**Challenge:** HawkEye Lab

**Platform:** CyberDefenders

**Category:** Network Forensics

**Difficulty:** Medium

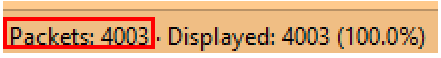
**Tools Used:** Wireshark, Zui, NetworkMiner, VirusTotal

**Summary:** This lab involved investigating a PCAP from a compromised host. It began with a phishing email that contained a download link for a keylogger. The primary tools used were Wireshark and NetworkMiner, although, you could easily complete this challenge through using only Wireshark. I found this lab to be enjoyable, as it walks you through a lot of Wireshark features that can be super helpful when baselining network traffic.

**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.

**How many packets does the capture have?**

If you open the PCAP file with Wireshark, you can find the number of packets contained within the PCAP near the bottom right-hand corner:

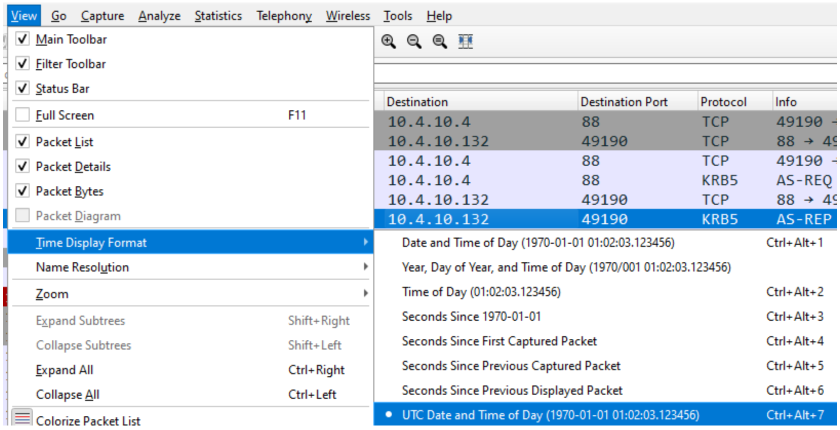


Packets: 4003 · Displayed: 4003 (100.0%)

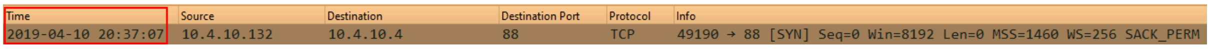
Answer: 4003

**At what time was the first packet captured?**

You can see when the first packet was captured by looking at the value under the Time column. However, make sure you have the time set to UTC, you can do so by navigating to View > Time Display Format:


View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
☑ Main Toolbar
☑ Filter Toolbar
☑ Status Bar
□ Full Screen F11
☑ Packet List
☑ Packet Details
☑ Packet Bytes
□ Packet Diagram
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since First Captured Packet Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
● UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7

```
Destination     Destination Port  Protocol  Info
10.4.10.4       88                TCP       49190 -
10.4.10.132     49190             TCP       88 → 49
10.4.10.4       88                TCP       49190 -
10.4.10.4       88                KRB5      AS-REQ
10.4.10.132     49190             TCP       88 → 49
10.4.10.132     49190             KRB5      AS-REP
```

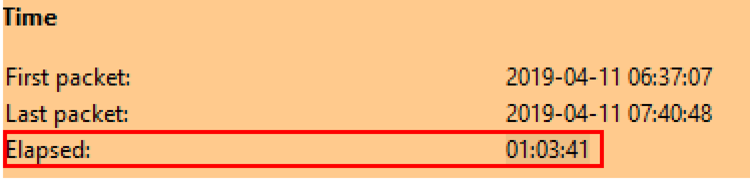


```
Time                 Source        Destination  Destination Port  Protocol  Info
2019-04-10 20:37:07  10.4.10.132   10.4.10.4    88                TCP       49190 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
```

Answer: 2019-04-10 20:37

**What is the duration of the capture?**

You can find the duration of the capture by navigating to Statistics > Capture File Properties:



**Time**

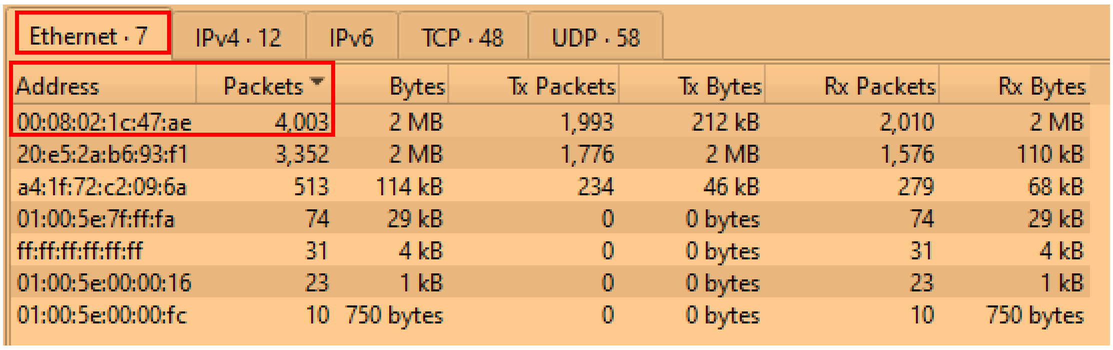
| | |
|---|---|
| First packet: | 2019-04-11 06:37:07 |
| Last packet: | 2019-04-11 07:40:48 |
| Elapsed: | 01:03:41 |

The elapsed time shows the time between the first and last packet being captured.

Answer: 01:03:41

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

To find the most active computer at the link level, we can navigate to Statistics > Endpoints > Ethernet, and filter the Packets column in descending order:



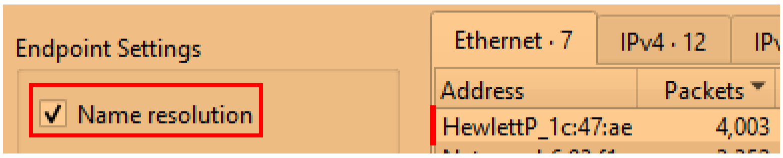
| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|---|---|---|---|---|---|---|
| 00:08:02:1c:47:ae | 4,003 | 2 MB | 1,993 | 212 kB | 2,010 | 2 MB |
| 20:e5:2a:b6:93:f1 | 3,352 | 2 MB | 1,776 | 2 MB | 1,576 | 110 kB |
| a4:1f:72:c2:09:6a | 513 | 114 kB | 234 | 46 kB | 279 | 68 kB |
| 01:00:5e:7f:ff:fa | 74 | 29 kB | 0 | 0 bytes | 74 | 29 kB |
| ff:ff:ff:ff:ff:ff | 31 | 4 kB | 0 | 0 bytes | 31 | 4 kB |
| 01:00:5e:00:00:16 | 23 | 1 kB | 0 | 0 bytes | 23 | 1 kB |
| 01:00:5e:00:00:fc | 10 | 750 bytes | 0 | 0 bytes | 10 | 750 bytes |

As the name suggests, the Endpoints statistics shows statistics about the endpoints captured.

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

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

If you tick the Name resolution box in the Endpoints statistics tab, you can resolve the OUI of the MAC address:



Endpoint Settings

☑ Name resolution

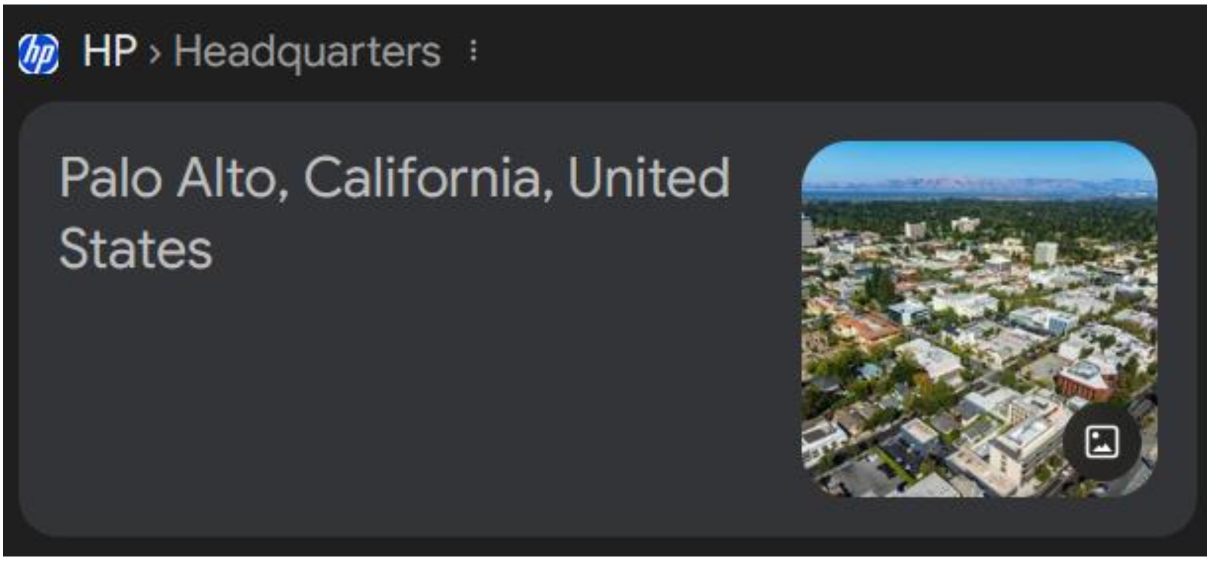
| Address | Packets |
|---|---|
| HewlettP_1c:47:ae | 4,003 |

Upon researching HewlettP, you can find results for Hewlett-Packet (i.e., HP).

Answer: Hewlett-Packard

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

If you search for the headquarters of Hewlett-Packard, you can see that it is located in Palo Alto:



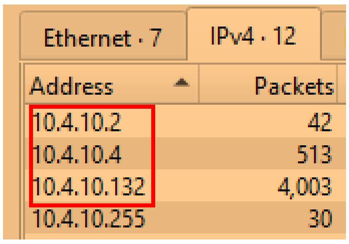
HP › Headquarters

Palo Alto, California, United States

Answer: Palo Alto

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

If you switch to the IPv4 tab in Endpoint statistics, we can see that 3 hosts are within a private IP address range. The reason 10.4.10.255 is not included in the total is because this is the broadcast address for the subnet /24 and does not count as a separate computer.

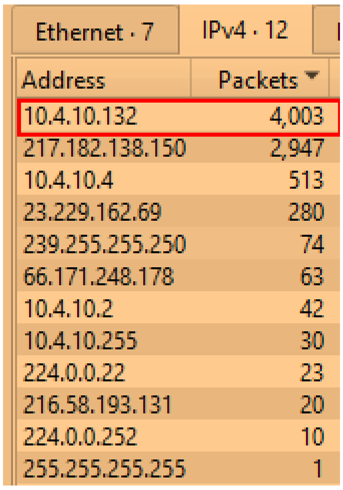


| Address | Packets |
|---|---|
| 10.4.10.2 | 42 |
| 10.4.10.4 | 513 |
| 10.4.10.132 | 4,003 |
| 10.4.10.255 | 30 |

Answer: 3

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

Staying within the IPv4 tab in Endpoint statistics, we can see that 10.4.10.132 is the most active:

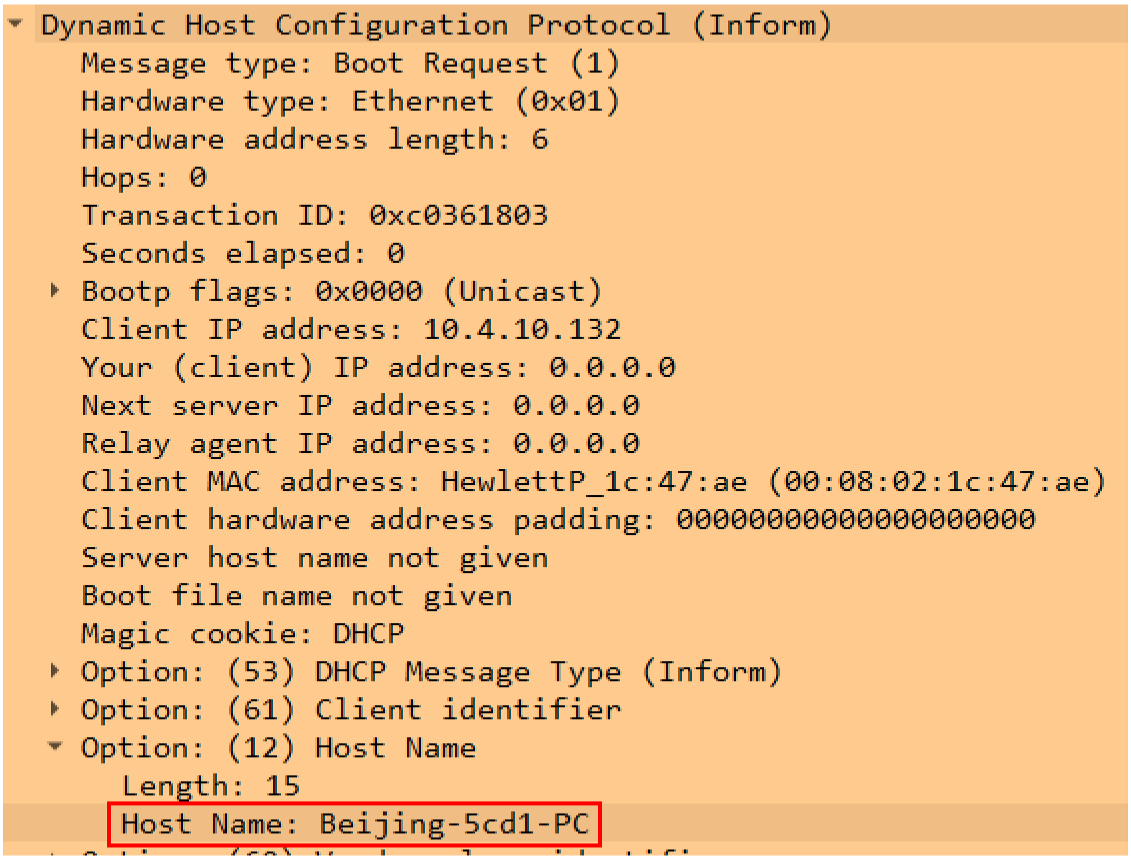


| Address | Packets |
|---|---|
| 10.4.10.132 | 4,003 |
| 217.182.138.150 | 2,947 |
| 10.4.10.4 | 513 |
| 23.229.162.69 | 280 |
| 239.255.255.250 | 74 |
| 66.171.248.178 | 63 |
| 10.4.10.2 | 42 |
| 10.4.10.255 | 30 |
| 224.0.0.22 | 23 |
| 216.58.193.131 | 20 |
| 224.0.0.252 | 10 |
| 255.255.255.255 | 1 |

A great resource from Unit42 talks about how to identify hosts and users using Wirehsark. In my case, I used the following display filter to find DHCP traffic associated with this host:

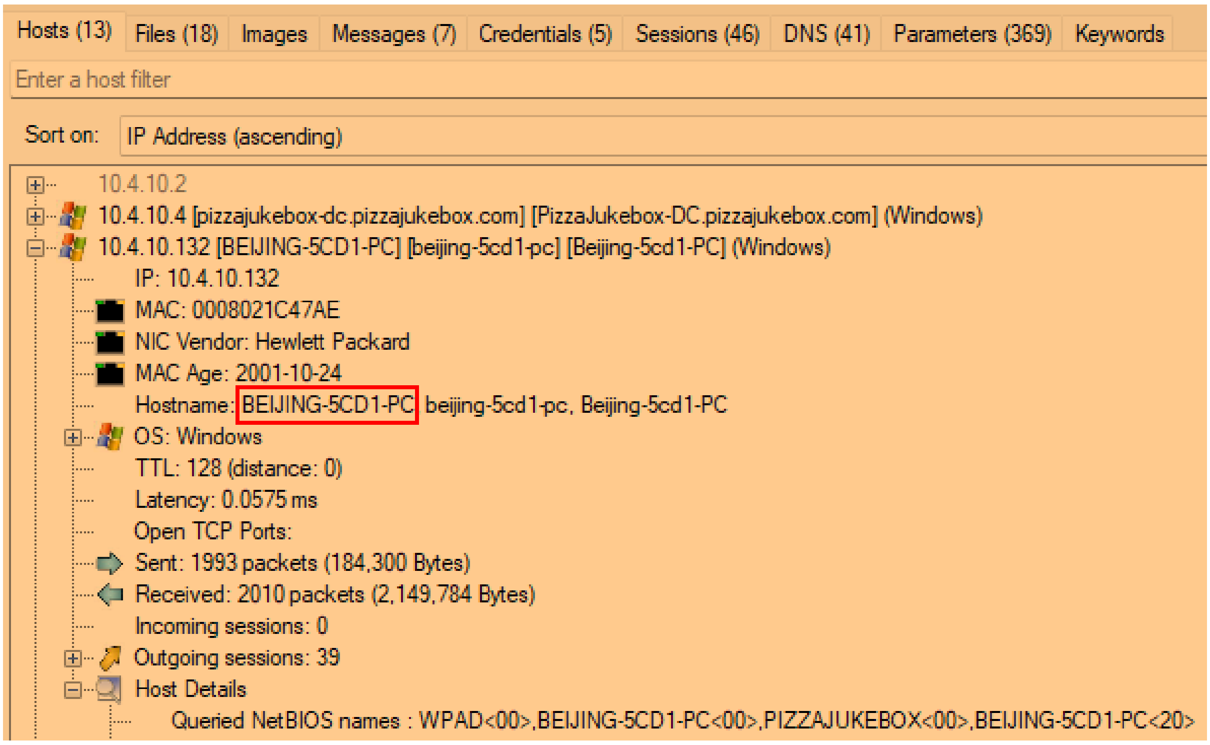
- `(ip.addr==10.4.10.132) && (dhcp)`

In the packet details pane, you can expand the DHCP dropdown to find the Host Name:



```
▾ 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: HewlettP_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-5cd1-PC
```

Alternatively, using a tool like NetworkMiner makes this much easier, as you can find the host name for this computer among other key information under the Hosts tab:



Sort on: IP Address (ascending)

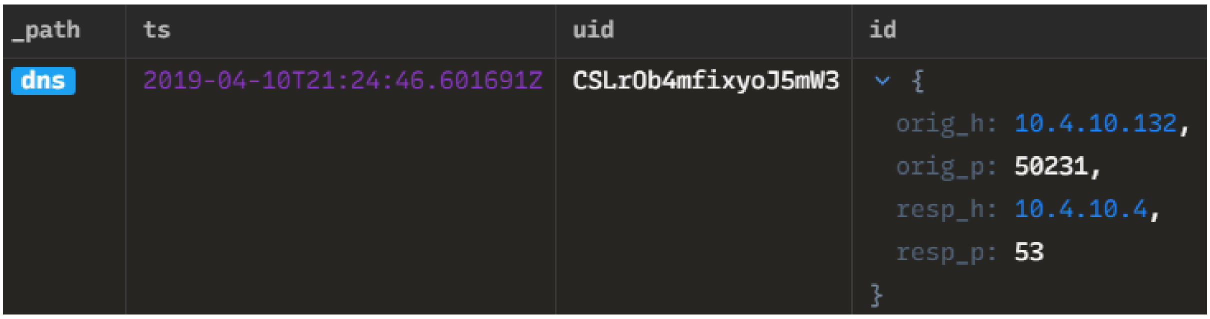
```
⊞ 10.4.10.2
⊞ 10.4.10.4 [pizzajukebox-dc.pizzajukebox.com] [PizzaJukebox-DC.pizzajukebox.com] (Windows)
⊟ 10.4.10.132 [BEIJING-5CD1-PC] [beijing-5cd1-pc] [Beijing-5cd1-PC] (Windows)
    IP: 10.4.10.132
    MAC: 0008021C47AE
    NIC Vendor: Hewlett Packard
    MAC Age: 2001-10-24
    Hostname: BEIJING-5CD1-PC beijing-5cd1-pc, Beijing-5cd1-PC
  ⊞ OS: Windows
    TTL: 128 (distance: 0)
    Latency: 0.0575 ms
    Open TCP Ports:
    Sent: 1993 packets (184,300 Bytes)
    Received: 2010 packets (2,149,784 Bytes)
    Incoming sessions: 0
  ⊞ Outgoing sessions: 39
  ⊟ Host Details
      Queried NetBIOS names : WPAD<00>,BEIJING-5CD1-PC<00>,PIZZAJUKEBOX<00>,BEIJING-5CD1-PC<20>
```

Answer: Beijing-5cd1-PC

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

If you use the dns display filter in Wireshark, you can see that all queries are sent to 10.4.10.4. This indicates that the DNS server is 10.4.10.4. Within Zui, you can use the following query to also see that the resp_h for DNS queries is 10.4.10.4:

- `_path=="dns"`

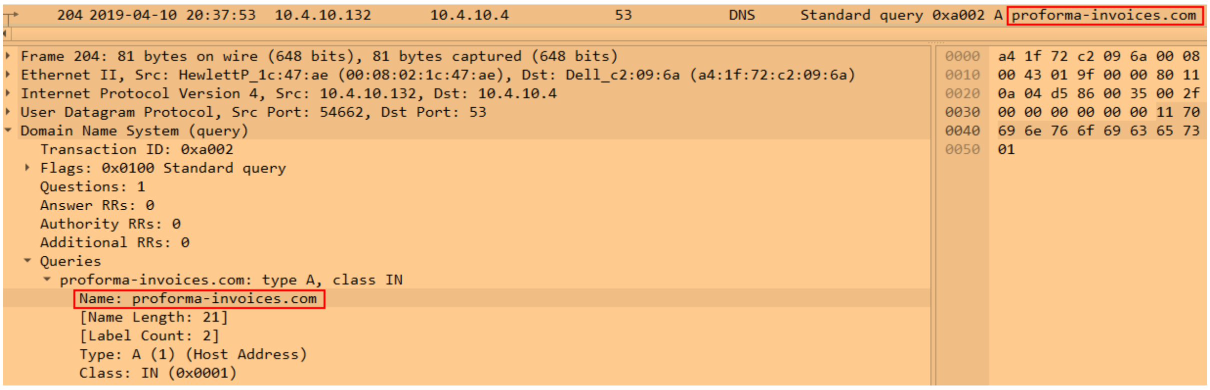


| _path | ts | uid | id |
|---|---|---|---|
| dns | 2019-04-10T21:24:46.601691Z | CSLrOb4mfixyoJ5mW3 | { <br> orig_h: 10.4.10.132, <br> orig_p: 50231, <br> resp_h: 10.4.10.4, <br> resp_p: 53 <br> } |

Answer: 10.4.10.4

**What domain is the victim asking about in packet 204?**

If you scroll down the dns display filter output, packet number 204 is very close to the top of the results. We can see that the victim is querying proforma-invoices.com:

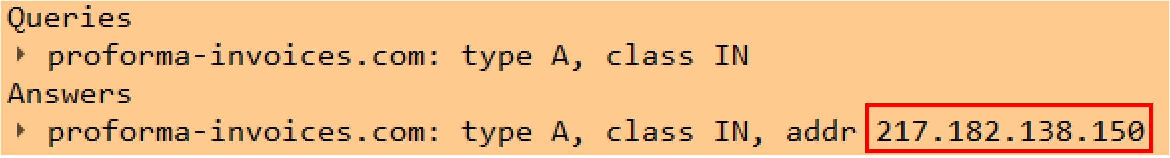


```
204 2019-04-10 20:37:53  10.4.10.132      10.4.10.4          53          DNS      Standard query 0xa002 A proforma-invoices.com

Frame 204: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)                         0000  a4 1f 72 c2 09 6a 00 08
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)  0010  00 43 01 9f 00 00 80 11
Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4                                 0020  0a 04 d5 86 00 35 00 2f
User Datagram Protocol, Src Port: 54662, Dst Port: 53                                         0030  00 00 00 00 00 00 11 70
Domain Name System (query)                                                                    0040  69 6e 76 6f 69 63 65 73
  Transaction ID: 0xa002                                                                      0050  01
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  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)
```

Answer: proforma-invoices.com

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

If you look at the query response from the query found in the previous question, we can see that it responded with 217.182.138.150:



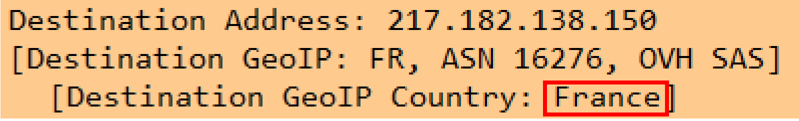
```
Queries
 ▸ proforma-invoices.com: type A, class IN
Answers
 ▸ proforma-invoices.com: type A, class IN, addr 217.182.138.150
```

Answer: 217.182.138.150

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

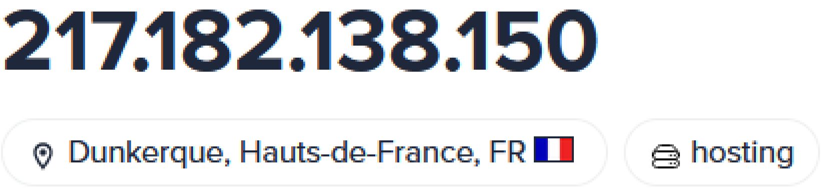
Fortunately for me, I have the Maxmind GeoIP databases installed, which shows GeoIP information. Using the following filter, I could see that the IP in question geolocates to France:

- `ip.addr==217.182.138.150`



```
Destination Address: 217.182.138.150
[Destination GeoIP: FR, ASN 16276, OVH SAS]
  [Destination GeoIP Country: France]
```

You could also use a tool like IPinfo to get the same answer:



217.182.138.150

Dunkerque, Hauts-de-France, FR

hosting

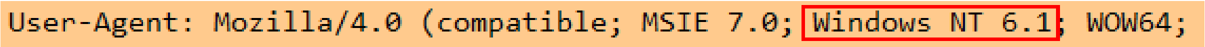
Answer: France

**What operating system does the victim's computer run?**

The user-agent field can provide a wealth of information, including the host OS behind the request (note, this can be spoofed/changed, so take it with a grain of salt). Using the following display filter, we can find HTTP requests associated with the victim host:

- `ip.addr==10.4.10.132 && http`

If you click on any of the GET requests and expand HTTP within the protocol details pane, you can find the OS and version:

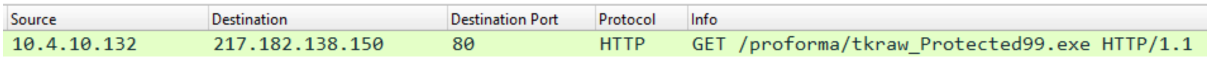


```
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
```

Answer: Windows NT 6.1

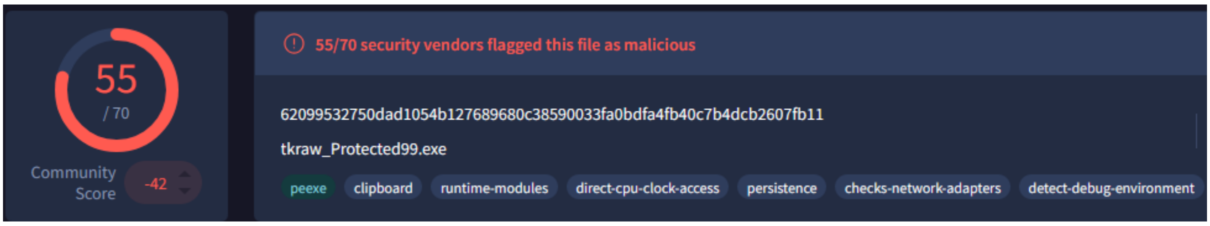
### What is the name of the malicious file downloaded by the accountant?

Using the same filter as the previous question, we can see that a file called tkraw_Protected99.exe was downloaded:



| Source | Destination | Destination Port | Protocol | Info |
|---|---|---|---|---|
| 10.4.10.132 | 217.182.138.150 | 80 | HTTP | GET /proforma/tkraw_Protected99.exe HTTP/1.1 |

If you export this HTTP object via File > Export Objects > HTTP, hash the file, and submit it to VirusTotal, we can see that it received 55/70 detections:



55/70 security vendors flagged this file as malicious

62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11

tkraw_Protected99.exe

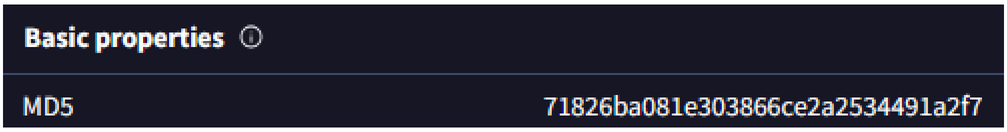
Answer: tkraw_Protected99.exe

### What is the md5 hash of the downloaded file?

To generate the MD5 hash of the file, we can use the Get-FileHash cmdlet in PowerShell like as follows:

- `Get-FileHash -algorithm MD5 .\tkraw_Protected99.exe`

Alternatively, if you used another hashing algorithm, you could submit it to VirusTotal and find the MD5 hash in the Details tab:



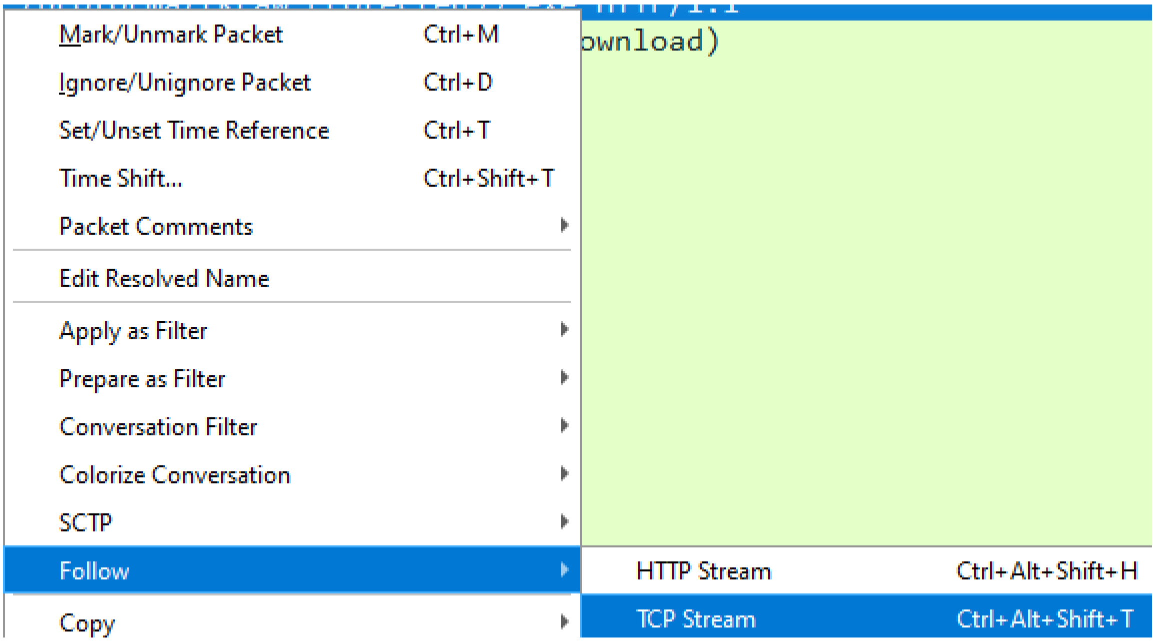
Basic properties

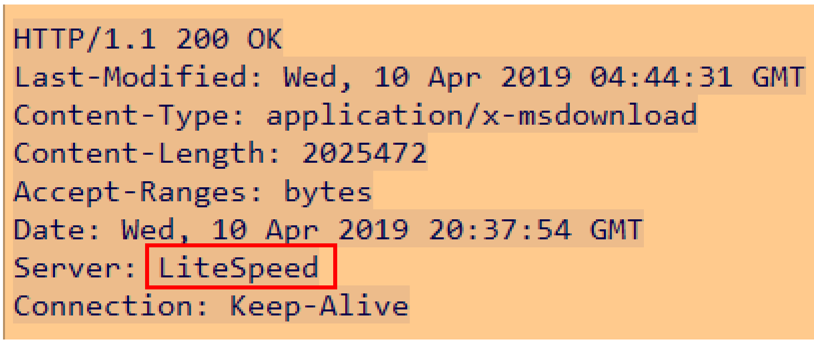
| | |
|---|---|
| MD5 | 71826ba081e303866ce2a2534491a2f7 |

Answer: 71826BA081E303866CE2A2534491A2F7

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

If you follow the TCP stream of the GET request to download the binary, we can find information about the webserver via its HTTP headers:


ownload)
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
HTTP Stream Ctrl+Alt+Shift+H
TCP Stream Ctrl+Alt+Shift+T



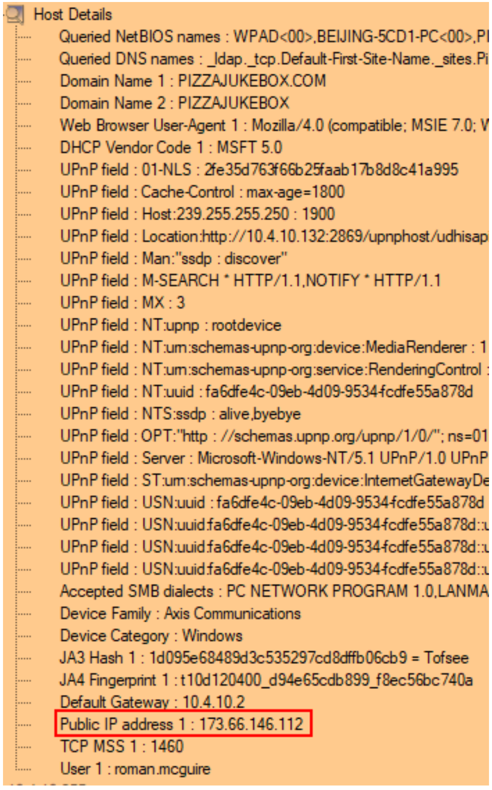
```
HTTP/1.1 200 OK
Last-Modified: Wed, 10 Apr 2019 04:44:31 GMT
Content-Type: application/x-msdownload
Content-Length: 2025472
Accept-Ranges: bytes
Date: Wed, 10 Apr 2019 20:37:54 GMT
Server: LiteSpeed
Connection: Keep-Alive
```

The blue text indicates responses from the server, as you can see in the above image, LiteSpeed is the software behind the webserver.

Answer: LiteSpeed

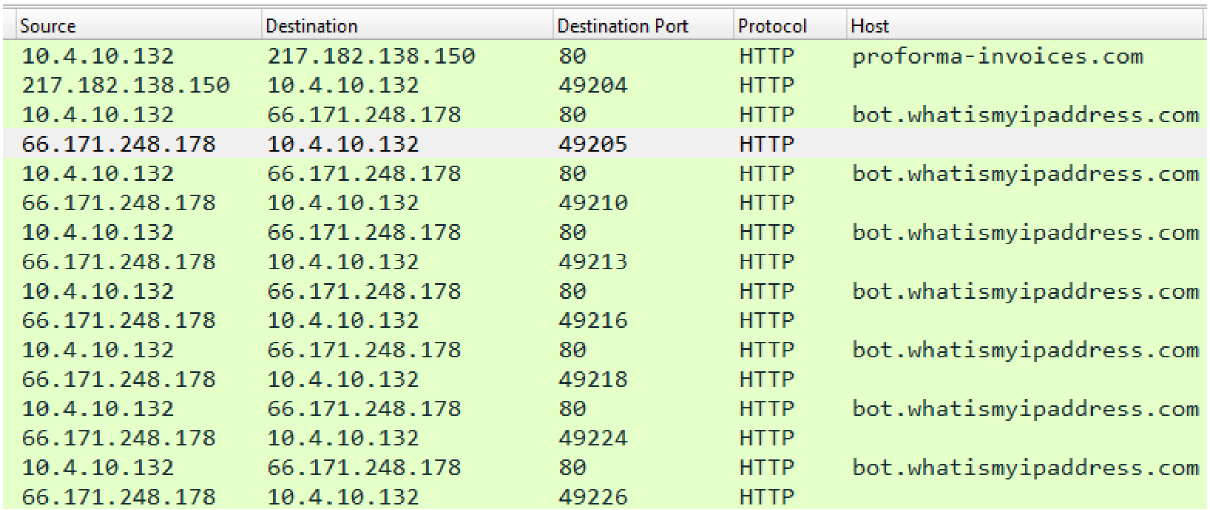
**What is the public IP of the victim's computer?**

If you expand the Host Details section for 10.4.10.132 in NetworkMiner, we can see the public IP address of the victim's host:



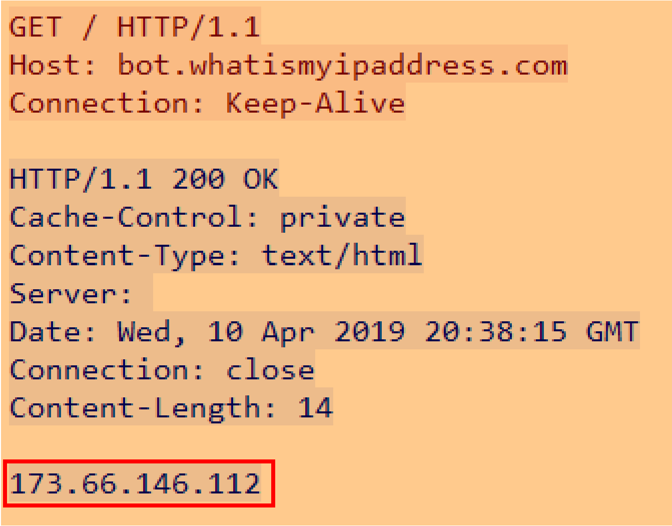
```
Host Details
    Queried NetBIOS names : WPAD<00>,BEIJING-5CD1-PC<00>,PI
    Queried DNS names : _ldap._tcp.Default-First-Site-Name._sites.Pi
    Domain Name 1 : PIZZAJUKEBOX.COM
    Domain Name 2 : PIZZAJUKEBOX
    Web Browser User-Agent 1 : Mozilla/4.0 (compatible; MSIE 7.0; W
    DHCP Vendor Code 1 : MSFT 5.0
    UPnP field : 01-NLS : 2fe35d763f66b25faab17b8d8c41a995
    UPnP field : Cache-Control : max-age=1800
    UPnP field : Host:239.255.255.250 : 1900
    UPnP field : Location:http://10.4.10.132:2869/upnphost/udhisap
    UPnP field : Man:"ssdp : discover"
    UPnP field : M-SEARCH * HTTP/1.1,NOTIFY * HTTP/1.1
    UPnP field : MX : 3
    UPnP field : NT:upnp : rootdevice
    UPnP field : NT:urn:schemas-upnp-org:device:MediaRenderer : 1
    UPnP field : NT:urn:schemas-upnp-org:service:RenderingControl :
    UPnP field : NT:uuid : fa6dfe4c-09eb-4d09-9534-fcdfe55a878d
    UPnP field : NTS:ssdp : alive,byebye
    UPnP field : OPT:"http : //schemas.upnp.org/upnp/1/0/"; ns=01
    UPnP field : Server : Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP
    UPnP field : ST:urn:schemas-upnp-org:device:InternetGatewayDe
    UPnP field : USN:uuid : fa6dfe4c-09eb-4d09-9534-fcdfe55a878d
    UPnP field : USN:uuid:fa6dfe4c-09eb-4d09-9534-fcdfe55a878d::u
    UPnP field : USN:uuid:fa6dfe4c-09eb-4d09-9534-fcdfe55a878d::u
    UPnP field : USN:uuid:fa6dfe4c-09eb-4d09-9534-fcdfe55a878d::u
    Accepted SMB dialects : PC NETWORK PROGRAM 1.0,LANMA
    Device Family : Axis Communications
    Device Category : Windows
    JA3 Hash 1 : 1d095e68489d3c535297cd8dffb06cb9 = Tofsee
    JA4 Fingerprint 1 : t10d120400_d94e65cdb899_f8ec56bc740a
    Default Gateway : 10.4.10.2
    Public IP address 1 : 173.66.146.112
    TCP MSS 1 : 1460
    User 1 : roman.mcguire
```

Alternatively, shortly after the malicious binary was downloaded, we can see several requests to bot,whatismyipaddress.com, this will likely return the user's public IP address:



| Source | Destination | Destination Port | Protocol | Host |
|---|---|---|---|---|
| 10.4.10.132 | 217.182.138.150 | 80 | HTTP | proforma-invoices.com |
| 217.182.138.150 | 10.4.10.132 | 49204 | HTTP | |
| 10.4.10.132 | 66.171.248.178 | 80 | HTTP | bot.whatismyipaddress.com |
| 66.171.248.178 | 10.4.10.132 | 49205 | HTTP | |
| 10.4.10.132 | 66.171.248.178 | 80 | HTTP | bot.whatismyipaddress.com |
| 66.171.248.178 | 10.4.10.132 | 49210 | HTTP | |
| 10.4.10.132 | 66.171.248.178 | 80 | HTTP | bot.whatismyipaddress.com |
| 66.171.248.178 | 10.4.10.132 | 49213 | HTTP | |
| 10.4.10.132 | 66.171.248.178 | 80 | HTTP | bot.whatismyipaddress.com |
| 66.171.248.178 | 10.4.10.132 | 49216 | HTTP | |
| 10.4.10.132 | 66.171.248.178 | 80 | HTTP | bot.whatismyipaddress.com |
| 66.171.248.178 | 10.4.10.132 | 49218 | HTTP | |
| 10.4.10.132 | 66.171.248.178 | 80 | HTTP | bot.whatismyipaddress.com |
| 66.171.248.178 | 10.4.10.132 | 49224 | HTTP | |
| 10.4.10.132 | 66.171.248.178 | 80 | HTTP | bot.whatismyipaddress.com |
| 66.171.248.178 | 10.4.10.132 | 49226 | HTTP | |

If you follow the TCP stream of one of these requests, we can find the public IP address of the victim in the response:



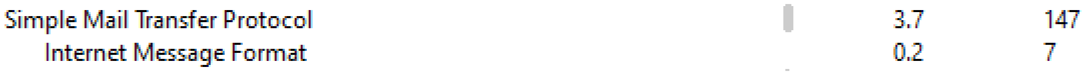
```
GET / HTTP/1.1
Host: bot.whatismyipaddress.com
Connection: Keep-Alive

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
```

Answer: 173.66.146.112

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

If you filter for the compromised host, and navigate to Statistics > Protocol Hierarchy, we can see some SMTP traffic:

- `ip.addr==10.4.10.132`



```
Simple Mail Transfer Protocol        3.7    147
    Internet Message Format          0.2    7
```

Using the following display filter, we can look for SMTP packets:

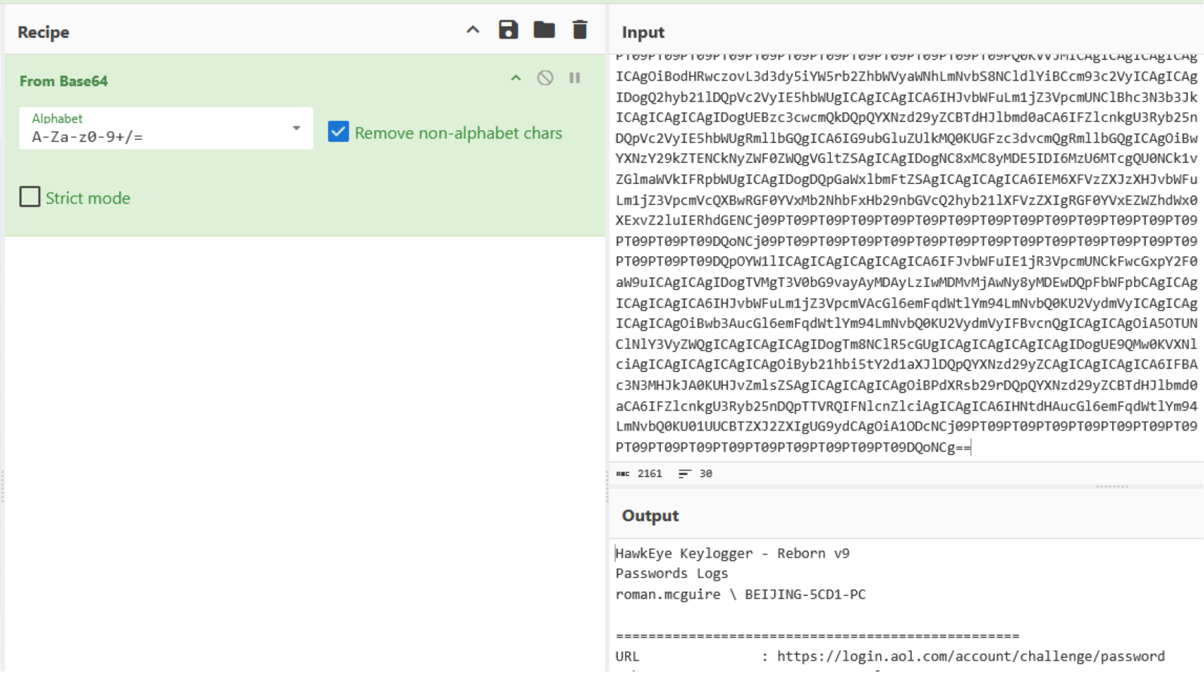
- `(ip.addr==10.4.10.132 ) && (smtp)`

If you followed the first packet's TCP stream, we can see a message being sent from sales.del@macwinlogistics.in to sales.del@macwinlogistics.in that contains a Base64 encoded payload:

```
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?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZ
YuMTQ2LjExMg==?=
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
```

```
SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkNClBhc3N3b3JkcyBMb2dzDQpyb21hbi5t
Y2d1aXJlIFwgQkVJSklORy01Q0QxLVBDDQoNCj09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09DQpVUkwgICAgICAgICAgICAgICA6IGh0dHBzOi8v
bG9naW4uYW9sLmNvbS9hY2NvdW50L2NoYWxsZW5nZS9wYXNzd29yZA0KV2ViIEJyb3dzZXIg
ICAgICAgOiBJbnRlcm5ldCBFeHBsb3JlciA3LjAgLSA5LjANClVzZXIgTmFtZSAgICAgICAg
IDogcm9tYW4ubWNndWlyZTkxNEBhb2wuY29tDQpQYXNzd29yZCAgICAgICAgICA6IFBAc3N3
MHJkJA0KUGFzc3dvcmQgU3RyZW5ndGggOiBWZXJ5IFN0cm9uZw0KVXNlciBOYW1lIEZpZWxk
ICAgOiANClBhc3N3b3JkIEZpZWxkICAgIDogDQpDcmVhdGVkIFRpbWUgICAgICA6IA0KTW9k
aWZpZWQgVGltZSAgICAgOiANCkZpbGVuYW1lICAgICAgICAgIDogDQo9PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PQ0KDQo9PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PQ0KVVJMICAgICAgICAgICAg
ICAgOiBodHRwczovL3d3dy5iYW5rb2ZhbWVyaWNhLmNvbS8NCldlYiBCcm93c2VyICAgICAg
IDogQ2hyb21lDQpVc2VyIE5hbWUgICAgICAgICA6IHJvbWFuLm1jZ3VpcmUNClBhc3N3b3Jk
ICAgICAgICAgIDogUEBzc3cwcmQkDQpQYXNzd29yZCBTdHJlbmd0aCA6IFZlcnkgU3Ryb25n
DQpVc2VyIE5hbWUgRmllbGQgICA6IG9ubGluZUlkMQ0KUGFzc3dvcmQgRmllbGQgICAgOiBw
YXNzY29kZTENCkNyZWF0ZWQgVGltZSAgICAgIDogNC8xMC8yMDE5IDI6MzU6MTcgQU0NCk1v
ZGlmaWVkIFRpbWUgICAgIDogDQpGaWxlbmFtZSAgICAgICAgICA6IEM6XFVzZXJzXHJvbWFu
Lm1jZ3VpcmVcQXBwRGF0YVxMb2NhbFxHb29nbGVcQ2hyb21lXFVzZXIgRGF0YVxEZWZhdWx0
XExvZ2luIERhdGENCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQpOYW1lICAgICAgICAgICAgICA6IFJvbWFuIE1jR3VpcmUNCkFwcGxpY2F0
aW9uICAgICAgIDogTVMgT3V0bG9vayAyMDAyLzIwMDMvMjAwNy8yMDEwDQpFbWFpbCAgICAg
ICAgICAgICA6IHJvbWFuLm1jZ3VpcmVAcGl6emFqdWtlYm94LmNvbQ0KU2VydmVyICAgICAg
ICAgICAgOiBwb3AucGl6emFqdWtlYm94LmNvbQ0KU2VydmVyIFBvcnQgICAgICAgOiA5OTUN
ClNlY3VyZWQgICAgICAgICAgIDogTm8NClR5cGUgICAgICAgICAgICAgIDogUE9QMw0KVXNl
ciAgICAgICAgICAgICAgOiByb21hbi5tY2d1aXJlDQpQYXNzd29yZCAgICAgICAgICA6IFBA
c3N3MHJkJA0KUHJvZmlsZSAgICAgICAgICAgOiBPdXRsb29rDQpQYXNzd29yZCBTdHJlbmd0
aCA6IFZlcnkgU3Ryb25nDQpTTVRQIFNlcnZlciAgICAgICA6IHNtdHAucGl6emFqdWtlYm94
LmNvbQ0KU01UUCBTZXJ2ZXIgUG9ydCAgOiA1ODcNCj09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PT09DQoNCg==
```

If you decode this payload using CyberChef, we can see the output of HawkEye Keylogger:



Alphabet A-Za-z0-9+/=

☑ Remove non-alphabet chars

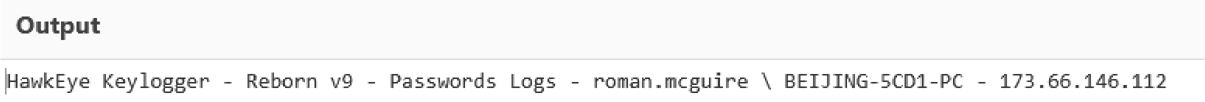
□ Strict mode

```
PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PQ0KVVJMICAgICAgICAgICAg
ICAgOiBodHRwczovL3d3dy5iYW5rb2ZhbWVyaWNhLmNvbS8NCldlYiBCcm93c2VyICAgICAg
IDogQ2hyb21lDQpVc2VyIE5hbWUgICAgICAgICA6IHJvbWFuLm1jZ3VpcmUNClBhc3N3b3Jk
ICAgICAgICAgIDogUEBzc3cwcmQkDQpQYXNzd29yZCBTdHJlbmd0aCA6IFZlcnkgU3Ryb25n
DQpVc2VyIE5hbWUgRmllbGQgICA6IG9ubGluZUlkMQ0KUGFzc3dvcmQgRmllbGQgICAgOiBw
YXNzY29kZTENCkNyZWF0ZWQgVGltZSAgICAgIDogNC8xMC8yMDE5IDI6MzU6MTcgQU0NCk1v
ZGlmaWVkIFRpbWUgICAgIDogDQpGaWxlbmFtZSAgICAgICAgICA6IEM6XFVzZXJzXHJvbWFu
Lm1jZ3VpcmVcQXBwRGF0YVxMb2NhbFxHb29nbGVcQ2hyb21lXFVzZXIgRGF0YVxEZWZhdWx0
XExvZ2luIERhdGENCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQpOYW1lICAgICAgICAgICAgICA6IFJvbWFuIE1jR3VpcmUNCkFwcGxpY2F0
aW9uICAgICAgIDogTVMgT3V0bG9vayAyMDAyLzIwMDMvMjAwNy8yMDEwDQpFbWFpbCAgICAg
ICAgICAgICA6IHJvbWFuLm1jZ3VpcmVAcGl6emFqdWtlYm94LmNvbQ0KU2VydmVyICAgICAg
ICAgICAgOiBwb3AucGl6emFqdWtlYm94LmNvbQ0KU2VydmVyIFBvcnQgICAgICAgOiA5OTUN
ClNlY3VyZWQgICAgICAgICAgIDogTm8NClR5cGUgICAgICAgICAgICAgIDogUE9QMw0KVXNl
ciAgICAgICAgICAgICAgOiByb21hbi5tY2d1aXJlDQpQYXNzd29yZCAgICAgICAgICA6IFBA
c3N3MHJkJA0KUHJvZmlsZSAgICAgICAgICAgOiBPdXRsb29rDQpQYXNzd29yZCBTdHJlbmd0
aCA6IFZlcnkgU3Ryb25nDQpTTVRQIFNlcnZlciAgICAgICA6IHNtdHAucGl6emFqdWtlYm94
LmNvbQ0KU01UUCBTZXJ2ZXIgUG9ydCAgOiA1ODcNCj09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PT09DQoNCg==
```

2161 30

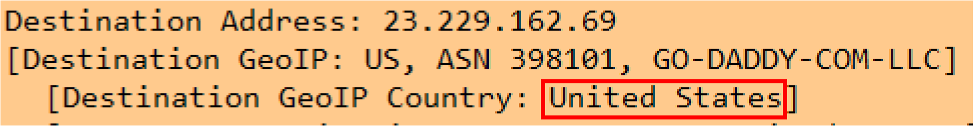
```
HawkEye Keylogger - Reborn v9
Passwords Logs
roman.mcguire \ BEIJING-5CD1-PC

==================================================
URL               : https://login.aol.com/account/challenge/password
```

The decoded subject is also as follows:



```
HawkEye Keylogger - Reborn v9 - Passwords Logs - roman.mcguire \ BEIJING-5CD1-PC - 173.66.146.112
```

If you take a look at the GeoIP information, we can see that this IP geolocates to the United States:



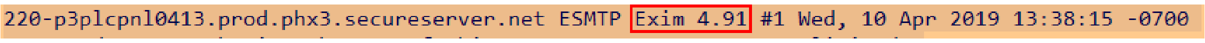
```
Destination Address: 23.229.162.69
[Destination GeoIP: US, ASN 398101, GO-DADDY-COM-LLC]
  [Destination GeoIP Country: United States]
```

This also shows that this IP is associated with GoDaddy.com.

Answer: United States

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

If you follow the TCP traffic like done previously, we can see in the server's response that it is running Exim 4.91:

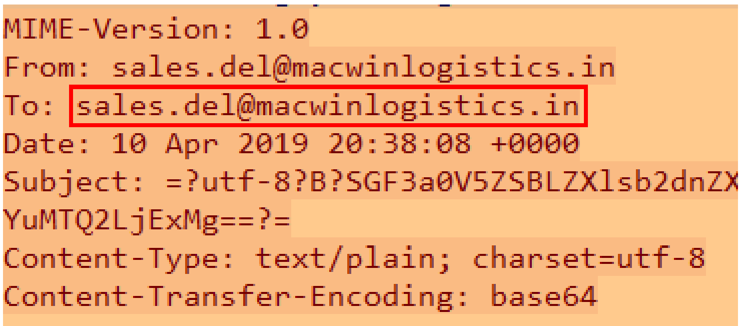


```
220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
```

Answer: Exim 4.91

**To which email account is the stolen information sent?**

As mentioned previously, the email header shows that the to address is sales.del@macwinlogistics.in:

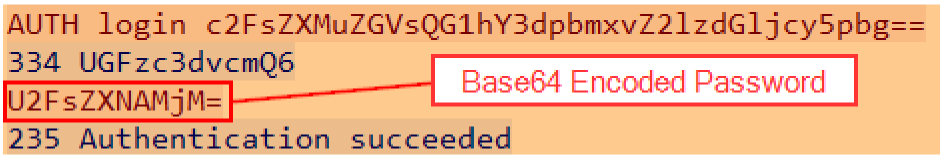


```
MIME-Version: 1.0
From: sales.del@macwinlogistics.in
To: sales.del@macwinlogistics.in
Date: 10 Apr 2019 20:38:08 +0000
Subject: =?utf-8?B?SGF3a0V5ZSBLZXlsb2dnZX
YuMTQ2LjExMg==?=
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
```

Answer: sales.del@macwinlogistics.in

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

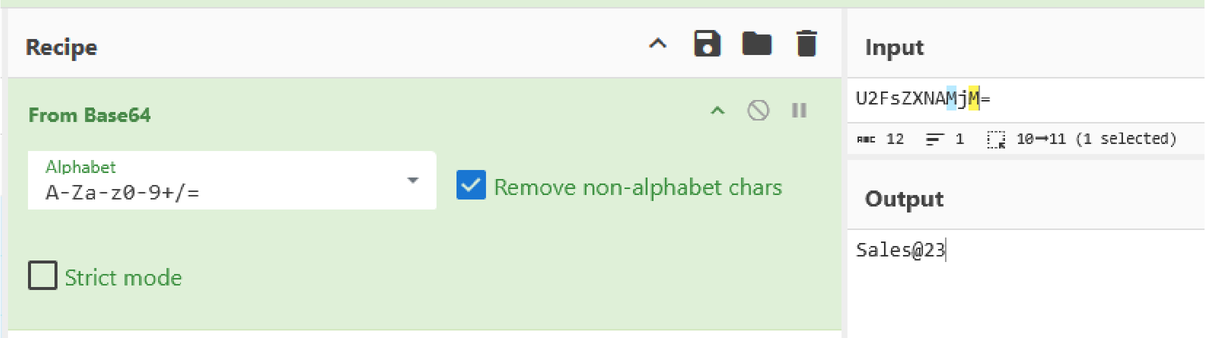
Within the TCP stream, we can see the command AUTH login, where the client sends the username encoded in Base64 followed by the client sending a password after being prompted by the server:



```
AUTH login c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
334 UGFzc3dvcmQ6
U2FsZXNAMjM=
235 Authentication succeeded
```

Base64 Encoded Password

We can use CyberChef to decode this string and find the password:



Alphabet A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

```
U2FsZXNAMjM=
```

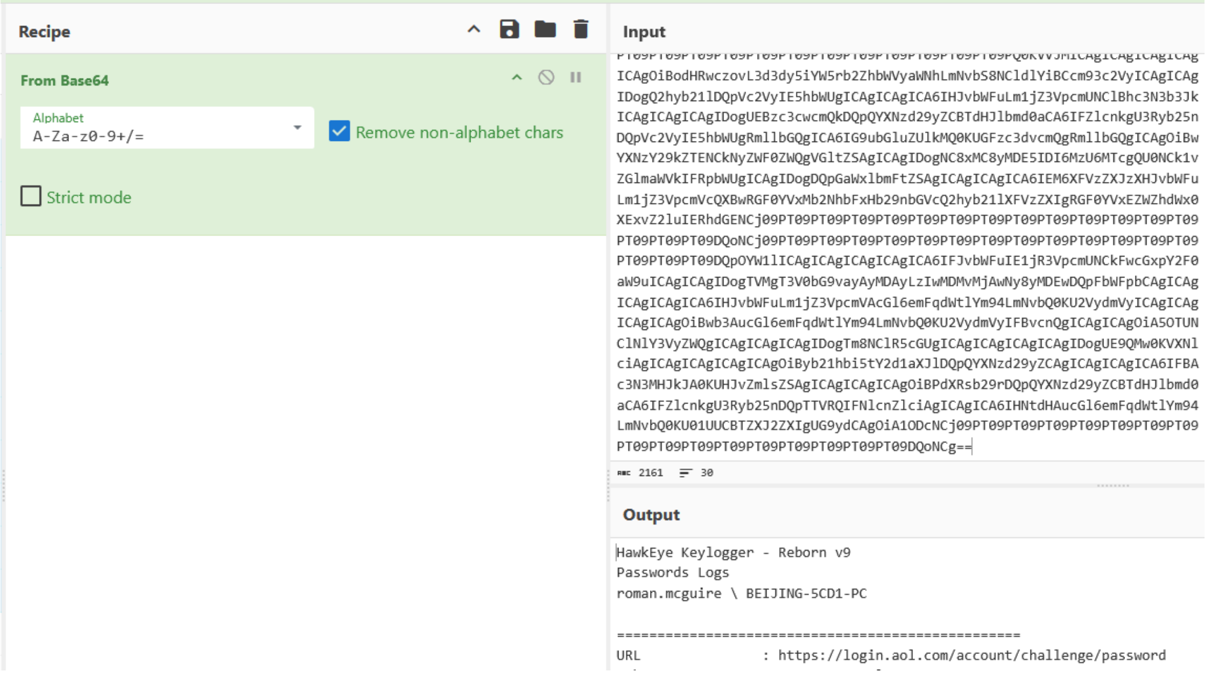
12 1 10→11 (1 selected)

```
Sales@23
```

Answer: Sales@23

### Which malware variant exfiltrated the data?

Within the decoded email body and subject, we can see that the malware variant is Reborn V9.



Alphabet A-Za-z0-9+/=

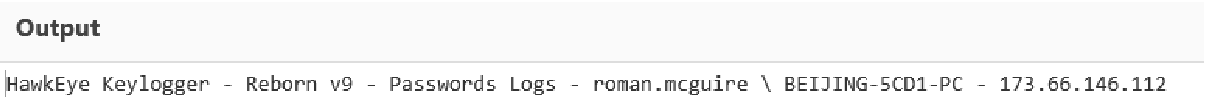
☑ Remove non-alphabet chars

□ Strict mode

```
PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PQ0KVVJMICAgICAgICAgICAg
ICAgOiBodHRwczovL3d3dy5iYW5rb2ZhbWVyaWNhLmNvbS8NCldlYiBCcm93c2VyICAgICAg
IDogQ2hyb21lDQpVc2VyIE5hbWUgICAgICAgICA6IHJvbWFuLm1jZ3VpcmUNClBhc3N3b3Jk
ICAgICAgICAgIDogUEBzc3cwcmQkDQpQYXNzd29yZCBTdHJlbmd0aCA6IFZlcnkgU3Ryb25n
DQpVc2VyIE5hbWUgRmllbGQgICA6IG9ubGluZUlkMQ0KUGFzc3dvcmQgRmllbGQgICAgOiBw
YXNzY29kZTENCkNyZWF0ZWQgVGltZSAgICAgIDogNC8xMC8yMDE5IDI6MzU6MTcgQU0NCk1v
ZGlmaWVkIFRpbWUgICAgIDogDQpGaWxlbmFtZSAgICAgICAgICA6IEM6XFVzZXJzXHJvbWFu
Lm1jZ3VpcmVcQXBwRGF0YVxMb2NhbFxHb29nbGVcQ2hyb21lXFVzZXIgRGF0YVxEZWZhdWx0
XExvZ2luIERhdGENCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09DQpOYW1lICAgICAgICAgICAgICA6IFJvbWFuIE1jR3VpcmUNCkFwcGxpY2F0
aW9uICAgICAgIDogTVMgT3V0bG9vayAyMDAyLzIwMDMvMjAwNy8yMDEwDQpFbWFpbCAgICAg
ICAgICAgICA6IHJvbWFuLm1jZ3VpcmVAcGl6emFqdWtlYm94LmNvbQ0KU2VydmVyICAgICAg
ICAgICAgOiBwb3AucGl6emFqdWtlYm94LmNvbQ0KU2VydmVyIFBvcnQgICAgICAgOiA5OTUN
ClNlY3VyZWQgICAgICAgICAgIDogTm8NClR5cGUgICAgICAgICAgICAgIDogUE9QMw0KVXNl
ciAgICAgICAgICAgICAgOiByb21hbi5tY2d1aXJlDQpQYXNzd29yZCAgICAgICAgICA6IFBA
c3N3MHJkJA0KUHJvZmlsZSAgICAgICAgICAgOiBPdXRsb29rDQpQYXNzd29yZCBTdHJlbmd0
aCA6IFZlcnkgU3Ryb25nDQpTTVRQIFNlcnZlciAgICAgICA6IHNtdHAucGl6emFqdWtlYm94
LmNvbQ0KU01UUCBTZXJ2ZXIgUG9ydCAgOiA1ODcNCj09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09DQoNCg==
```

2161 30

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

==================================================
URL              : https://login.aol.com/account/challenge/password
```

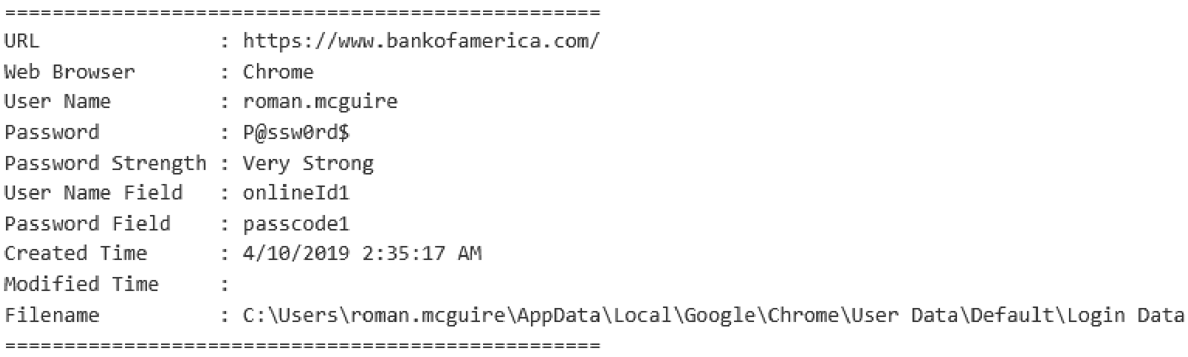


```
HawkEye Keylogger - Reborn v9 - Passwords Logs - roman.mcguire \ BEIJING-5CD1-PC - 173.66.146.112
```

Answer: Reborn V9

### What are the bankofamerica access credentials? (username:password)

You can find the credentials in the decoded Base64 email body:



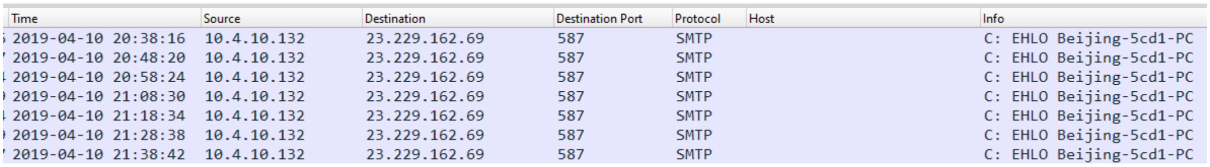
```
==================================================
URL               : https://www.bankofamerica.com/
Web Browser       : Chrome
User Name         : roman.mcguire
Password          : P@ssw0rd$
Password Strength : Very Strong
User Name Field   : onlineId1
Password Field    : passcode1
Created Time      : 4/10/2019 2:35:17 AM
Modified Time     :
Filename          : C:\Users\roman.mcguire\AppData\Local\Google\Chrome\User Data\Default\Login Data
==================================================
```

Answer: roman.mcguire:P@ssw0rd$

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

Using the following filter, we can see that the data is exfiltrated every 10 minutes:

- `(ip.addr==10.4.10.132 ) && ( smtp.req.command == EHLO)`



| Time | Source | Destination | Destination Port | Protocol | Host | Info |
|---|---|---|---|---|---|---|
| 2019-04-10 20:38:16 | 10.4.10.132 | 23.229.162.69 | 587 | SMTP | | C: EHLO Beijing-5cd1-PC |
| 2019-04-10 20:48:20 | 10.4.10.132 | 23.229.162.69 | 587 | SMTP | | C: EHLO Beijing-5cd1-PC |
| 2019-04-10 20:58:24 | 10.4.10.132 | 23.229.162.69 | 587 | SMTP | | C: EHLO Beijing-5cd1-PC |
| 2019-04-10 21:08:30 | 10.4.10.132 | 23.229.162.69 | 587 | SMTP | | C: EHLO Beijing-5cd1-PC |
| 2019-04-10 21:18:34 | 10.4.10.132 | 23.229.162.69 | 587 | SMTP | | C: EHLO Beijing-5cd1-PC |
| 2019-04-10 21:28:38 | 10.4.10.132 | 23.229.162.69 | 587 | SMTP | | C: EHLO Beijing-5cd1-PC |
| 2019-04-10 21:38:42 | 10.4.10.132 | 23.229.162.69 | 587 | SMTP | | C: EHLO Beijing-5cd1-PC |

Answer: 10