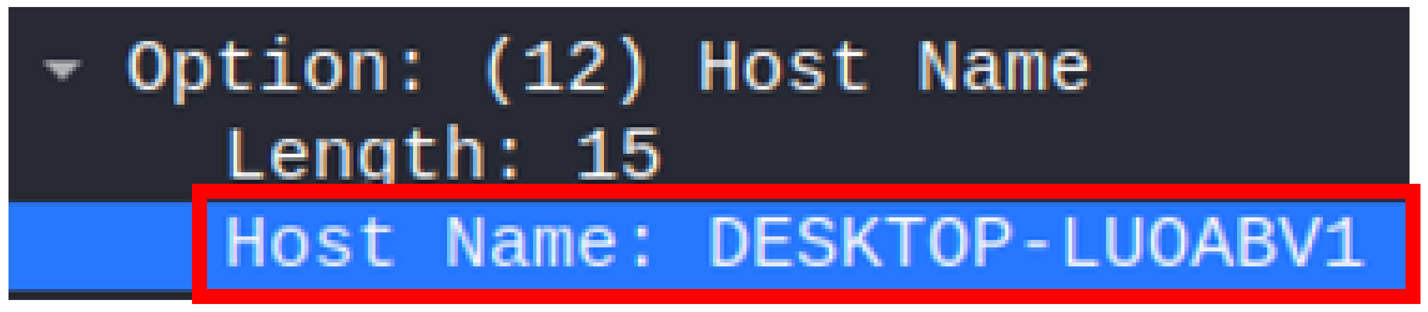
WHAT WAS THE HOST NAME OF THE INFECTED WINDOWS COMPUTER?



```
    3 0.005884      0.0.0.0             255.255.255.255     DHCP      387 DHCP Request  - Transaction I…
```



```
▸ Frame 3: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits)
▸ Ethernet II, Src: Realtek_e7:81:3d (00:4f:49:e7:81:3d), Dst: Broadcast
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x26cb2be0
    Seconds elapsed: 0
```



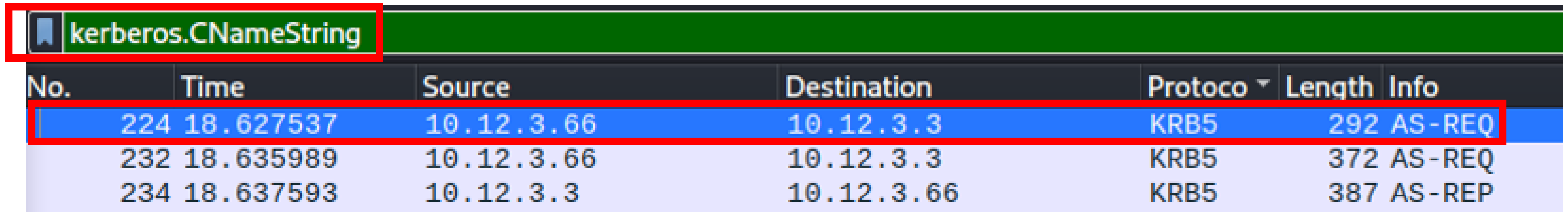
```
▾ Option: (12) Host Name
     Length: 15
     Host Name: DESKTOP-LUOABV1
```

WHAT WAS THE HOST NAME OF THE INFECTED WINDOWS COMPUTER?

Jawaban: DESKTOP-LUOABV1

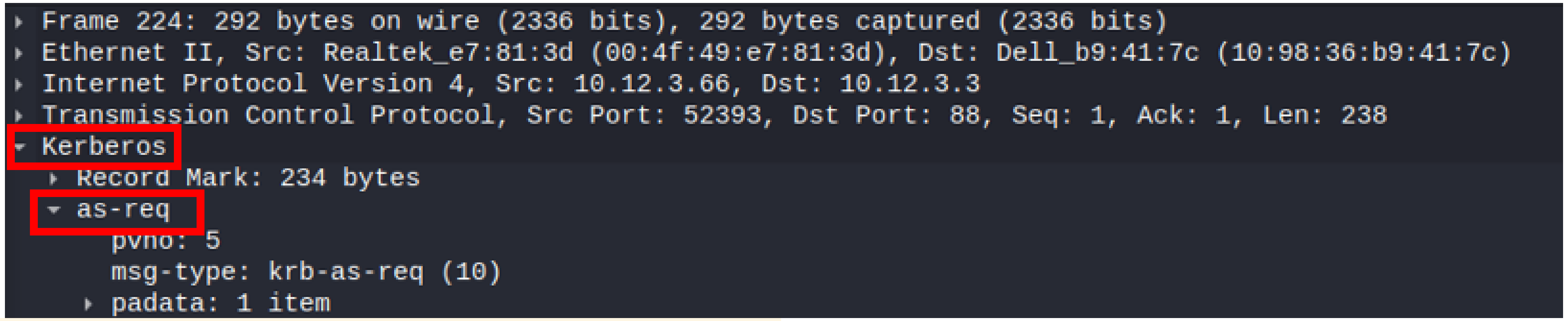
Melalui DHCP Request, kita bisa menemukan hostname dari komputer yang terinfeksi melalui detail dari request DHCP. Host name ditemukan melalui “Dynamic Host Configuration Protocol (Request) -> Option: (12) Host Name” dan didapatkan bahwa hostnamenya adalah “DESKTOP-LUOABV1”.

WHAT WAS THE USER ACCOUNT NAMES FROM THE INFECTED WINDOWS COMPUTER? (SHOULD BE "NAME" NOT "NAMES")

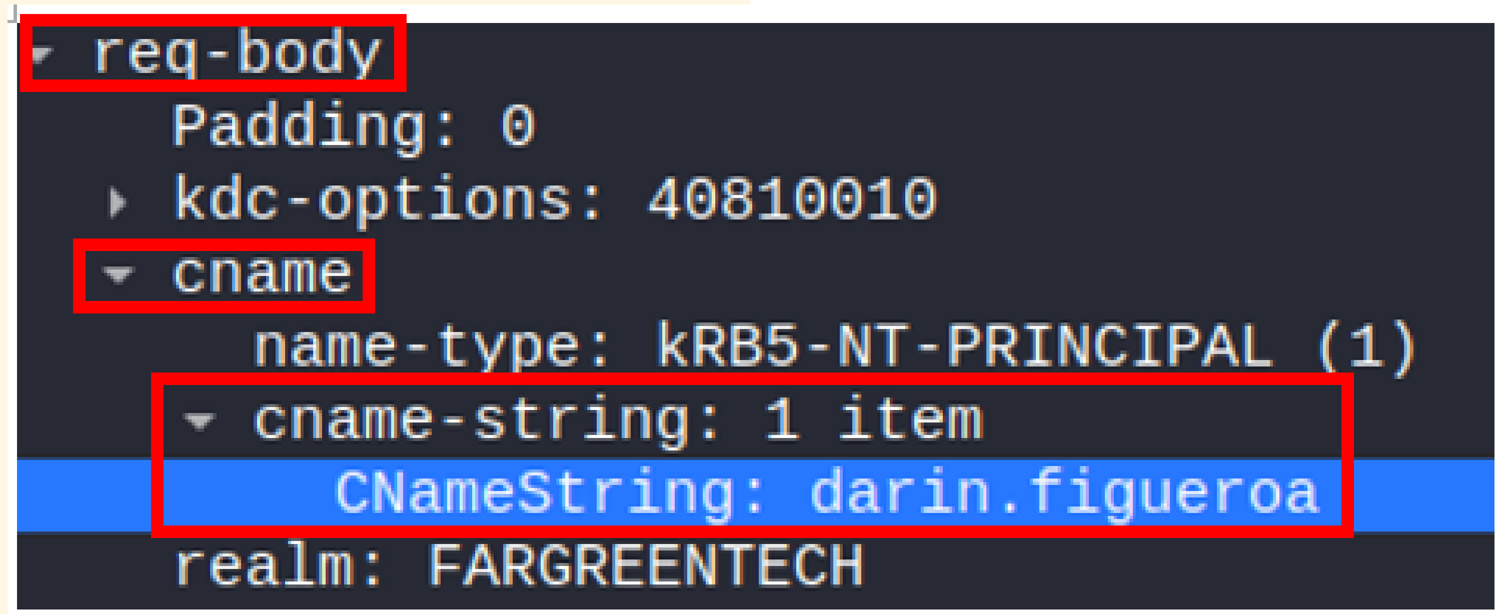


kerberos.CNameString

```
No.    Time        Source        Destination    Protoco  Length Info
   224 18.627537   10.12.3.66    10.12.3.3      KRB5        292 AS-REQ
   232 18.635989   10.12.3.66    10.12.3.3      KRB5        372 AS-REQ
   234 18.637593   10.12.3.3     10.12.3.66     KRB5        387 AS-REP
```



```
▸ Frame 224: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits)
▸ Ethernet II, Src: Realtek_e7:81:3d (00:4f:49:e7:81:3d), Dst: Dell_b9:41:7c (10:98:36:b9:41:7c)
▸ Internet Protocol Version 4, Src: 10.12.3.66, Dst: 10.12.3.3
▸ Transmission Control Protocol, Src Port: 52393, Dst Port: 88, Seq: 1, Ack: 1, Len: 238
▾ Kerberos
  ▸ Record Mark: 234 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 1 item
```



```
▾ req-body
    Padding: 0
  ▸ kdc-options: 40810010
  ▾ cname
      name-type: kRB5-NT-PRINCIPAL (1)
    ▾ cname-string: 1 item
        CNameString: darin.figueroa
    realm: FARGREENTECH
```

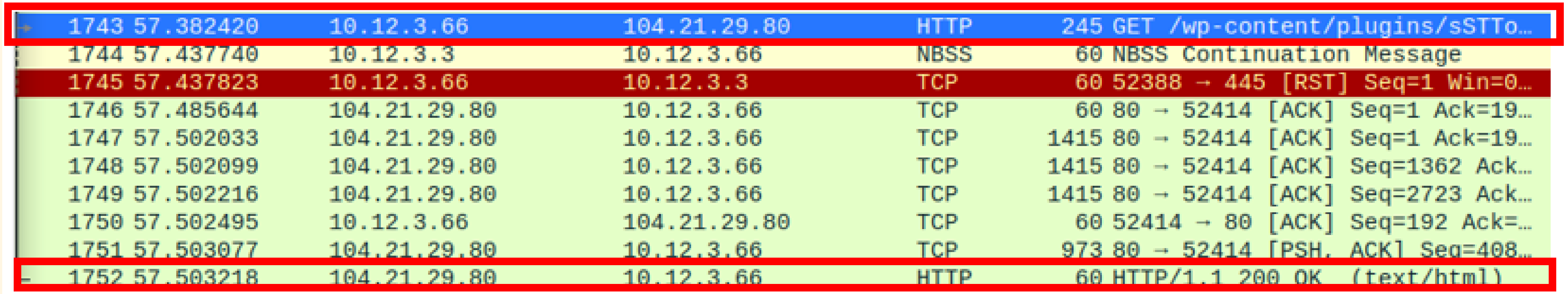
WHAT WAS THE USER ACCOUNT NAMES FROM THE INFECTED WINDOWS COMPUTER? (SHOULD BE "NAME" NOT "NAMES")

Jawaban: darin.figueroa

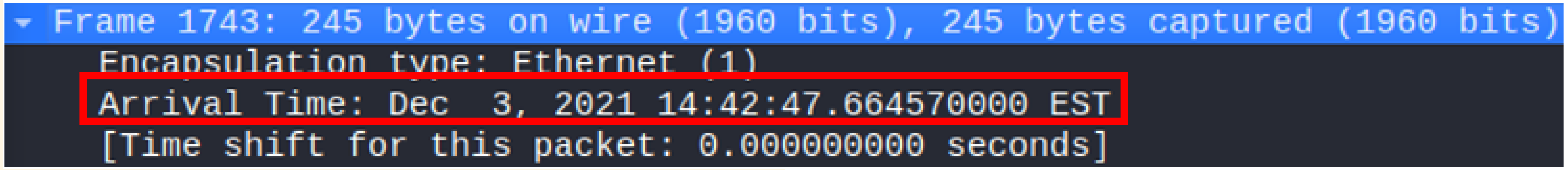
Untuk mencari nama user account, kita bisa melihatnya melaui protocol Kerberos yang merupakan protocol single sign-on dimana kita bisa mengakses beberapa aplikasi dengan satu set kredensial. Biasanya, nama user ditampung dalam cname sehingga kita lakukan filtering agar hanya line yang memiliki detail mengenai cname tampil dalam wireshark.

Setelah itu, dalam line AS-REQ yang merupakan request dari client ke authentication server, kita lihat bagian detail dari request tersebut melalui “Kerberos -> as-req -> req-body -> cname -> cname-string: 1 item”. Dalam cname-string, didapatkan bahwa nama user adalah “darin.figueroa”.

WHAT WAS THE DATE AND TIME THE INFECTION ACTIVITY BEGAN?



```
1743 57.382420   10.12.3.66      104.21.29.80    HTTP    245 GET /wp-content/plugins/sSTTo…
1744 57.437740   10.12.3.3       10.12.3.66      NBSS     60 NBSS Continuation Message
1745 57.437823   10.12.3.66      10.12.3.3       TCP      60 52388 → 445 [RST] Seq=1 Win=0…
1746 57.485644   104.21.29.80    10.12.3.66      TCP      60 80 → 52414 [ACK] Seq=1 Ack=19…
1747 57.502033   104.21.29.80    10.12.3.66      TCP    1415 80 → 52414 [ACK] Seq=1 Ack=19…
1748 57.502099   104.21.29.80    10.12.3.66      TCP    1415 80 → 52414 [ACK] Seq=1362 Ack…
1749 57.502216   104.21.29.80    10.12.3.66      TCP    1415 80 → 52414 [ACK] Seq=2723 Ack…
1750 57.502495   10.12.3.66      104.21.29.80    TCP      60 52414 → 80 [ACK] Seq=192 Ack=…
1751 57.503077   104.21.29.80    10.12.3.66      TCP     973 80 → 52414 [PSH, ACK] Seq=408…
1752 57.503218   104.21.29.80    10.12.3.66      HTTP     60 HTTP/1.1 200 OK  (text/html)
```



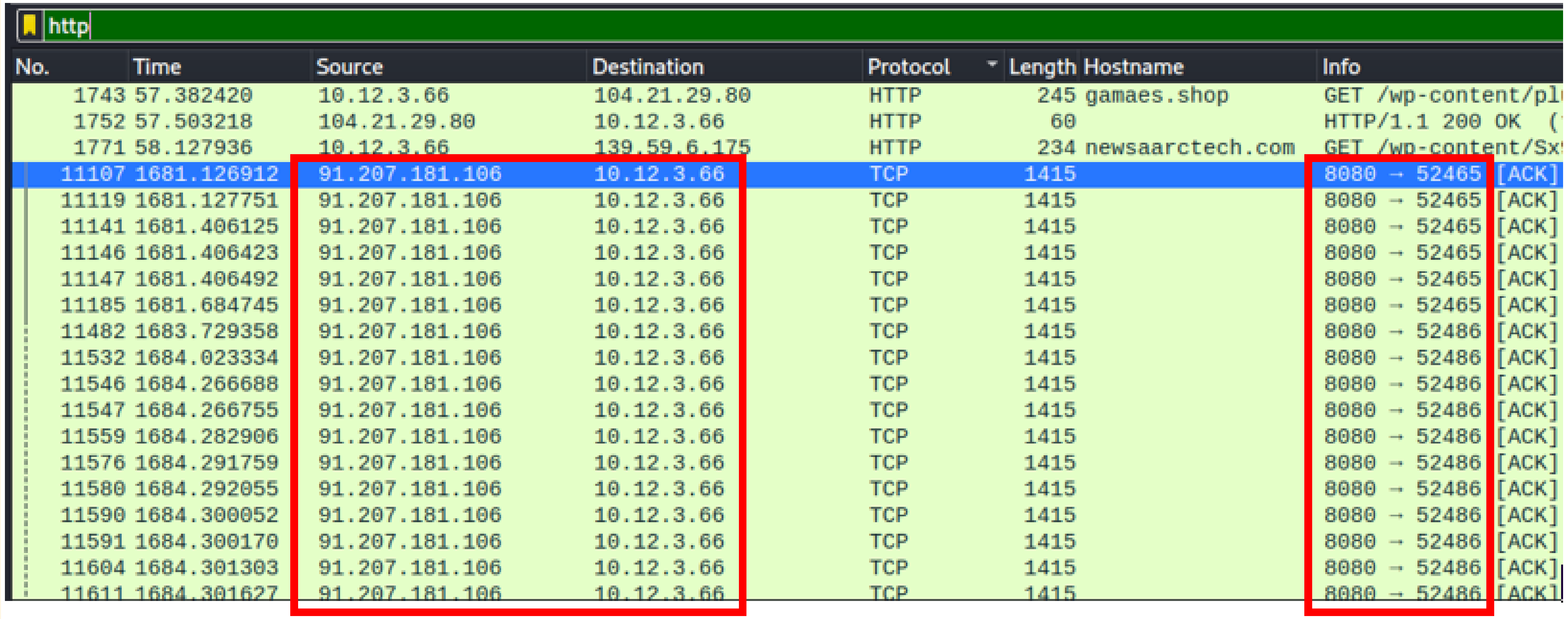
```
▾ Frame 1743: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec  3, 2021 14:42:47.664570000 EST
    [Time shift for this packet: 0.000000000 seconds]
```

WHAT WAS THE DATE AND TIME THE INFECTION ACTIVITY BEGAN?

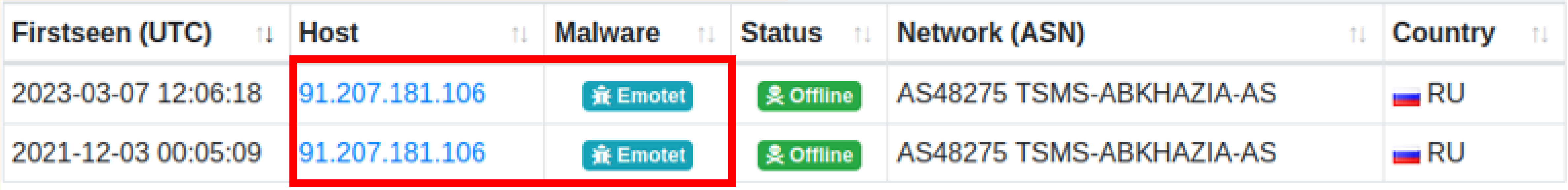
Jawaban: 3 Desember 2021 pada waktu 14:42:47 EST (19:42:47 UTC)

Pada line 1743 request GET content yang berisi konten yang berbahaya dan dijawab dengan http response OK pada line 1752. Pada line tersebut, arrival time terjadi pada 3 Desember 2021 pada waktu 14:42:47 EST (19:42:47 UTC) yang merupakan tanggal dan waktu infeksi pada komputer dimulai.

WHAT WAS THE FAMILY OF MALWARE THAT CAUSED THIS INFECTION?



```
http
No.      Time          Source           Destination      Protocol    Length Hostname          Info
   1743 57.382420     10.12.3.66       104.21.29.80     HTTP           245 gamaes.shop       GET /wp-content/pl
   1752 57.503218     104.21.29.80     10.12.3.66       HTTP            60                   HTTP/1.1 200 OK  (
   1771 58.127936     10.12.3.66       139.59.6.175     HTTP           234 newsaarctech.com  GET /wp-content/Sx
  11107 1681.126912   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52465 [ACK]
  11119 1681.127751   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52465 [ACK]
  11141 1681.406125   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52465 [ACK]
  11146 1681.406423   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52465 [ACK]
  11147 1681.406492   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52465 [ACK]
  11185 1681.684745   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52465 [ACK]
  11482 1683.729358   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11532 1684.023334   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11546 1684.266688   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11547 1684.266755   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11559 1684.282906   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11576 1684.291759   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11580 1684.292055   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11590 1684.300052   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11591 1684.300170   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11604 1684.301303   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
  11611 1684.301627   91.207.181.106   10.12.3.66       TCP           1415                   8080 → 52486 [ACK]
```



Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2023-03-07 12:06:18	91.207.181.106	Emotet	Offline	AS48275 TSMS-ABKHAZIA-AS	RU
2021-12-03 00:05:09	91.207.181.106	Emotet	Offline	AS48275 TSMS-ABKHAZIA-AS	RU

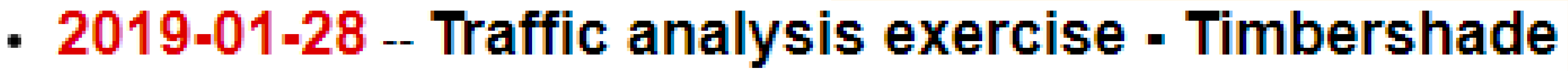
WHAT WAS THE FAMILY OF MALWARE THAT CAUSED THIS INFECTION?

Jawaban: Emotet

Dengan melakukan filter untuk menampilkan http, terdapat banyak sekali line TCP dimana Ip yang sama mengirim request dengan jumlah yang tidak wajar pada suatu port, sehingga serangan ini dapat berasal dari server command and control. Dengan website Feodo Tracker, ditemukan bahwa IP tersebut berupa malware Emotet.

TUGAS TAMBAHAN

FILE PCAP: 2019-01-28-TRAFFIC-ANALYSIS-EXERCISE.PCAP

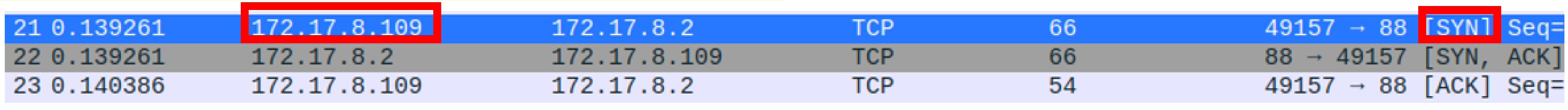


- 2019-01-28 -- Traffic analysis exercise - Timbershade

PERTANYAAN

1. What is the IP address of the infected Windows host?
2. What is the MAC address of the infected Windows host?
3. What is the host name of the infected Windows host?
4. What is the Windows user account name for the infected Windows host?
5. What is the SHA256 file hash of the Windows executable file sent to the infected Windows host?
6. Based on the IDS alerts, what type of infection is this?

WHAT IS THE IP ADDRESS OF THE INFECTED WINDOWS HOST?

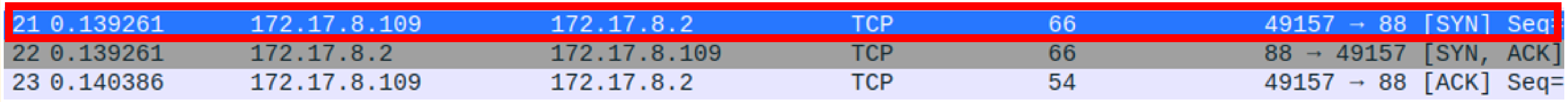


```
21 0.139261   172.17.8.109   172.17.8.2     TCP   66   49157 → 88 [SYN] Seq=
22 0.139261   172.17.8.2     172.17.8.109   TCP   66   88 → 49157 [SYN, ACK]
23 0.140386   172.17.8.109   172.17.8.2     TCP   54   49157 → 88 [ACK] Seq=
```

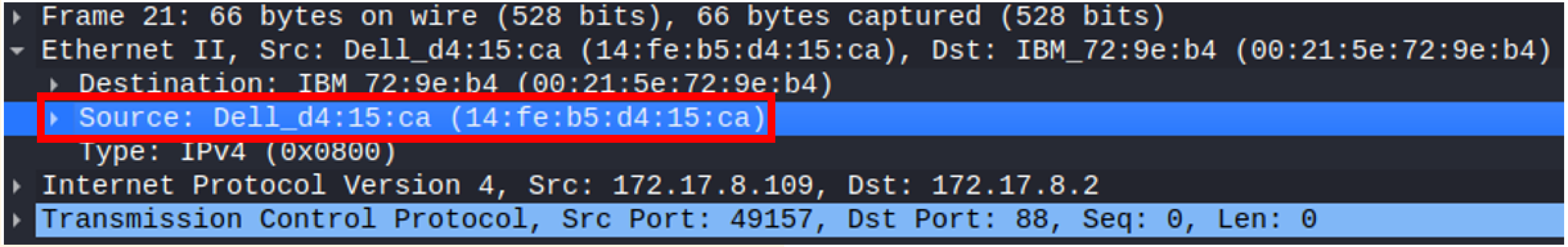
Jawaban: 172.17.8.109

Dari three-way handshake tersebut, dapat dilihat bahwa IP client adalah 172.17.8.109, karena IP tersebut mengirim SYN ke IP 172.17.8.2, dimana SYN merupakan proses client meminta server untuk membuka koneksi untuk client.

WHAT IS THE MAC ADDRESS OF THE INFECTED WINDOWS HOST?



```
21 0.139261    172.17.8.109    172.17.8.2      TCP    66    49157 → 88 [SYN] Seq
22 0.139261    172.17.8.2      172.17.8.109    TCP    66    88 → 49157 [SYN, ACK]
23 0.140386    172.17.8.109    172.17.8.2      TCP    54    49157 → 88 [ACK] Seq=
```



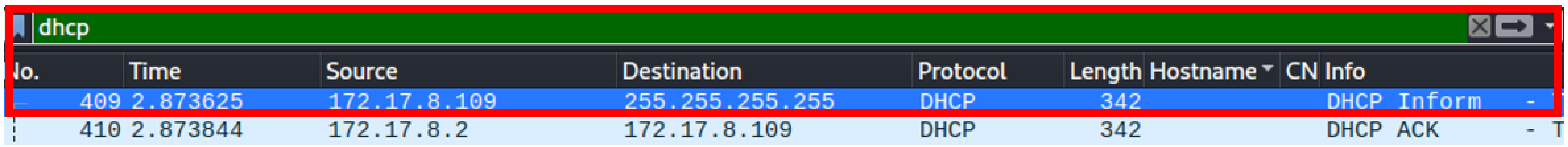
```
▸ Frame 21: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▾ Ethernet II, Src: Dell_d4:15:ca (14:fe:b5:d4:15:ca), Dst: IBM_72:9e:b4 (00:21:5e:72:9e:b4)
  ▸ Destination: IBM_72:9e:b4 (00:21:5e:72:9e:b4)
  ▸ Source: Dell_d4:15:ca (14:fe:b5:d4:15:ca)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 172.17.8.109, Dst: 172.17.8.2
▸ Transmission Control Protocol, Src Port: 49157, Dst Port: 88, Seq: 0, Len: 0
```

WHAT IS THE MAC ADDRESS OF THE INFECTED WINDOWS HOST?

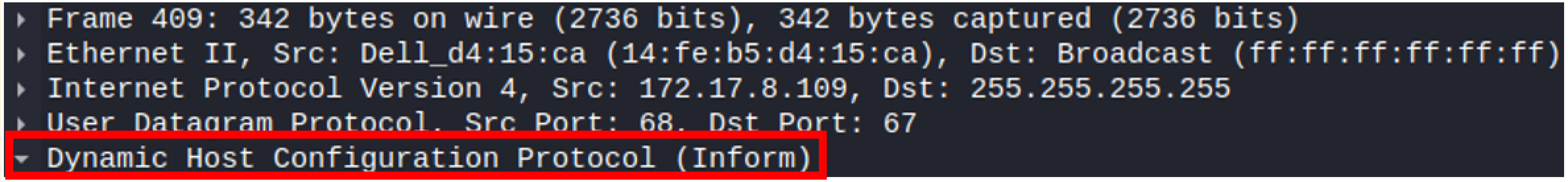
Jawaban: 14:fe:b5:d4:15:ca (Dell_d4:15:ca)

Melalui SYN request dari client, kita bisa menemukan hostname dari komputer yang terinfeksi melalui detail dari request SYN. MAC address ditemukan melalui Ethernet II dan didapatkan bahwa MAC addressnya adalah “14:fe:b5:d4:15:ca (Dell_d4:15:ca)”.

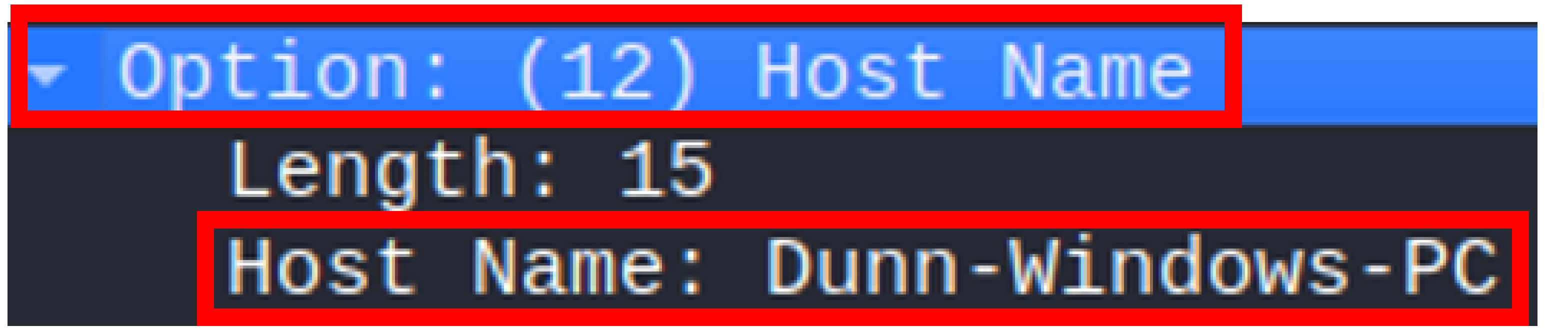
WHAT IS THE HOST NAME OF THE INFECTED WINDOWS HOST?



```
dhcp
No.  Time      Source        Destination      Protocol  Length  Hostname  CN  Info
409 2.873625  172.17.8.109  255.255.255.255  DHCP      342                     DHCP Inform   -
410 2.873844  172.17.8.2    172.17.8.109     DHCP      342                     DHCP ACK      - T
```



```
▸ Frame 409: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: Dell_d4:15:ca (14:fe:b5:d4:15:ca), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 172.17.8.109, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration Protocol (Inform)
```



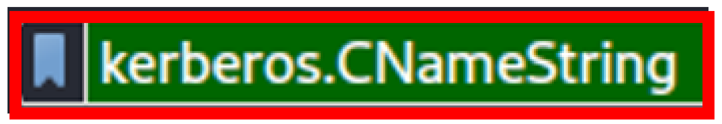
```
▾ Option: (12) Host Name
      Length: 15
      Host Name: Dunn-Windows-PC
```

WHAT IS THE HOST NAME OF THE INFECTED WINDOWS HOST?

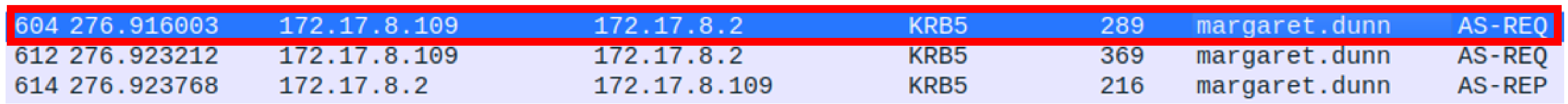
Jawaban: Dunn-Windows-PC

Melalui DHCP Inform, kita bisa menemukan hostname dari komputer yang terinfeksi melalui detail dari DHCP Inform. Host name ditemukan melalui “Dynamic Host Configuration Protocol (Inform) -> Option: (12) Host Name” dan didapatkan bahwa hostnamenya adalah “Dunn-Windows-PC”.

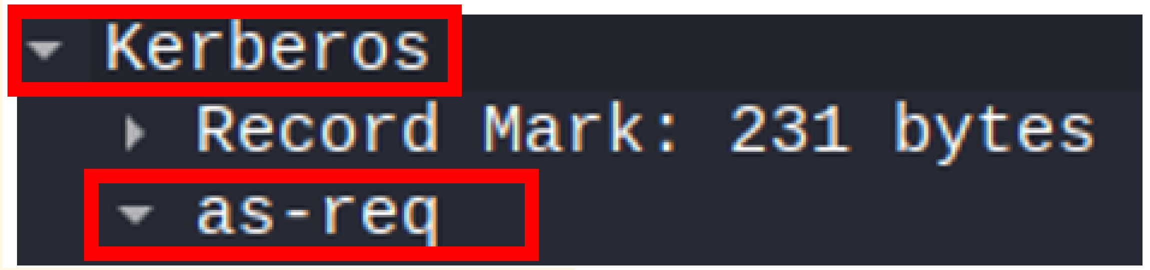
WHAT IS THE WINDOWS USER ACCOUNT NAME FOR THE INFECTED WINDOWS HOST?



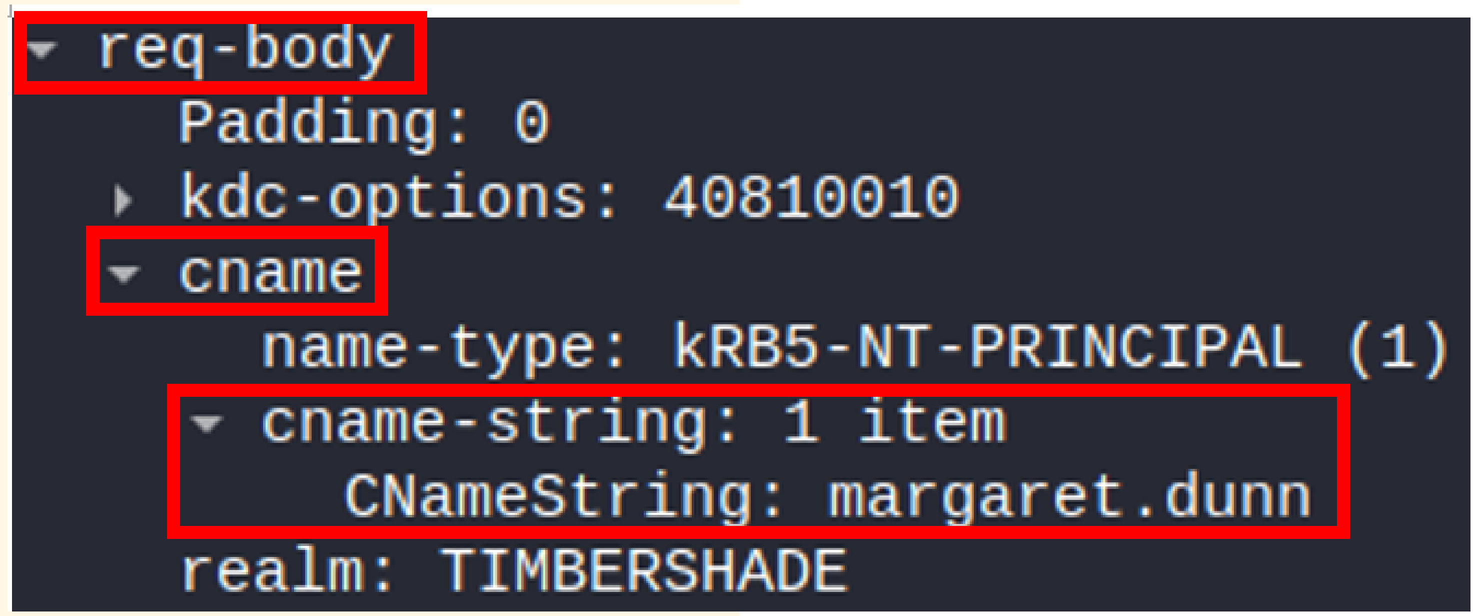
```
kerberos.CNameString
```



```
604 276.916003    172.17.8.109        172.17.8.2          KRB5      289    margaret.dunn    AS-REQ
612 276.923212    172.17.8.109        172.17.8.2          KRB5      369    margaret.dunn    AS-REQ
614 276.923768    172.17.8.2          172.17.8.109        KRB5      216    margaret.dunn    AS-REP
```



```
▾ Kerberos
   ▸ Record Mark: 231 bytes
   ▾ as-req
```



```
▾ req-body
     Padding: 0
   ▸ kdc-options: 40810010
   ▾ cname
       name-type: kRB5-NT-PRINCIPAL (1)
     ▾ cname-string: 1 item
         CNameString: margaret.dunn
     realm: TIMBERSHADE
```

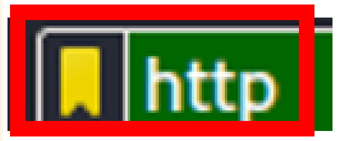
WHAT IS THE WINDOWS USER ACCOUNT NAME FOR THE INFECTED WINDOWS HOST?

Jawaban: margaret.dunn

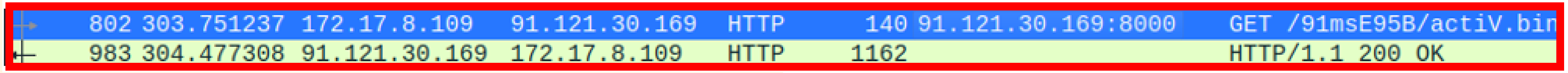
Untuk mencari nama user account, kita bisa melihatnya melaui protocol Kerberos yang merupakan protocol single sign-on dimana kita bisa mengakses beberapa aplikasi dengan satu set kredensial. Biasanya, nama user ditampung dalam cname sehingga kita lakukan filtering agar hanya line yang memiliki detail mengenai cname tampil dalam wireshark.

Setelah itu, dalam line AS-REQ yang merupakan request dari client ke authentication server, kita lihat bagian detail dari request tersebut melalui “Kerberos -> as-req -> req-body -> cname -> cname-string: 1 item”. Dalam cname-string, didapatkan bahwa nama user adalah “margaret.dunn”.

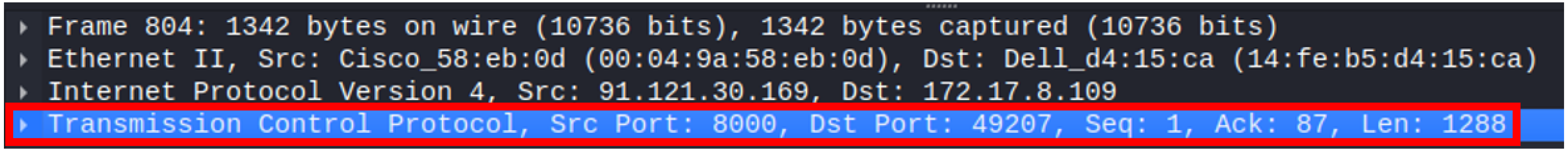
WHAT IS THE SHA256 FILE HASH OF THE WINDOWS EXECUTABLE FILE SENT TO THE INFECTED WINDOWS HOST?



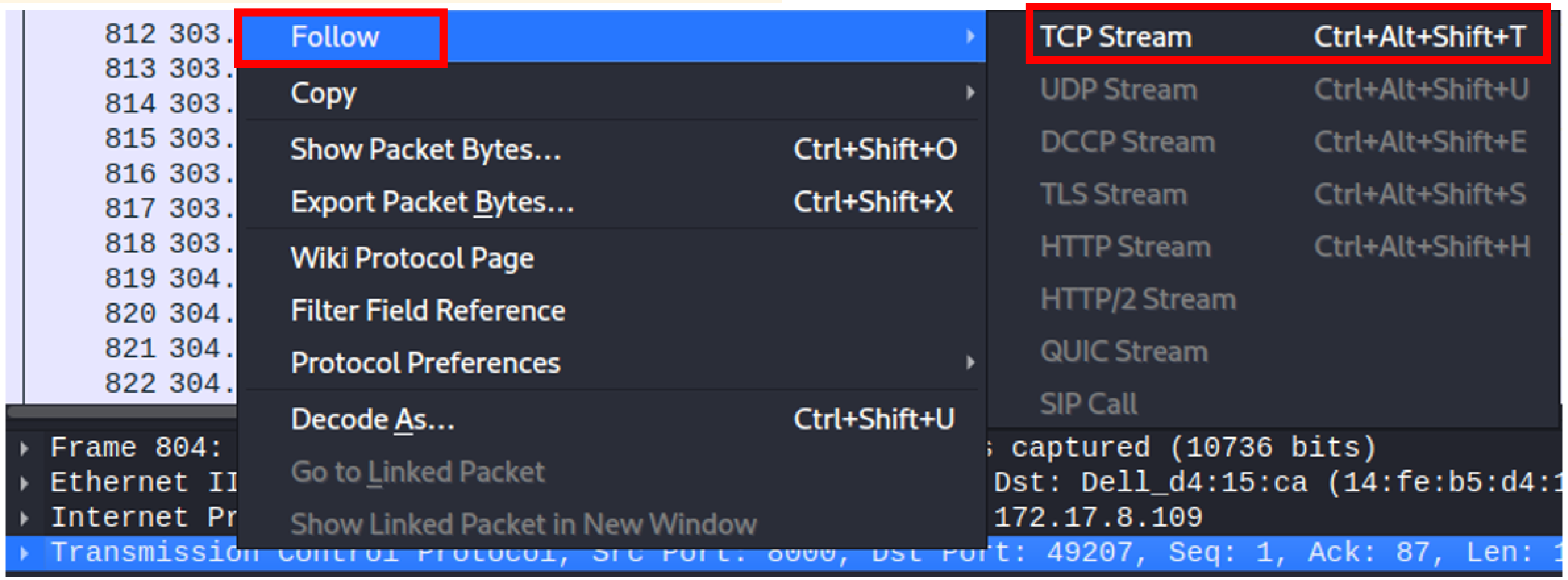
```
http
```



```
802 303.751237 172.17.8.109   91.121.30.169  HTTP     140 91.121.30.169:8000    GET /91msE95B/actiV.bin
983 304.477308 91.121.30.169  172.17.8.109   HTTP    1162                       HTTP/1.1 200 OK
```



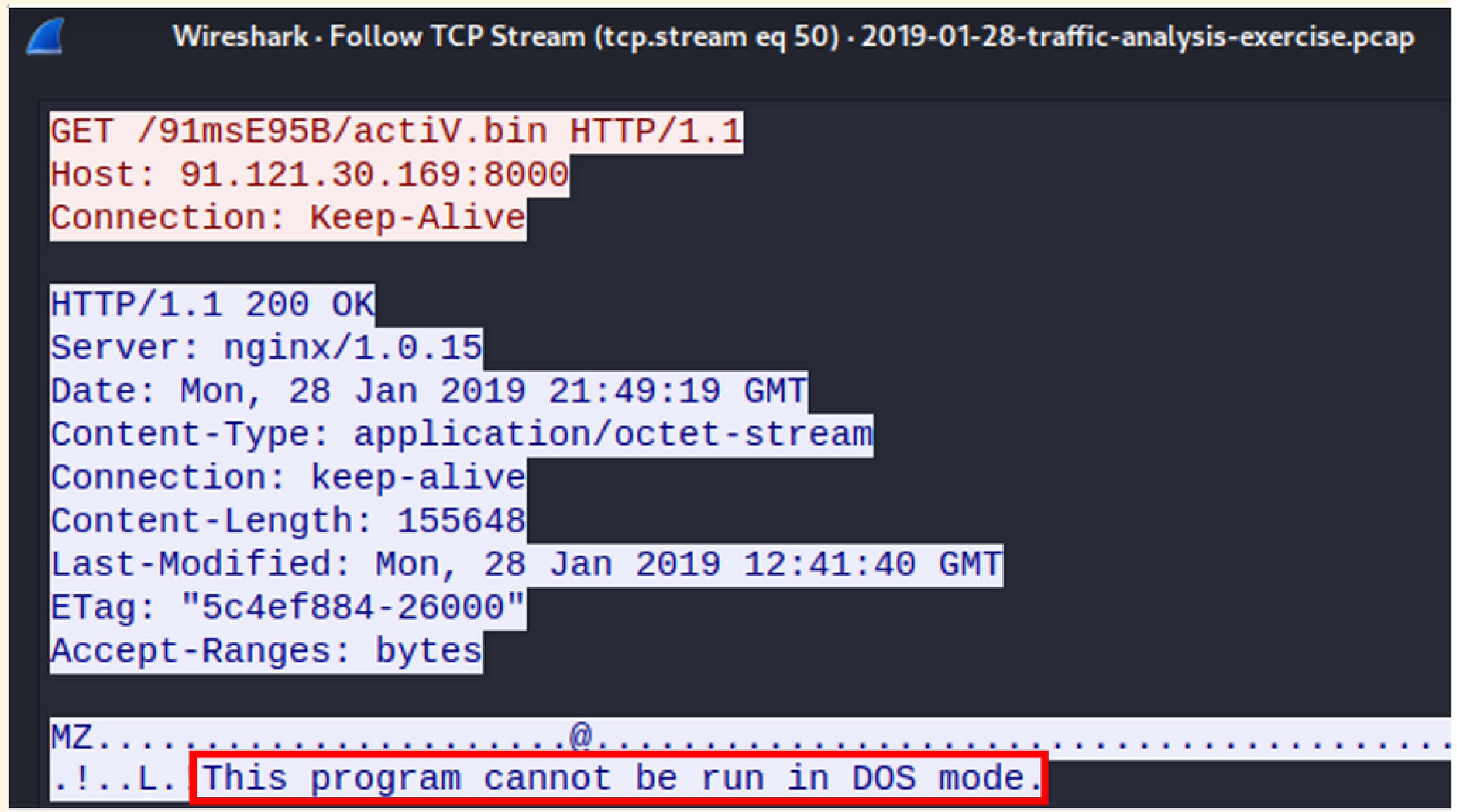
```
Frame 804: 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits)
Ethernet II, Src: Cisco_58:eb:0d (00:04:9a:58:eb:0d), Dst: Dell_d4:15:ca (14:fe:b5:d4:15:ca)
Internet Protocol Version 4, Src: 91.121.30.169, Dst: 172.17.8.109
Transmission Control Protocol, Src Port: 8000, Dst Port: 49207, Seq: 1, Ack: 87, Len: 1288
```



```
812 303.
813 303.
814 303.
815 303.
816 303.
817 303.
818 303.
819 304.
820 304.
821 304.
822 304.
Frame 804:                                                 ; captured (10736 bits)
Ethernet II                                                 Dst: Dell_d4:15:ca (14:fe:b5:d4:1
Internet Pr                                                 172.17.8.109
Transmission Control Protocol, Src Port: 8000, Dst Port: 49207, Seq: 1, Ack: 87, Len: 1
```

Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call

WHAT IS THE SHA256 FILE HASH OF THE WINDOWS EXECUTABLE FILE SENT TO THE INFECTED WINDOWS HOST?

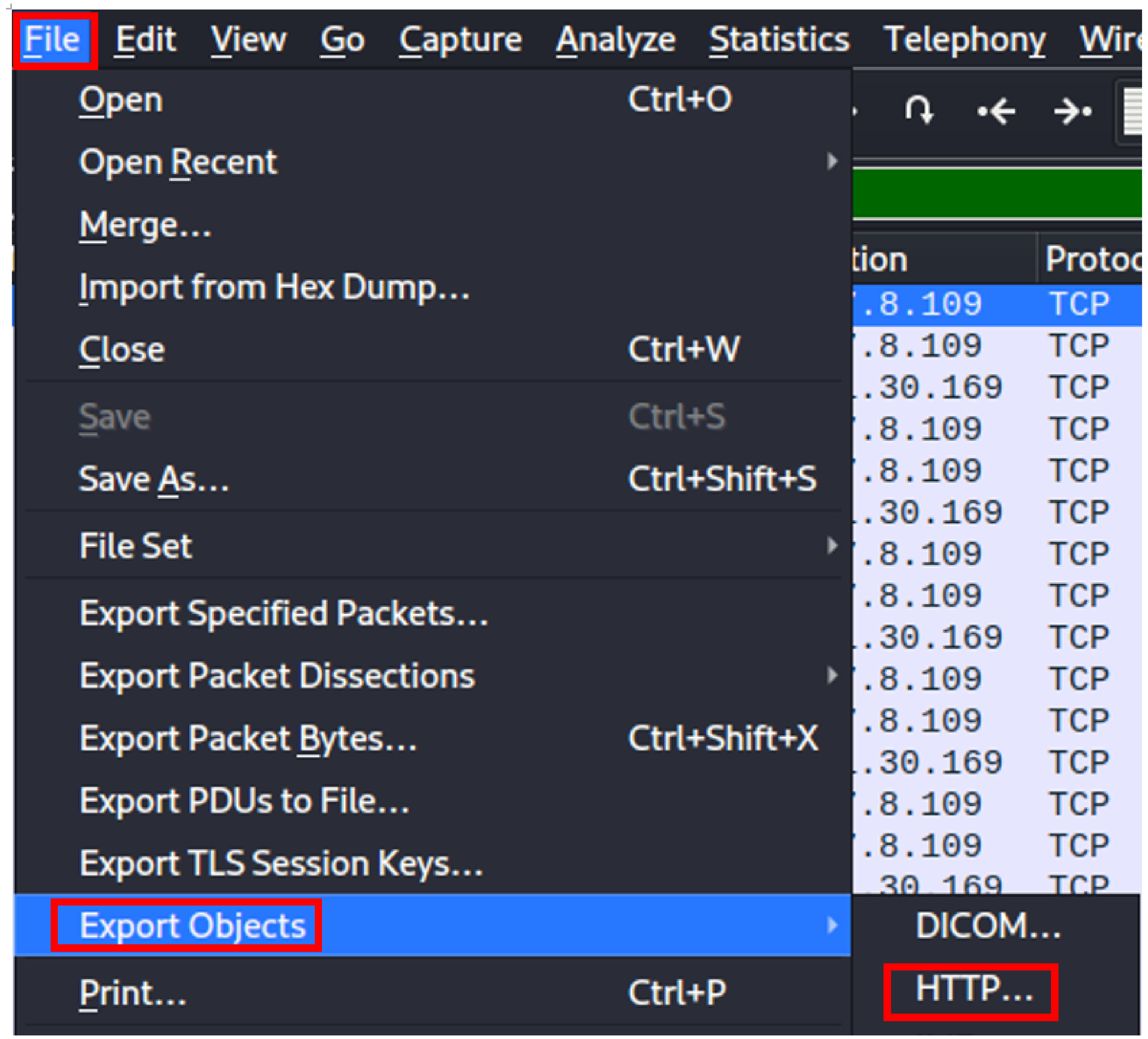


Wireshark · Follow TCP Stream (tcp.stream eq 50) · 2019-01-28-traffic-analysis-exercise.pcap

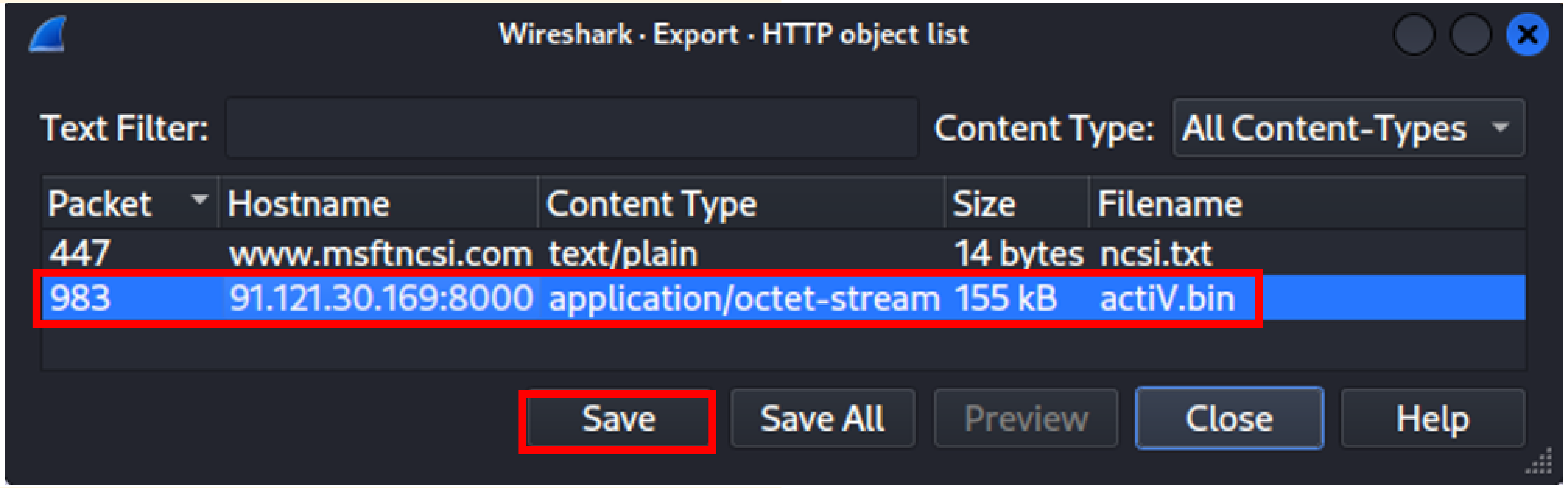
```
GET /91msE95B/actiV.bin HTTP/1.1
Host: 91.121.30.169:8000
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Mon, 28 Jan 2019 21:49:19 GMT
Content-Type: application/octet-stream
Connection: keep-alive
Content-Length: 155648
Last-Modified: Mon, 28 Jan 2019 12:41:40 GMT
ETag: "5c4ef884-26000"
Accept-Ranges: bytes

MZ......................@...................................
.!..L. This program cannot be run in DOS mode.
```



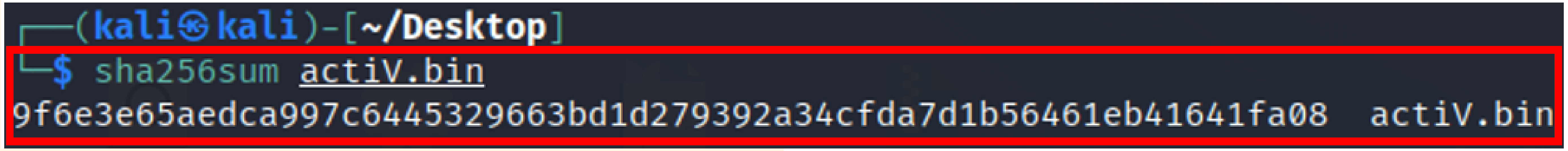
WHAT IS THE SHA256 FILE HASH OF THE WINDOWS EXECUTABLE FILE SENT TO THE INFECTED WINDOWS HOST?



Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
447	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
983	91.121.30.169:8000	application/octet-stream	155 kB	actiV.bin



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sha256sum actiV.bin
9f6e3e65aedca997c6445329663bd1d279392a34cfda7d1b56461eb41641fa08  actiV.bin
```

WHAT IS THE SHA256 FILE HASH OF THE WINDOWS EXECUTABLE FILE SENT TO THE INFECTED WINDOWS HOST?

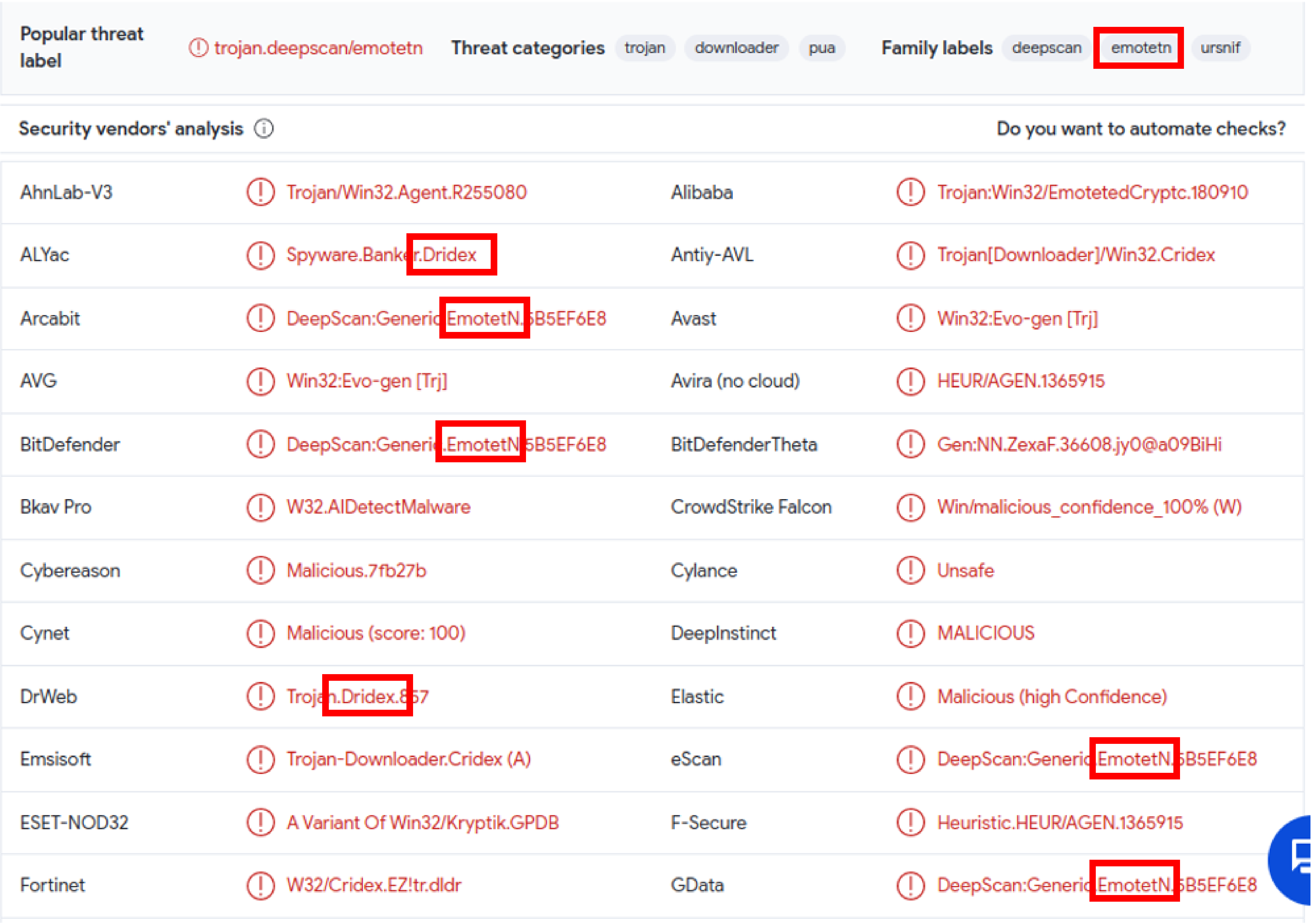
Jawaban:

9f6e3e65aedca997c6445329663bd1d279392a34cfda7d1b56461eb41641fa08

Dengan filter http, terdapat traffic yang mencurigakan pada line 802 yang merupakan GET request dan line 983 yang memberikan http response “OK”. Pada details line 983, kita lihat TCP stream melalui right click “Transmission Control Protocol”, lalu click “Follow” dan click “TCP Stream”. Dalam TCP Stream, ada pesan “This program cannot be run in DOS mode” yang menandakan bahwa file dapat berupa exe yang tidak bisa run di Linux.

Setelah itu, lakukan download file dengan cara “File -> Export Objects -> HTTP”, lalu click packet 983 dan click “Save” untuk save file. Setelah file berhasil disave, menggunakan tool sha256 sum, didapatkan hash dari file tersebut.

BASED ON THE IDS ALERTS, WHAT TYPE OF INFECTION IS THIS?



Popular threat label: trojan.deepscan/emotetn

Threat categories: trojan, downloader, pua

Family labels: deepscan, emotetn, ursnif

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R255080	Alibaba	Trojan:Win32/EmotetedCryptc.180910
ALYac	Spyware.Banker.Dridex	Antiy-AVL	Trojan[Downloader]/Win32.Cridex
Arcabit	DeepScan:Generic.EmotetN.5B5EF6E8	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1365915
BitDefender	DeepScan:Generic.EmotetN.5B5EF6E8	BitDefenderTheta	Gen:NN.ZexaF.36608.jy0@a09BiHi
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.7fb27b	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Dridex.857	Elastic	Malicious (high Confidence)
Emsisoft	Trojan-Downloader.Cridex (A)	eScan	DeepScan:Generic.EmotetN.5B5EF6E8
ESET-NOD32	A Variant Of Win32/Kryptik.GPDB	F-Secure	Heuristic.HEUR/AGEN.1365915
Fortinet	W32/Cridex.EZ!tr.dldr	GData	DeepScan:Generic.EmotetN.5B5EF6E8

BASED ON THE IDS ALERTS, WHAT TYPE OF INFECTION IS THIS?

Jawaban: Botnet (EmotetN/Dridex)

Menggunakan VirusTotal, didapatkan bahwa file tersebut berupa EmotetN, tetapi ada beberapa layanan antivirus dan writeup menyatakan bahwa file tersebut berupa Dridex, dimana EmotetN dan Dridex merupakan jenis malware botnet yang berupa trojan perbankan sehingga jenis infeksi ini adalah botnet.

TERIMA KASIH