Network Forensics Report: Hawkeye Keylogger Exfiltration via SMTP (CyberDefenders Lab)

Executive Summary:

This project involved a full forensic analysis of a suspicious PCAP file from the **CyberDefenders "Hawkeye" challenge**, which simulated a targeted data exfiltration using the **Hawkeye malware family** — a well-known Windows-based keylogger and data stealer. The investigation revealed credential exfiltration via SMTP, host reconnaissance, and attacker behavior across several network layers.

Key findings included:

- Use of the malware to determine public IP via external lookup to `whatismyipaddress.com`
- Exfiltration of sensitive credentials over SMTP using a fake business email
- A complete mapping of compromised systems using Layer 2 MAC address analysis and DNS activity
- Estimation of the full attack duration with accurate timeline correlation using Wireshark timestamps

---

Tools and Techniques Used:

- **Wireshark**: Packet-level investigation, protocol inspection, SMTP decoding, conversation tracking
- **VirusTotal**: Malware behavior verification via hash analysis
- **CyberDefenders Platform**: Incident simulation environment and structured investigation flow
- **OSINT Techniques**: Whois, OUI (MAC Vendor Lookup), DNS & SMTP hostname attribution
- **Base64 Decoding**: Manual decoding of SMTP payloads to retrieve stolen password contents
- **MITRE ATT&CK Mapping** (implicitly): Techniques such as `T1041 - Exfiltration Over Command and Control Channel`, and `T1056 - Input Capture` (Keylogging)

Objective:

To simulate a Tier 1/Tier 2 SOC analyst workflow for detecting, investigating, and reporting a malware-driven data exfiltration campaign using packet capture (PCAP) analysis. The goal was to:

- Identify the malware behavior and source host
- Decode and confirm credential theft
- Trace exfiltration paths
- Map internal and external assets
- Extract Indicators of Compromise (IOCs)
- Produce a timeline and root cause analysis

Investigation Highlights:

Event	Details
Malware Type	Hawkeye keylogger (credential stealer, exfiltrator)
Initial Activity	Host `beijing-d5cd1-pc` queried `whatismyipaddress.com` (20:38:15)
SMTP Exfiltration	Credentials emailed to `sales@dellmacwinlogistics.com`
Credentials Identified	Belonging to "Roman Maguire", exfiltrated twice
Last Known Exfil Activity	21:40:04
Total Compromise Duration	1 hour, 2 minutes, 10 seconds
Internal Hosts Involved	3 total, using 10.x.x.x addressing
Most Active Host (MAC)	`00:80:2f:xx:xx:xx` → HP NIC
NIC Vendor	Hewlett-Packard (Palo Alto, California HQ)
DNS Server IP	Identified via traffic pattern (see detailed logs)

Lab Scenario

An accountant at your organization receives an email referencing an invoice with a download link. Shortly after opening the email, suspicious network traffic is detected.

As a SOC analyst, your task is to investigate the network trace and determine whether data exfiltration occurred.

---

1. Lab Setup

1. Visit **CyberDefenders.org** and create an account (if not already registered).

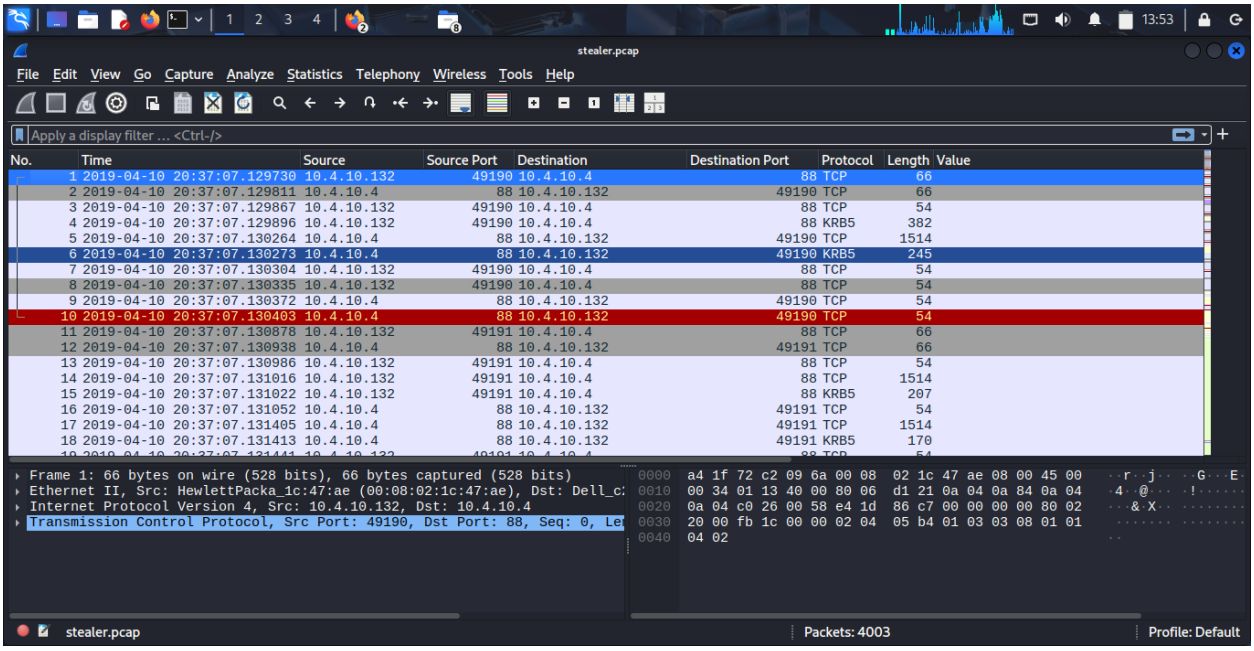
2. Navigate to **BlueYard > Labs > Practice**.
3. Search for the lab titled **"Hawkeye"** and launch it.
4. Accept the platform rules and download the provided lab files.
5. Extract the PCAP file using the password:

   `cyberdefenders.org`

Security Note: Always analyze potentially malicious PCAPs within a virtual machine.

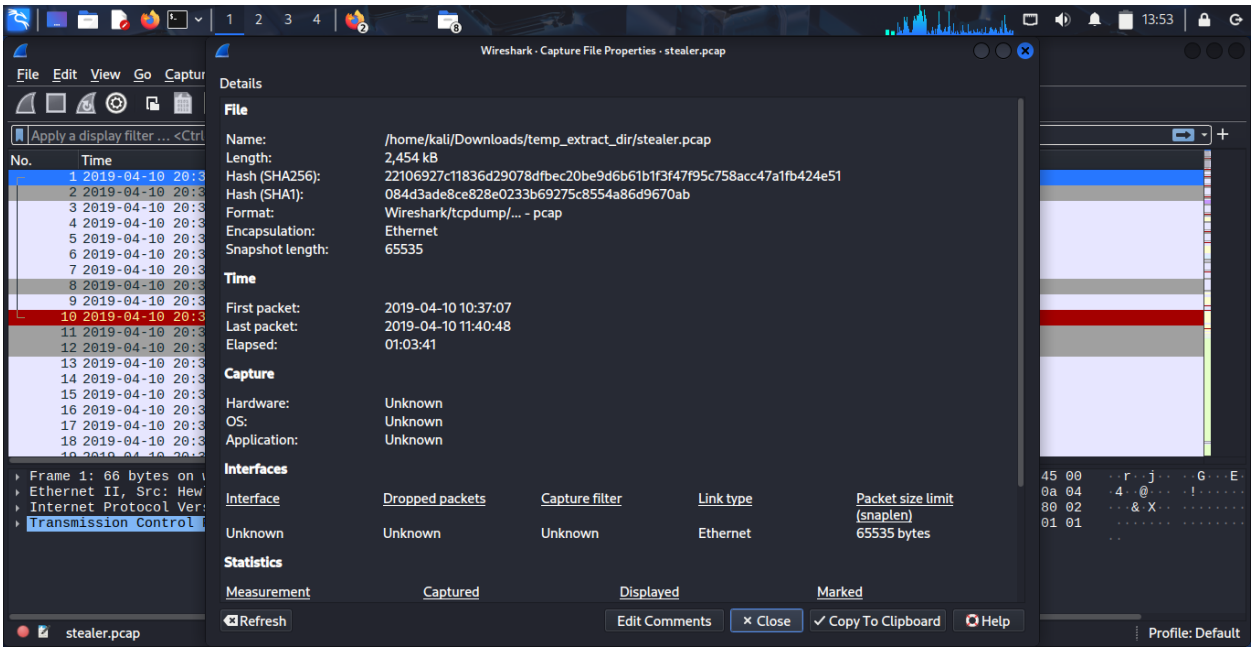
2. Open and Configure Wireshark

Double-click the `.pcap` file to open it in Wireshark. Ensure your Wireshark settings match those from the introductory video for consistency.



3. Initial Analysis: Capture File Properties

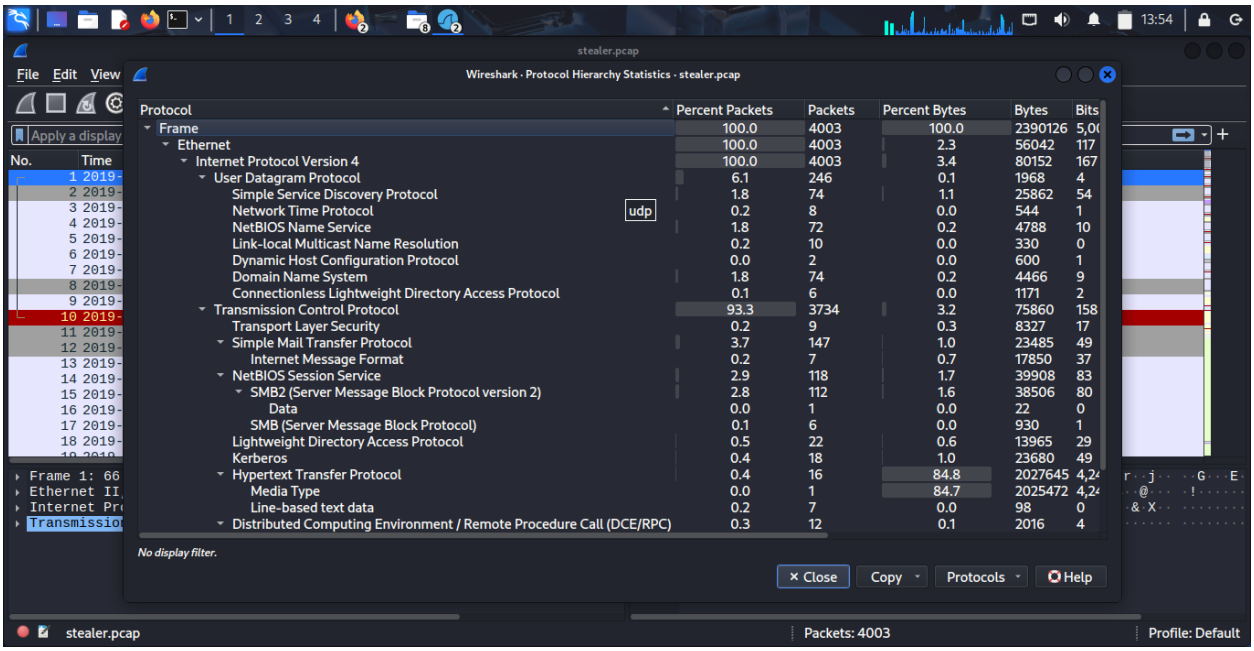
- Navigate to:
  `Statistics > Capture File Properties`
- Duration: The capture spans **~1 hour and 3 minutes**, starting from **April 10, 2019, at 8:37 PM UTC** and ending at **9:40 PM UTC**.



4. Protocol Hierarchy Analysis

- Navigate to:
  `Statistics > Protocol Hierarchy`
- Observed Protocols:
  - **SMB** (Server Message Block)
  - **SMTP** (Simple Mail Transfer Protocol)
  - **Kerberos** (authentication)
  - **HTTP/HTTPS**
  - Others: LDAP, NTP, DNS

Make note of these protocols as they suggest communication types and potential attack vectors.



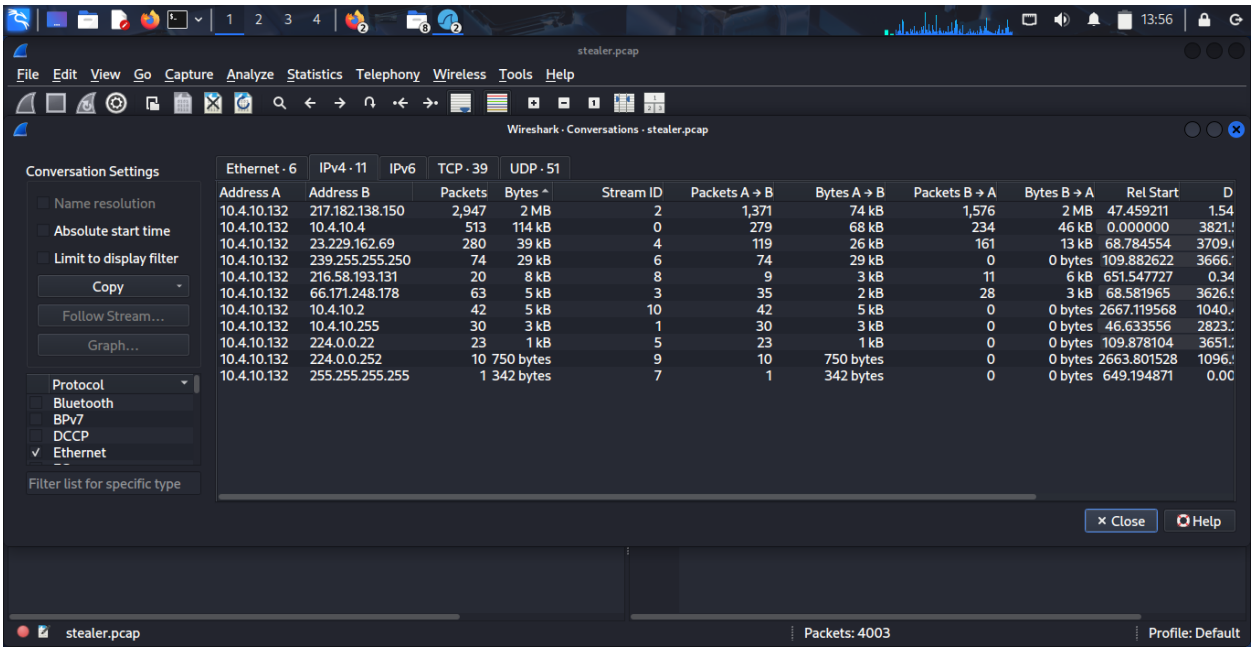
5. Identify Top Talkers (Conversations)

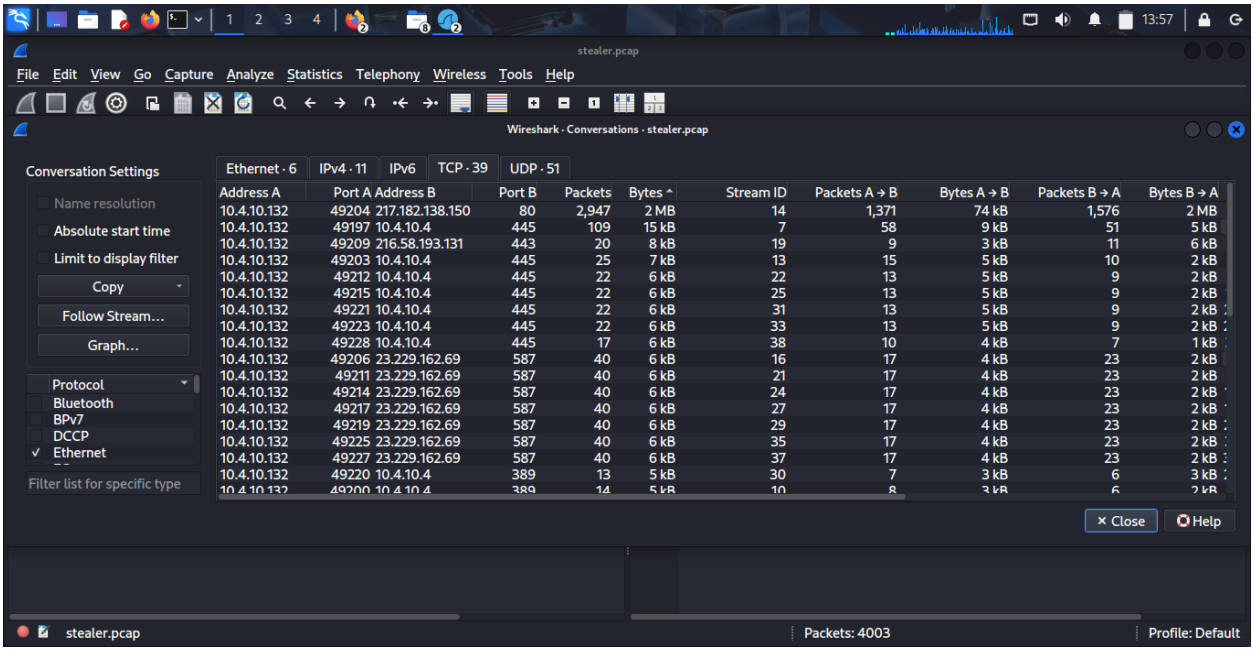
Navigate to:

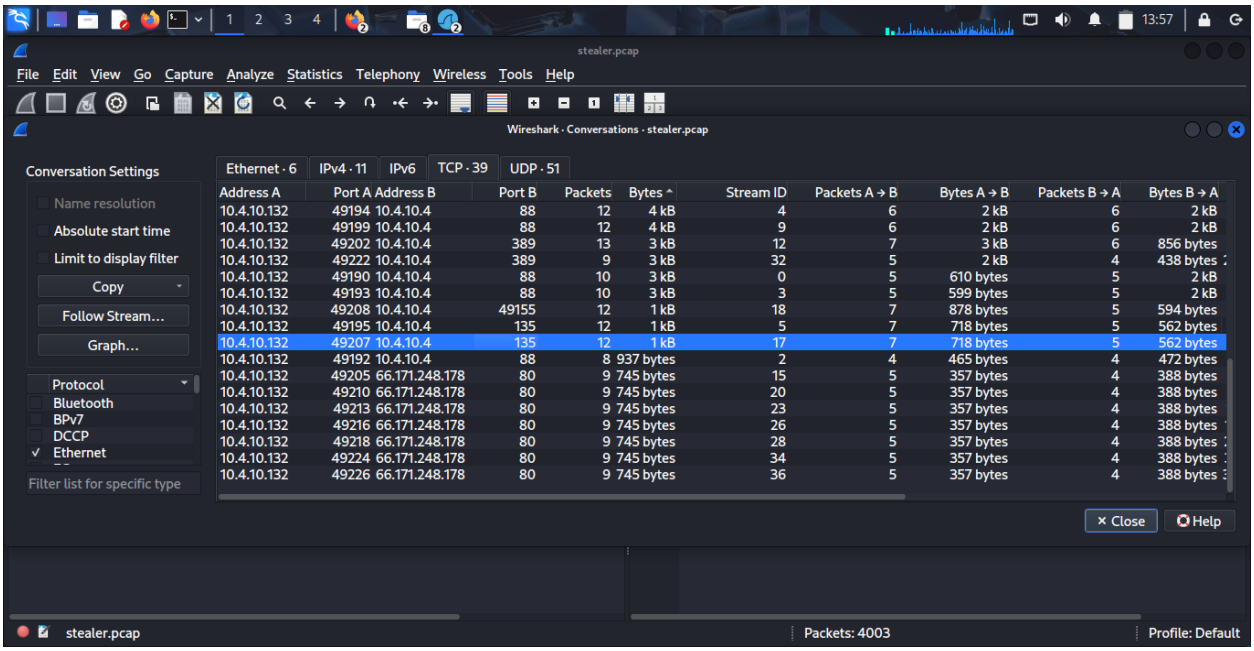
- `Statistics > Conversations > IPv4 Tab`
  Sort by **Bytes** to identify the highest-traffic IP addresses.

Top external IPs of interest:

- `217.11.182.38` (potential C2 or exfiltration destination)
- `104.104.x.x`
- `232.29.162.69` (possible mail server)


13:56
stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · stealer.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream…
Graph…
Protocol
Bluetooth
BPv7
DCCP
Ethernet
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 Rel Start D
10.4.10.132 217.182.138.150 2,947 2 MB 2 1,371 74 kB 1,576 2 MB 47.459211 1.54
10.4.10.132 10.4.10.4 513 114 kB 0 279 68 kB 234 46 kB 0.000000 3821.
10.4.10.132 23.229.162.69 280 39 kB 4 119 26 kB 161 13 kB 68.784554 3709.
10.4.10.132 239.255.255.250 74 29 kB 6 74 29 kB 0 0 bytes 109.882622 3666.
10.4.10.132 216.58.193.131 20 8 kB 8 9 3 kB 11 6 kB 651.547727 0.34
10.4.10.132 66.171.248.178 63 5 kB 3 35 2 kB 28 3 kB 68.581965 3626.
10.4.10.132 10.4.10.2 42 5 kB 10 42 5 kB 0 0 bytes 2667.119568 1040.
10.4.10.132 10.4.10.255 30 3 kB 1 30 3 kB 0 0 bytes 46.633556 2823.
10.4.10.132 224.0.0.22 23 1 kB 5 23 1 kB 0 0 bytes 109.878104 3651.
10.4.10.132 224.0.0.252 10 750 bytes 9 10 750 bytes 0 0 bytes 2663.801528 1096.
10.4.10.132 255.255.255.255 1 342 bytes 7 1 342 bytes 0 0 bytes 649.194871 0.00
× Close
Help
stealer.pcap
Packets: 4003
Profile: Default

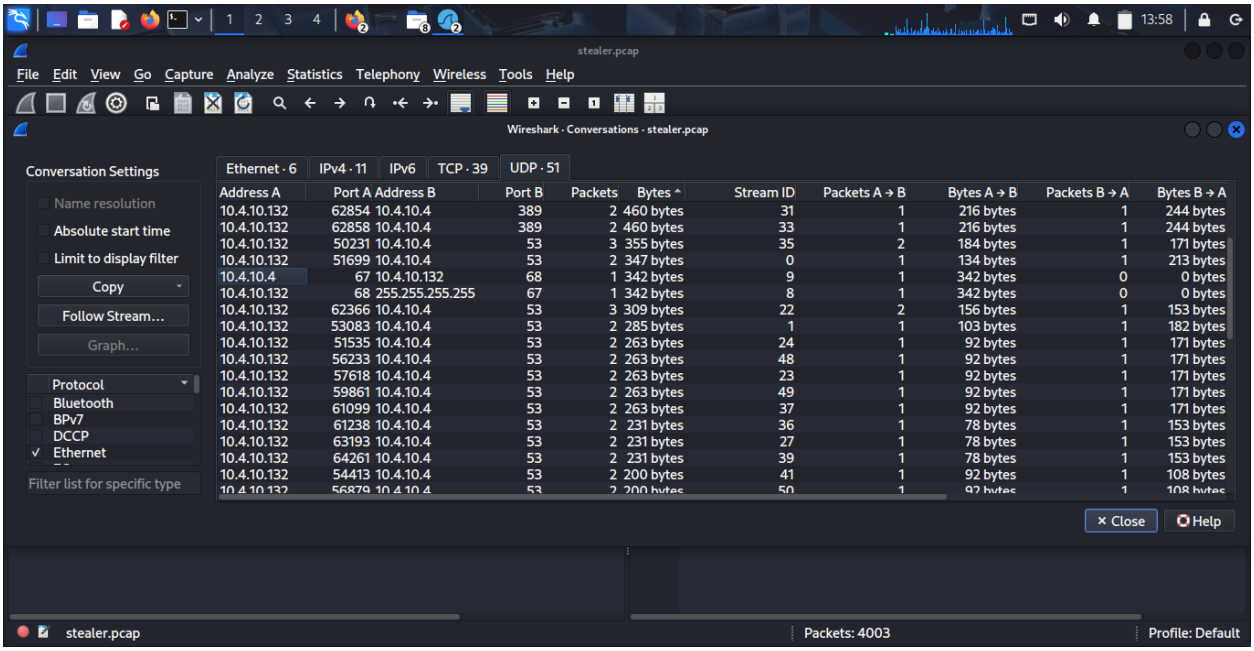

13:57
stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · stealer.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream…
Graph…
Protocol
Bluetooth
BPv7
DCCP
Ethernet
Filter list for specific type
Ethernet · 6
IPv4 · 11
IPv6
TCP · 39
UDP · 51
Address A Port A Address B Port B Packets Bytes Stream ID Packets A → B Bytes A → B Packets B → A Bytes B → A
10.4.10.132 49204 217.182.138.150 80 2,947 2 MB 14 1,371 74 kB 1,576 2 MB
10.4.10.132 49197 10.4.10.4 445 109 15 kB 7 58 9 kB 51 5 kB
10.4.10.132 49209 216.58.193.131 443 20 8 kB 19 9 3 kB 11 6 kB
10.4.10.132 49203 10.4.10.4 445 25 7 kB 13 15 5 kB 10 2 kB
10.4.10.132 49212 10.4.10.4 445 22 6 kB 22 13 5 kB 9 2 kB
10.4.10.132 49215 10.4.10.4 445 22 6 kB 25 13 5 kB 9 2 kB
10.4.10.132 49221 10.4.10.4 445 22 6 kB 31 13 5 kB 9 2 kB
10.4.10.132 49223 10.4.10.4 445 22 6 kB 33 13 5 kB 9 2 kB
10.4.10.132 49228 10.4.10.4 445 17 6 kB 38 10 4 kB 7 1 kB
10.4.10.132 49206 23.229.162.69 587 40 6 kB 16 17 4 kB 23 2 kB
10.4.10.132 49211 23.229.162.69 587 40 6 kB 21 17 4 kB 23 2 kB
10.4.10.132 49214 23.229.162.69 587 40 6 kB 24 17 4 kB 23 2 kB
10.4.10.132 49217 23.229.162.69 587 40 6 kB 27 17 4 kB 23 2 kB
10.4.10.132 49219 23.229.162.69 587 40 6 kB 29 17 4 kB 23 2 kB
10.4.10.132 49225 23.229.162.69 587 40 6 kB 35 17 4 kB 23 2 kB
10.4.10.132 49227 23.229.162.69 587 40 6 kB 37 17 4 kB 23 2 kB
10.4.10.132 49220 10.4.10.4 389 13 5 kB 30 7 3 kB 6 3 kB
× Close
Help
stealer.pcap
Packets: 4003
Profile: Default



6. Analyze TCP Conversations

- Check for common ports:
  - `80` (HTTP)
  - `443` (HTTPS)
  - `445` (SMB)
  - `587` (SMTP)

This reinforces the presence of email and file sharing protocols.



8. Filter and Investigate Suspicious IP

Let's investigate the top external IP:

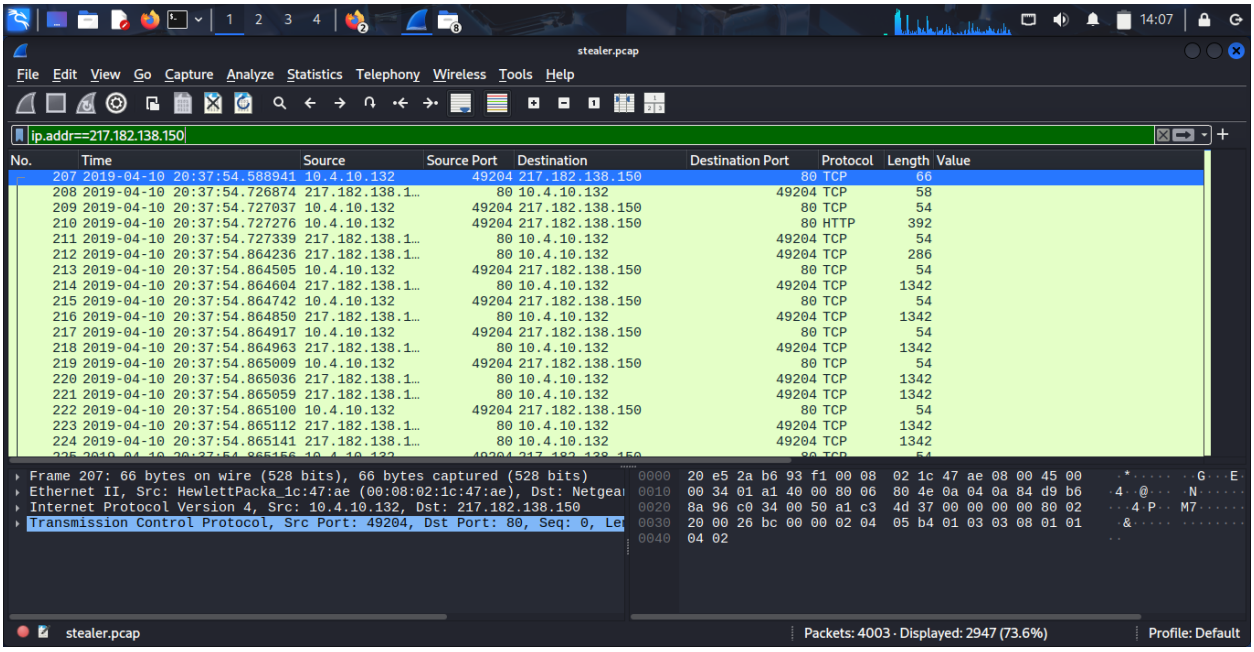
```
wireshark
ip.addr == 217.11.182.38
```

- First appearance: **Packet 210**
- Observed activity: **HTTP GET request**
- Right-click the packet → `Follow > HTTP Stream`

File Download Discovered

- Content-Type: `application/x-msdownload`
- Header: `MZ` (indicates a Windows executable)

This confirms a binary was downloaded from an external IP — possibly malware.



9. Trace Domain Resolution (DNS)

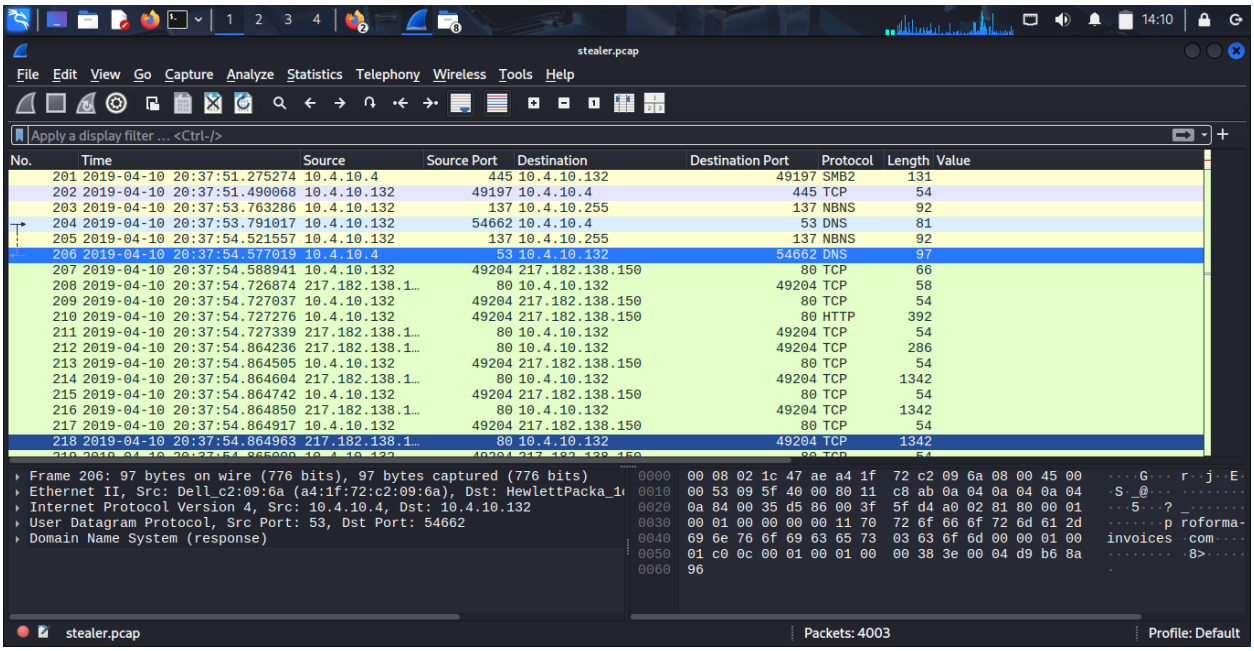
Backtrack to earlier packets (e.g., **packet 206**) to observe:

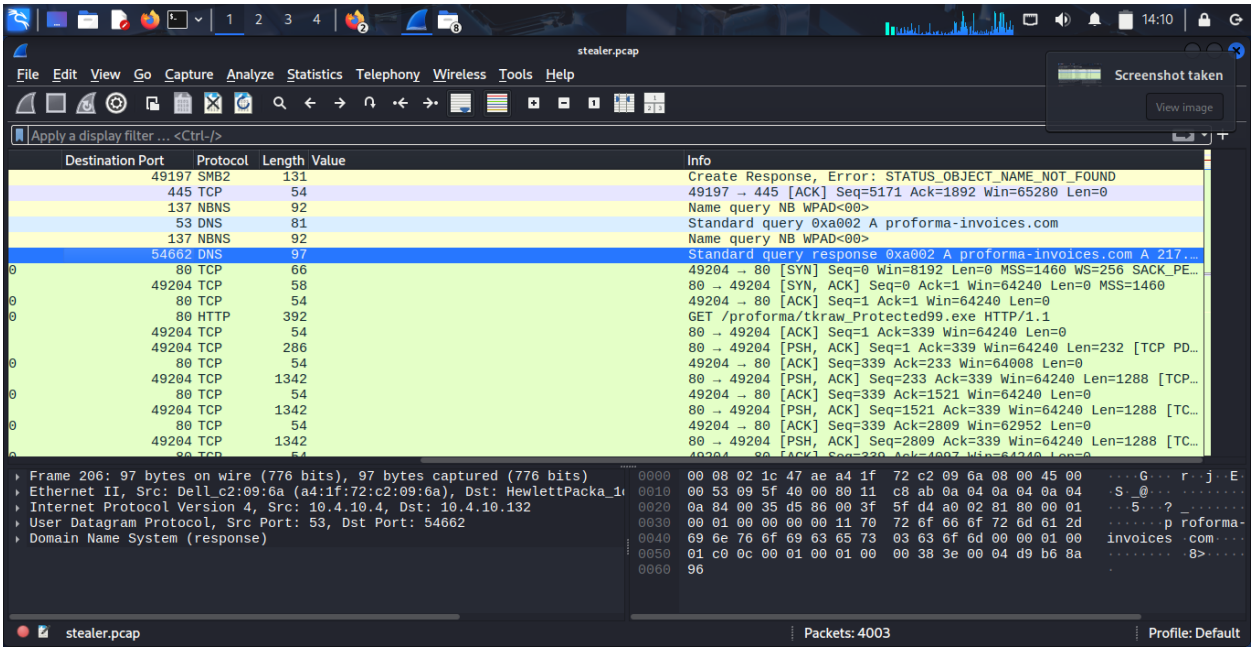
- DNS query/response for:

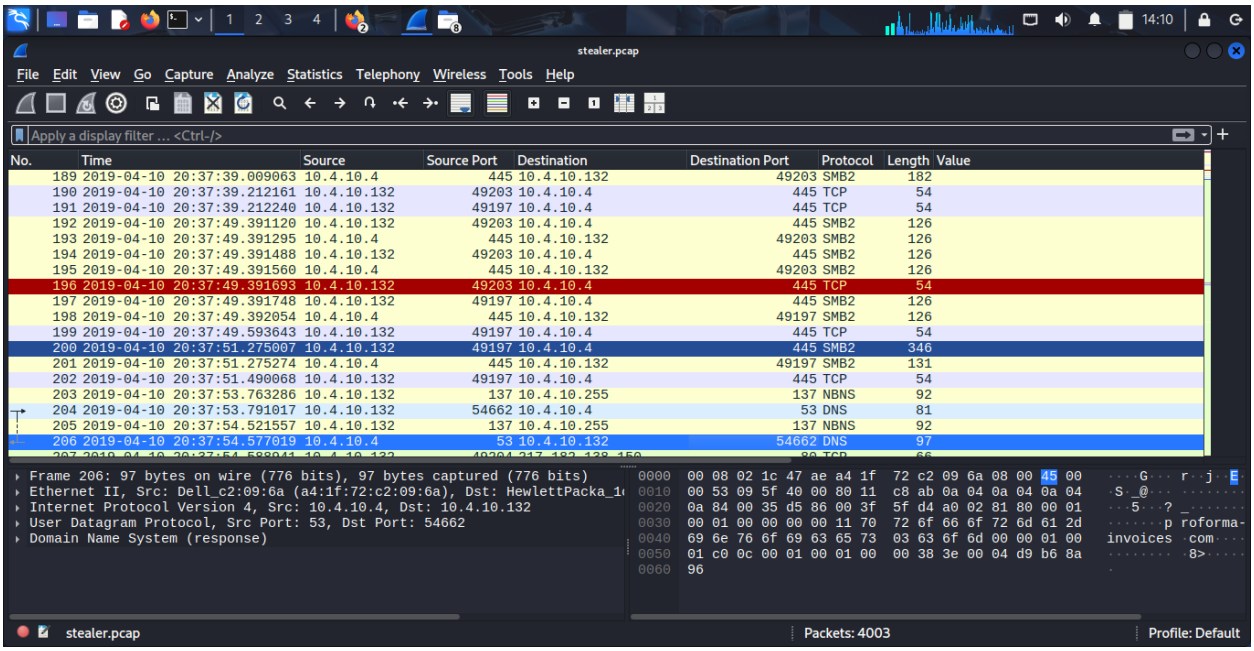
  `pro-invoices.com`

This likely matches the invoice download link mentioned in the scenario. It also reveals the attacker's domain infrastructure.


Wireshark · Follow HTTP Stream (tcp.stream eq 14) · stealer.pcap
GET /proforma/tkraw_Protected99.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: proforma-invoices.com
Connection: Keep-Alive
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
MZ.....@..... .!..L.!This program cannot be run in DOS mode.
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (2,026 kB)
Show as ASCII
No delta times
Stream 14
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Source Port Destination Destination Port Protocol Length Value
201 2019-04-10 20:37:51.275274 10.4.10.4 445 10.4.10.132 49197 SMB2 131
202 2019-04-10 20:37:51.490068 10.4.10.132 49197 10.4.10.4 445 TCP 54
203 2019-04-10 20:37:53.763286 10.4.10.132 137 10.4.10.255 137 NBNS 92
204 2019-04-10 20:37:53.791017 10.4.10.132 54662 10.4.10.4 53 DNS 81
205 2019-04-10 20:37:54.521557 10.4.10.132 137 10.4.10.255 137 NBNS 92
206 2019-04-10 20:37:54.577019 10.4.10.4 53 10.4.10.132 54662 DNS 97
207 2019-04-10 20:37:54.588941 10.4.10.132 49204 217.182.138.150 80 TCP 66
208 2019-04-10 20:37:54.726874 217.182.138.1… 80 10.4.10.132 49204 TCP 58
209 2019-04-10 20:37:54.727037 10.4.10.132 49204 217.182.138.150 80 TCP 54
210 2019-04-10 20:37:54.727276 10.4.10.132 49204 217.182.138.150 80 HTTP 392
211 2019-04-10 20:37:54.727339 217.182.138.1… 80 10.4.10.132 49204 TCP 54
212 2019-04-10 20:37:54.864236 217.182.138.1… 80 10.4.10.132 49204 TCP 286
213 2019-04-10 20:37:54.864505 10.4.10.132 49204 217.182.138.150 80 TCP 54
214 2019-04-10 20:37:54.864604 217.182.138.1… 80 10.4.10.132 49204 TCP 1342
215 2019-04-10 20:37:54.864742 10.4.10.132 49204 217.182.138.150 80 TCP 54
216 2019-04-10 20:37:54.864850 217.182.138.1… 80 10.4.10.132 49204 TCP 1342
217 2019-04-10 20:37:54.864917 10.4.10.132 49204 217.182.138.150 80 TCP 54
218 2019-04-10 20:37:54.864963 217.182.138.1… 80 10.4.10.132 49204 TCP 1342
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_1
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)
0000 00 08 02 1c 47 ae a4 1f 72 c2 09 6a 08 00 45 00
0010 00 53 09 5f 40 00 80 11 c8 ab 0a 04 0a 04 0a 84
0020 00 35 d5 86 00 3f 5f d4 a0 02 81 80 00 01
0030 00 01 00 00 00 00 11 70 72 6f 66 6f 72 6d 61 2d
0040 69 6e 76 6f 69 63 65 73 03 63 6f 6d 00 00 01 00
0050 01 c0 0c 00 01 00 01 00 00 38 3e 00 04 d9 b6 8a
0060 96
stealer.pcap
Packets: 4003
Profile: Default


stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Screenshot taken
View image
Apply a display filter ... <Ctrl-/>
Destination Port Protocol Length Value Info
49197 SMB2 131 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
445 TCP 54 49197 → 445 [ACK] Seq=5171 Ack=1892 Win=65280 Len=0
137 NBNS 92 Name query NB WPAD<00>
53 DNS 81 Standard query 0xa002 A proforma-invoices.com
137 NBNS 92 Name query NB WPAD<00>
54662 DNS 97 Standard query response 0xa002 A proforma-invoices.com A 217…
80 TCP 66 49204 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
49204 TCP 58 80 → 49204 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80 TCP 54 49204 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
80 HTTP 392 GET /proforma/tkraw_Protected99.exe HTTP/1.1
49204 TCP 54 80 → 49204 [ACK] Seq=1 Ack=339 Win=64240 Len=0
49204 TCP 286 80 → 49204 [PSH, ACK] Seq=1 Ack=339 Win=64240 Len=232 [TCP PD…
80 TCP 54 49204 → 80 [ACK] Seq=339 Ack=233 Win=64008 Len=0
49204 TCP 1342 80 → 49204 [PSH, ACK] Seq=233 Ack=339 Win=64240 Len=1288 [TCP…
80 TCP 54 49204 → 80 [ACK] Seq=339 Ack=1521 Win=64240 Len=0
49204 TCP 1342 80 → 49204 [PSH, ACK] Seq=1521 Ack=339 Win=64240 Len=1288 [TC…
80 TCP 54 49204 → 80 [ACK] Seq=339 Ack=2809 Win=62952 Len=0
49204 TCP 1342 80 → 49204 [PSH, ACK] Seq=2809 Ack=339 Win=64240 Len=1288 [TC…
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_1
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)
0000 00 08 02 1c 47 ae a4 1f 72 c2 09 6a 08 00 45 00
0010 00 53 09 5f 40 00 80 11 c8 ab 0a 04 0a 04 0a 84
0020 00 35 d5 86 00 3f 5f d4 a0 02 81 80 00 01
0030 00 01 00 00 00 00 11 70 72 6f 66 6f 72 6d 61 2d
0040 69 6e 76 6f 69 63 65 73 03 63 6f 6d 00 00 01 00
0050 01 c0 0c 00 01 00 01 00 00 38 3e 00 04 d9 b6 8a
0060 96
stealer.pcap
Packets: 4003
Profile: Default



10. Investigate Email Activity (SMTP)

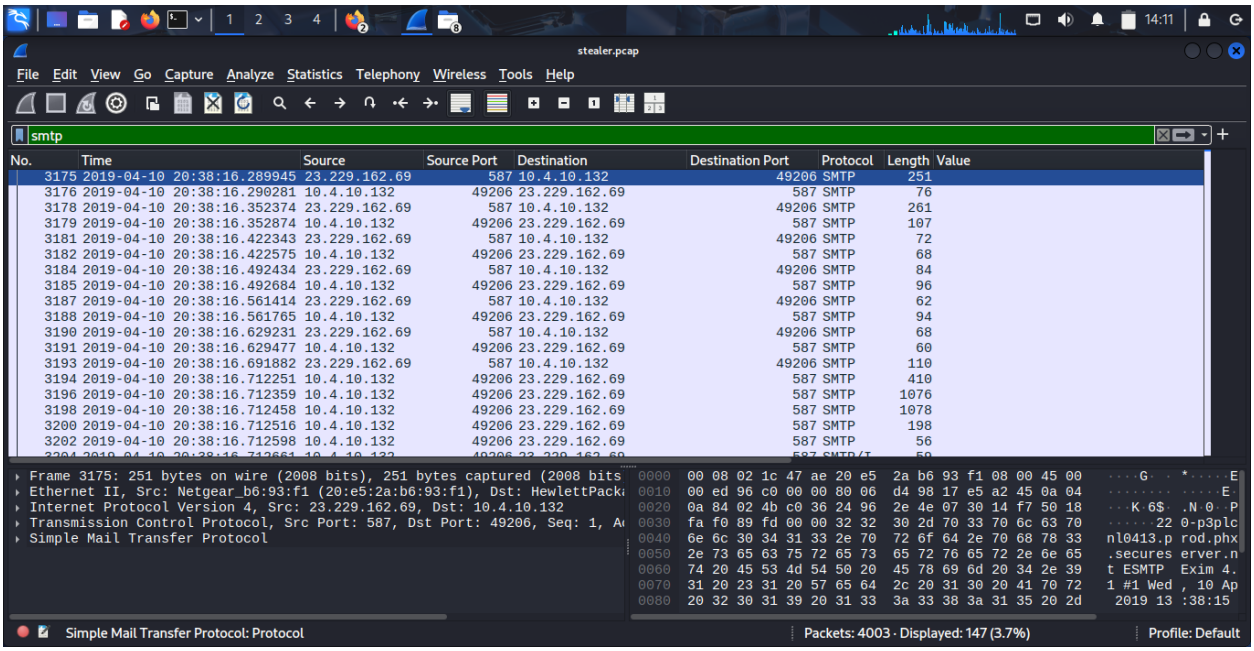
Apply filter:

```
wireshark
smtp
```

- SMTP activity begins around packet **3175**, timestamped **8:38 PM UTC**
- Right-click the first SMTP packet → `Follow > TCP Stream`

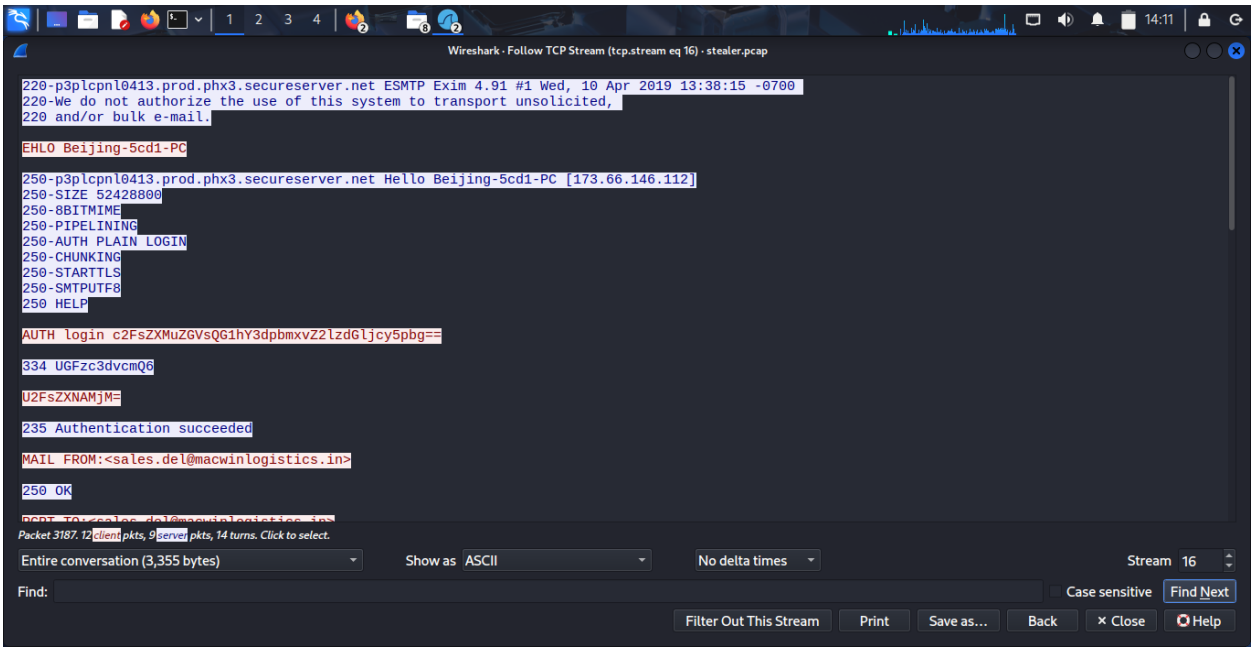
Observations:

- Mail server hostname: `secure-server.net`
- SMTP software version: `Exim 4.91`
- Client hostname: `Beijing-5C-D1-DPC`
- Public IP: `173.66.1.146`
- SMTP Authentication observed (likely Base64-encoded)



Key Indicators of Compromise (IOCs)

Indicator Type	Value
Suspicious Domain	`pro-invoices.com`
Malicious File Type	`.exe` (`MZ` header)
External IP	`217.11.182.38`
Mail Server	`secure-server.net`
SMTP Port	587
HTTP Port	80
Base64 Credentials	Observed in SMTP

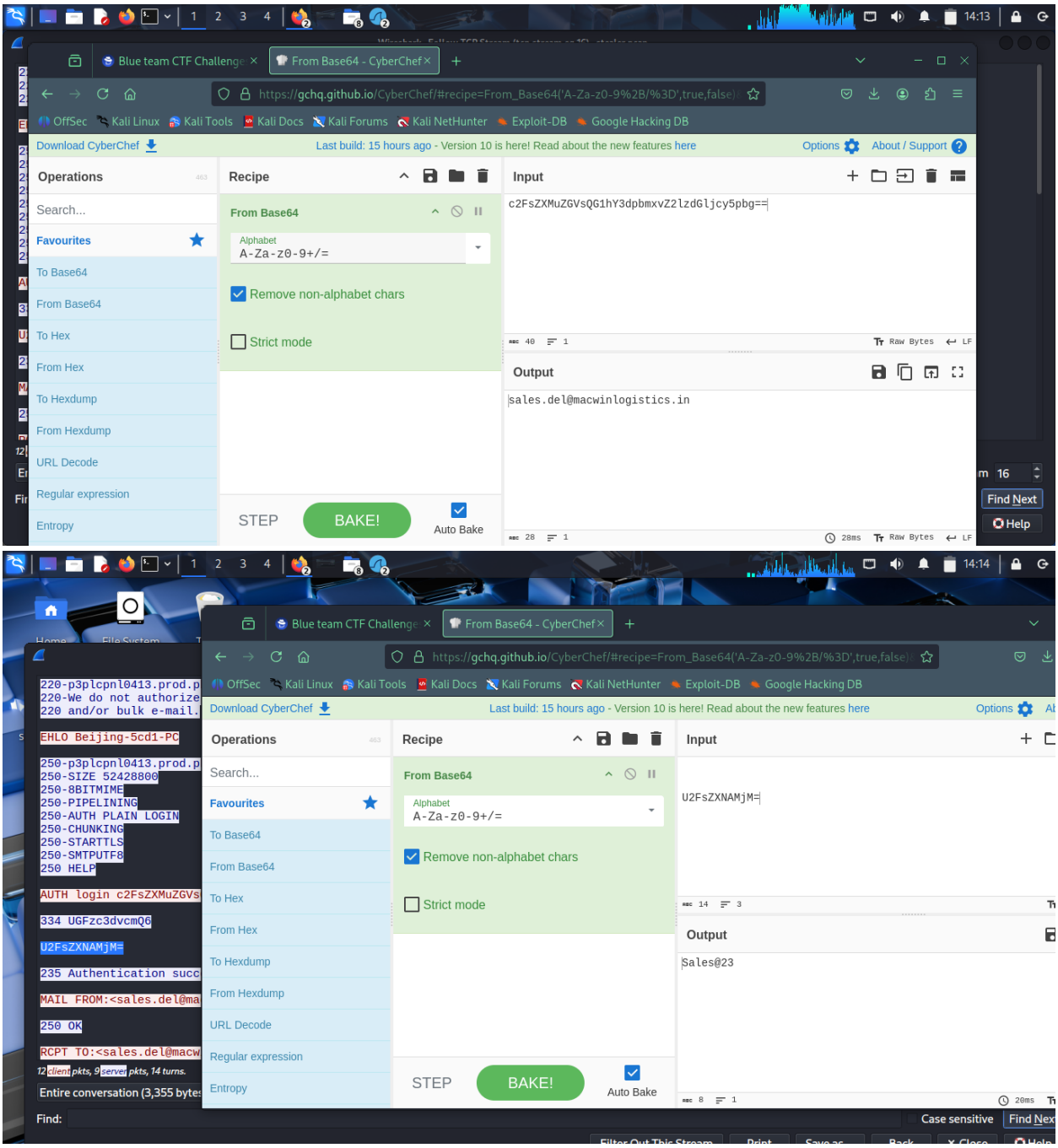


Decoding with CyberChef

Using CyberChef:

- **Username**: `sales.dell@macwinlogistics.com`
- **Password**: `Sales@23`

These credentials were likely used by the attacker to authenticate and send exfiltrated data via SMTP.

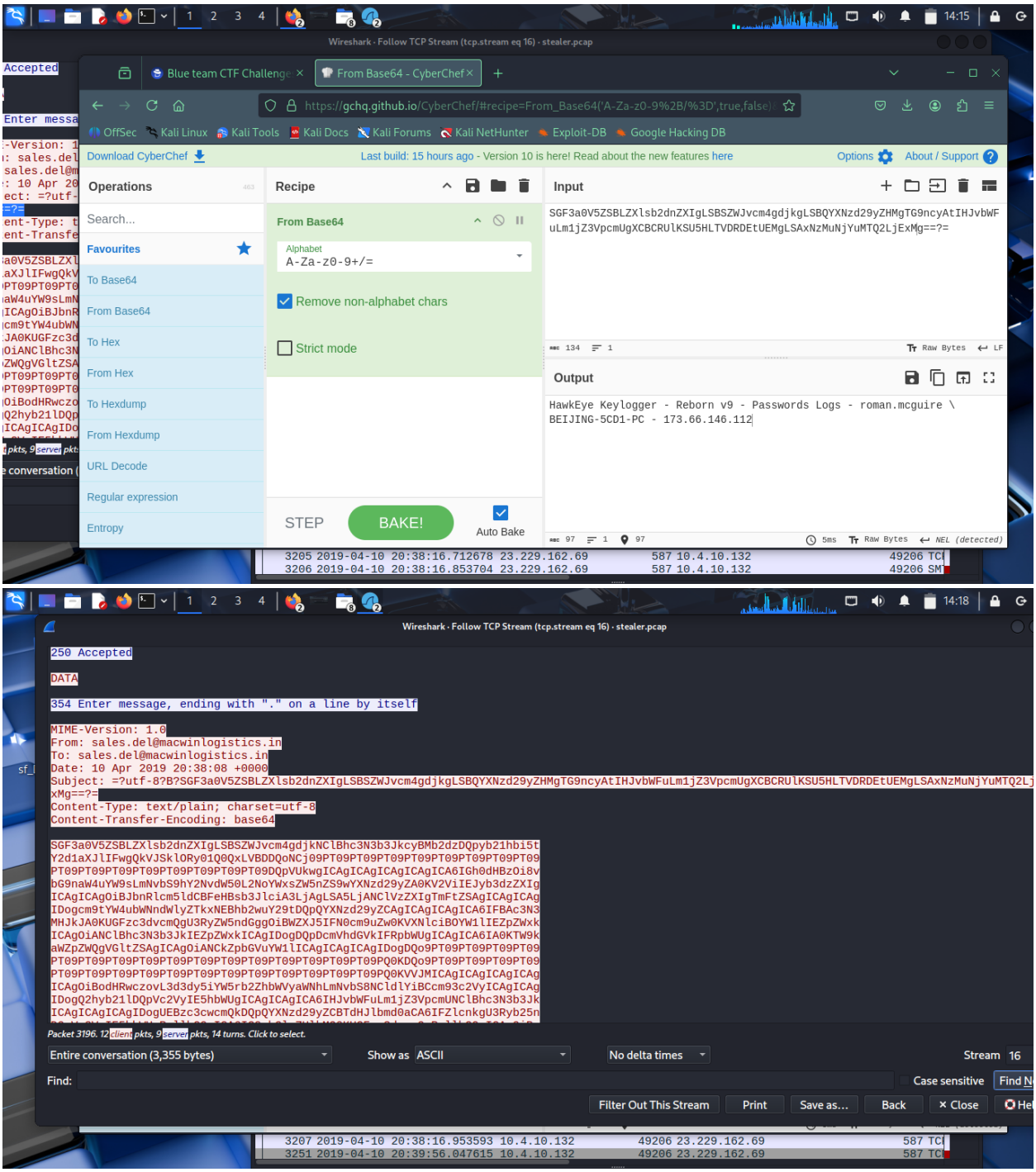


Decoding the Email Subject Line

The subject line was also Base64-encoded. After decoding in CyberChef, it read:

```
mathematica
Hawkeye Keylogger D Reborn V9 - Password Logs
```

This strongly indicates the use of **Hawkeye**, a commodity malware family known for credential theft and keylogging.



. Decoding the Exfiltrated Email Content

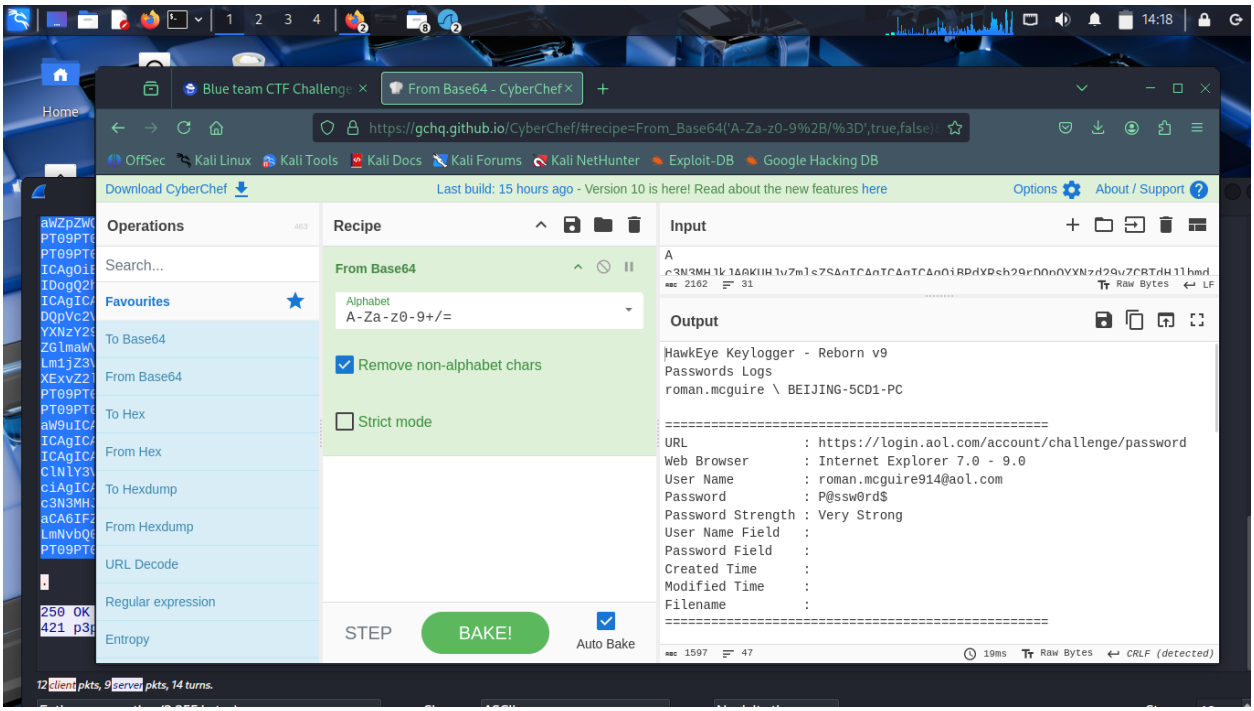
The SMTP body contained another Base64-encoded payload. Decoding revealed multiple stolen credentials:

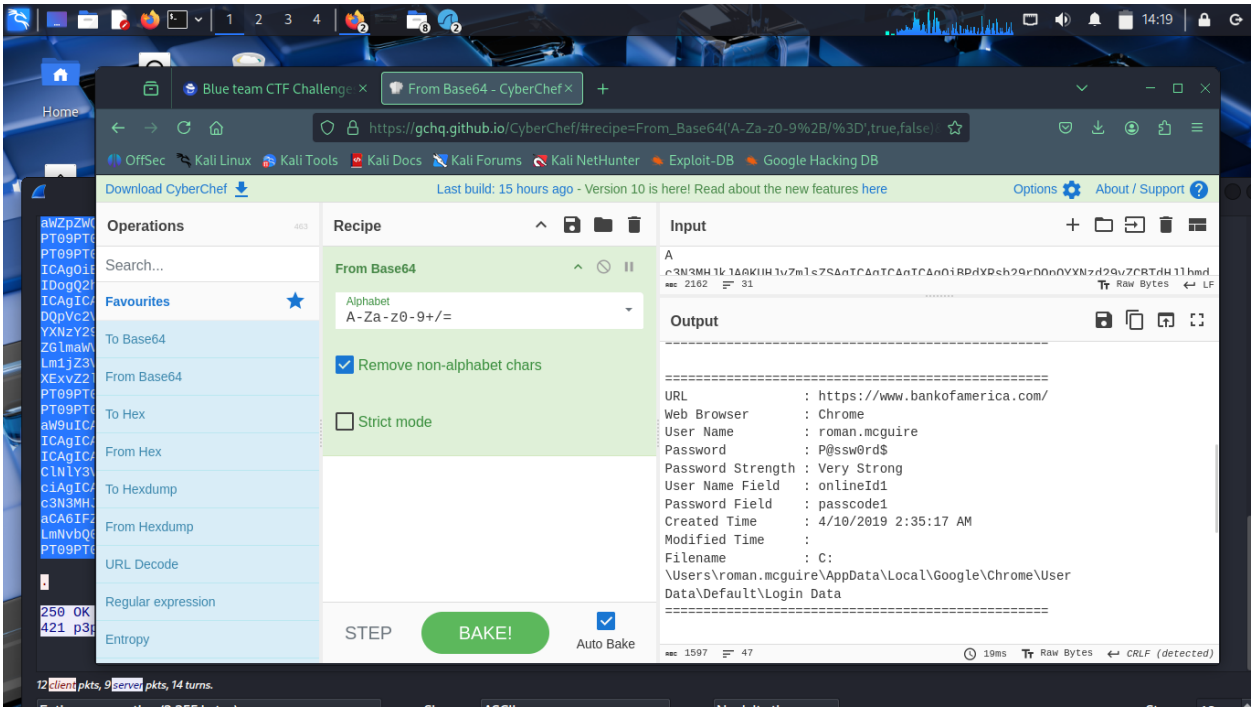
```
plaintext
Username: roman.maguire914@aol.com
```

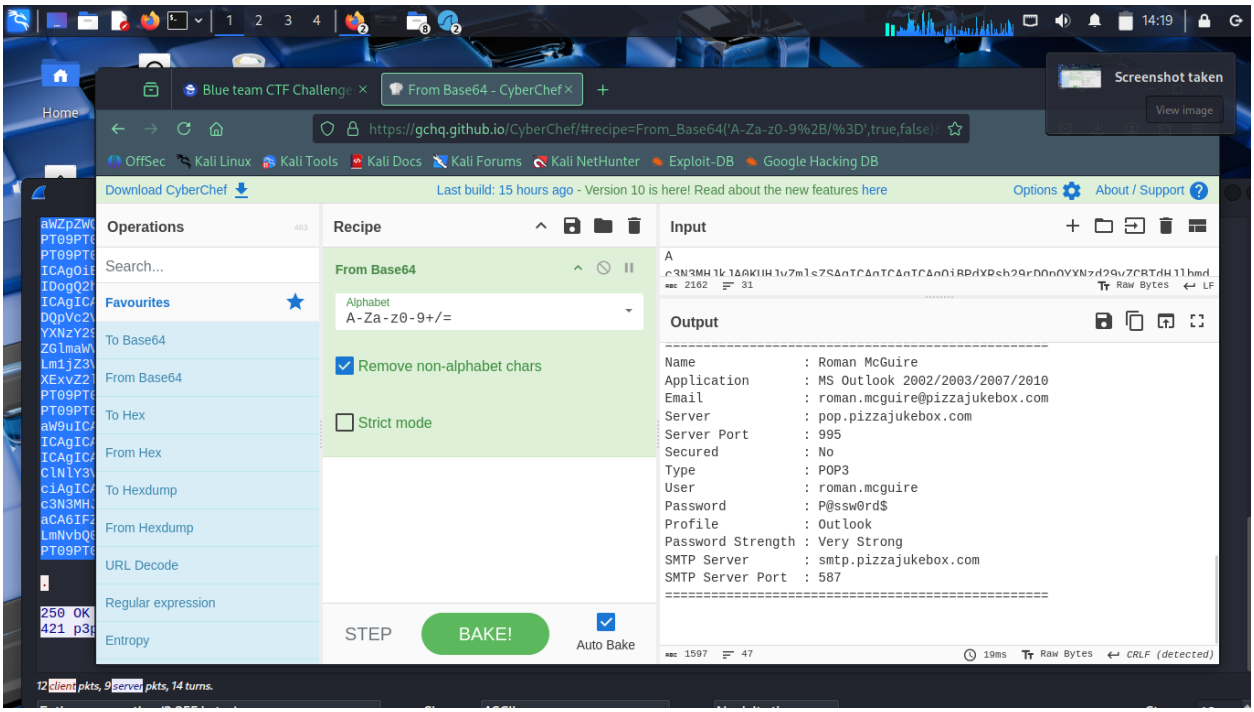
```
Password: p@ssw0rd$
Service: Bank of America

Service: Outlook
Service: PizzaJukebox (assumed company)
Password reused across accounts
```

Key Finding:

Passwords were reused across sensitive platforms — a critical operational security failure by the victim.


Blue team CTF Challenge
From Base64 - CyberChef
https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Download CyberChef
Last build: 15 hours ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
A
Raw Bytes
LF
Output
HawkEye Keylogger - Reborn v9
Passwords Logs
roman.mcguire \ BEIJING-5CD1-PC
==========
URL : https://login.aol.com/account/challenge/password
Web Browser : Internet Explorer 7.0 - 9.0
User Name : roman.mcguire914@aol.com
Password : P@ssw0rd$
Password Strength : Very Strong
User Name Field :
Password Field :
Created Time :
Modified Time :
Filename :
==========
19ms
CRLF (detected)

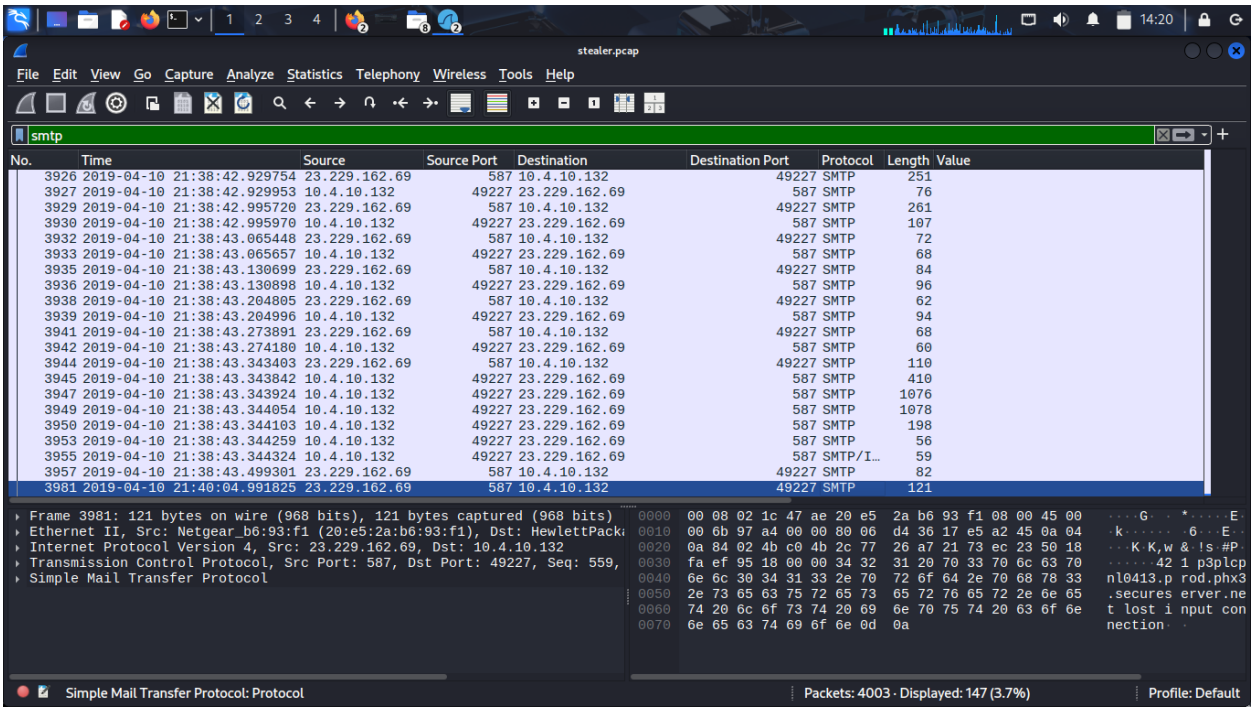

Blue team CTF Challenge
From Base64 - CyberChef
https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Download CyberChef
Last build: 15 hours ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
A
Raw Bytes
LF
Output
==========
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
==========
19ms
CRLF (detected)

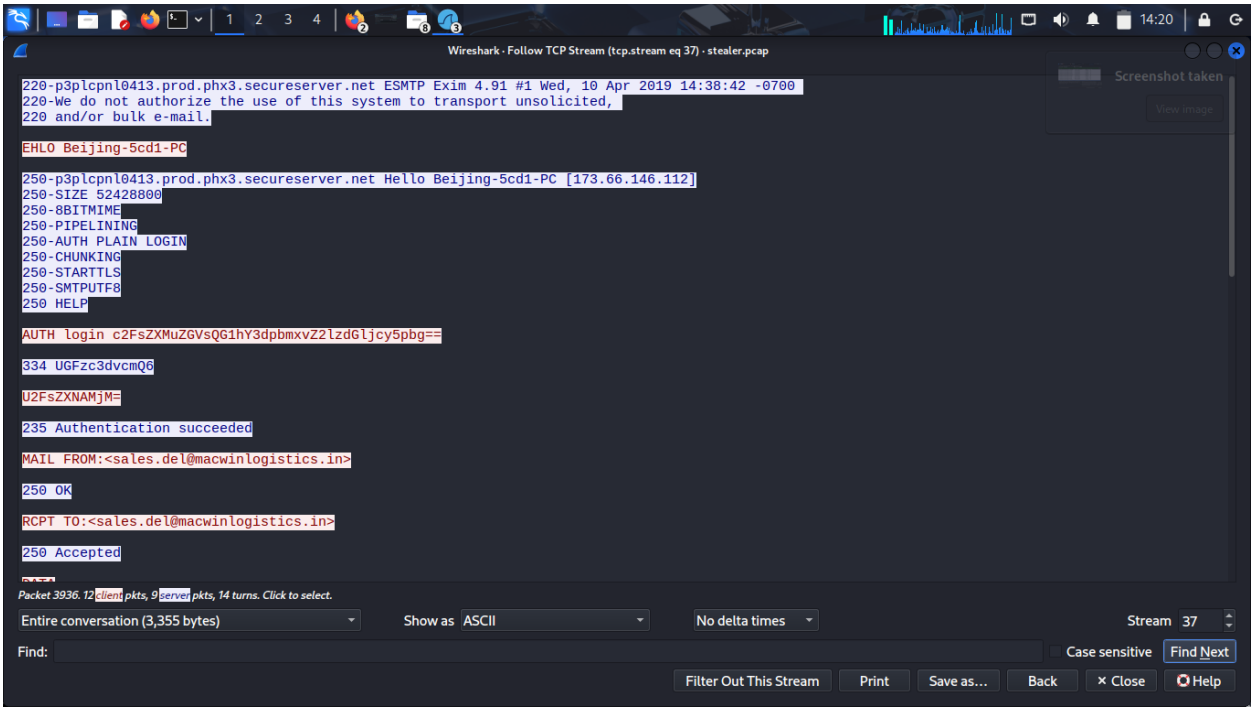


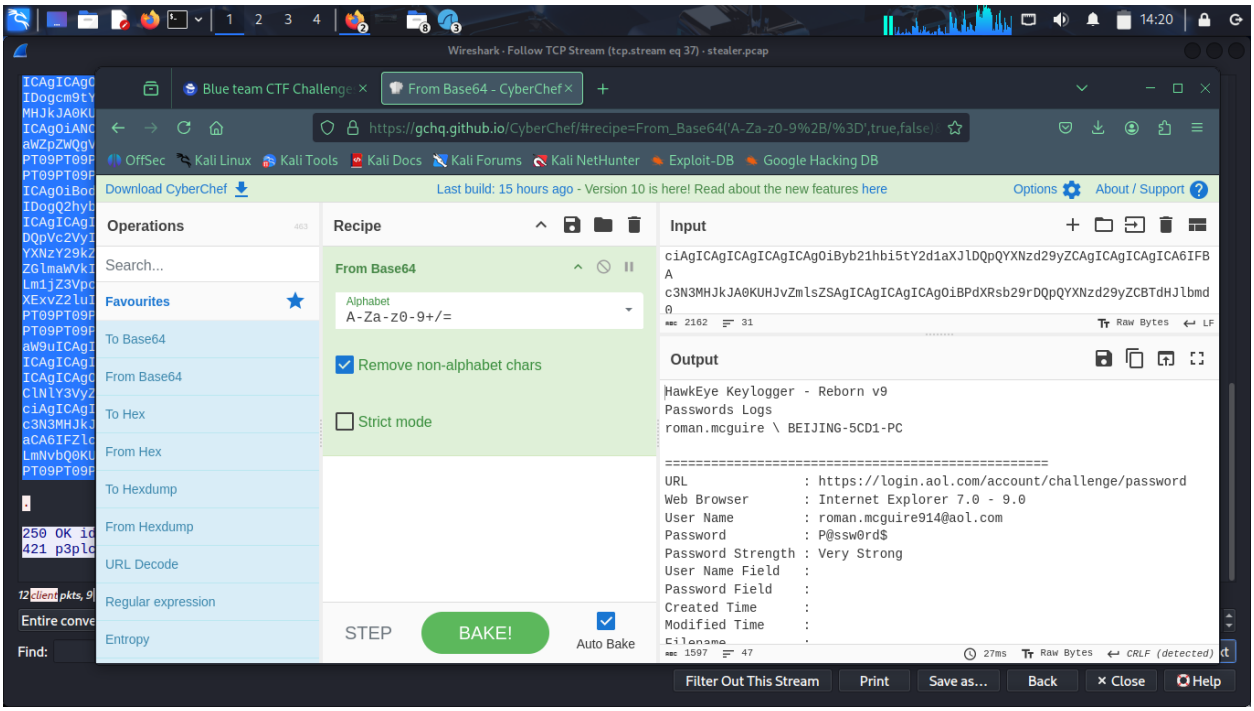
Timeline Reconstruction

- **Initial File Download**: 20:37:54 UTC
- **SMTP Exfiltration End**: 21:40:04 UTC

All events occurred within ~1 hour of the initial infection, showing rapid execution of the malware payload and data exfiltration.


stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
smtp
No. Time Source Source Port Destination Destination Port Protocol Length Value
3926 2019-04-10 21:38:42.929754 23.229.162.69 587 10.4.10.132 49227 SMTP 251
3927 2019-04-10 21:38:42.929953 10.4.10.132 49227 23.229.162.69 587 SMTP 76
3929 2019-04-10 21:38:42.995720 23.229.162.69 587 10.4.10.132 49227 SMTP 261
3930 2019-04-10 21:38:42.995970 10.4.10.132 49227 23.229.162.69 587 SMTP 107
3932 2019-04-10 21:38:43.065448 23.229.162.69 587 10.4.10.132 49227 SMTP 72
3933 2019-04-10 21:38:43.065657 10.4.10.132 49227 23.229.162.69 587 SMTP 68
3935 2019-04-10 21:38:43.130699 23.229.162.69 587 10.4.10.132 49227 SMTP 84
3936 2019-04-10 21:38:43.130898 10.4.10.132 49227 23.229.162.69 587 SMTP 96
3938 2019-04-10 21:38:43.204805 23.229.162.69 587 10.4.10.132 49227 SMTP 62
3939 2019-04-10 21:38:43.204996 10.4.10.132 49227 23.229.162.69 587 SMTP 94
3941 2019-04-10 21:38:43.273891 23.229.162.69 587 10.4.10.132 49227 SMTP 68
3942 2019-04-10 21:38:43.274180 10.4.10.132 49227 23.229.162.69 587 SMTP 60
3944 2019-04-10 21:38:43.343403 23.229.162.69 587 10.4.10.132 49227 SMTP 110
3945 2019-04-10 21:38:43.343842 10.4.10.132 49227 23.229.162.69 587 SMTP 410
3947 2019-04-10 21:38:43.343924 10.4.10.132 49227 23.229.162.69 587 SMTP 1076
3949 2019-04-10 21:38:43.344054 10.4.10.132 49227 23.229.162.69 587 SMTP 1078
3950 2019-04-10 21:38:43.344103 10.4.10.132 49227 23.229.162.69 587 SMTP 198
3953 2019-04-10 21:38:43.344259 10.4.10.132 49227 23.229.162.69 587 SMTP 56
3955 2019-04-10 21:38:43.344324 10.4.10.132 49227 23.229.162.69 587 SMTP/I… 59
3957 2019-04-10 21:38:43.499301 23.229.162.69 587 10.4.10.132 49227 SMTP 82
3981 2019-04-10 21:40:04.991825 23.229.162.69 587 10.4.10.132 49227 SMTP 121
Frame 3981: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPack
Internet Protocol Version 4, Src: 23.229.162.69, Dst: 10.4.10.132
Transmission Control Protocol, Src Port: 587, Dst Port: 49227, Seq: 559,
Simple Mail Transfer Protocol
0000 00 08 02 1c 47 ae 20 e5 2a b6 93 f1 08 00 45 00
0010 00 6b 97 a4 00 00 80 06 d4 36 17 e5 a2 45 0a 04
0020 0a 84 02 4b c0 4b 2c 77 26 a7 21 73 ec 23 50 18
0030 fa ef 95 18 00 00 34 32 31 20 70 33 70 6c 63 70
0040 6e 6c 30 34 31 33 2e 70 72 6f 64 2e 70 68 78 33
0050 2e 73 65 63 75 72 65 73 65 72 76 65 72 2e 6e 65
0060 74 20 6c 6f 73 74 20 69 6e 70 75 74 20 63 6f 6e
0070 6e 65 63 74 69 6f 6e 0d 0a
Simple Mail Transfer Protocol: Protocol
Packets: 4003 · Displayed: 147 (3.7%)
Profile: Default


Wireshark · Follow TCP Stream (tcp.stream eq 37) · stealer.pcap
220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 14:38:42 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO Beijing-5cd1-PC
250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-CHUNKING
250-STARTTLS
250-SMTPUTF8
250 HELP
AUTH login c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
334 UGFzc3dvcmQ6
U2FsZXNAMjM=
235 Authentication succeeded
MAIL FROM:<sales.del@macwinlogistics.in>
250 OK
RCPT TO:<sales.del@macwinlogistics.in>
250 Accepted
Packet 3936. 12 client pkts, 9 server pkts, 14 turns. Click to select.
Entire conversation (3,355 bytes)
Show as ASCII
No delta times
Stream 37
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as…
Back
× Close
Help

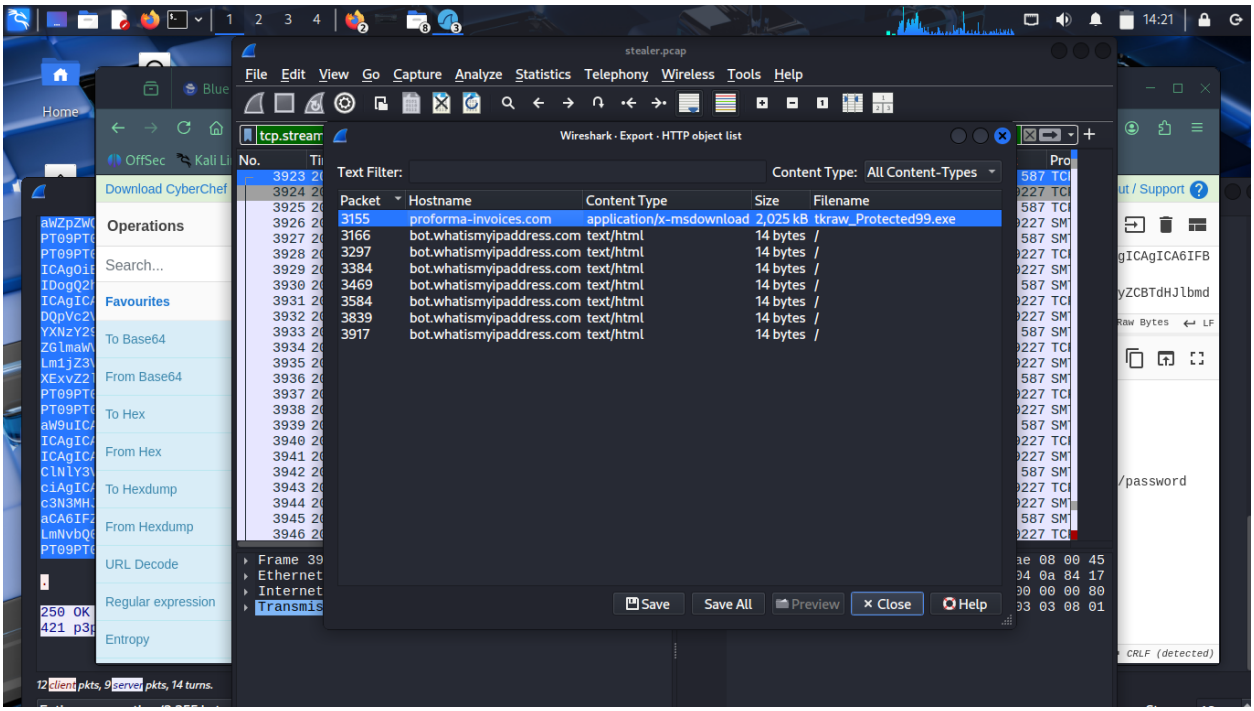


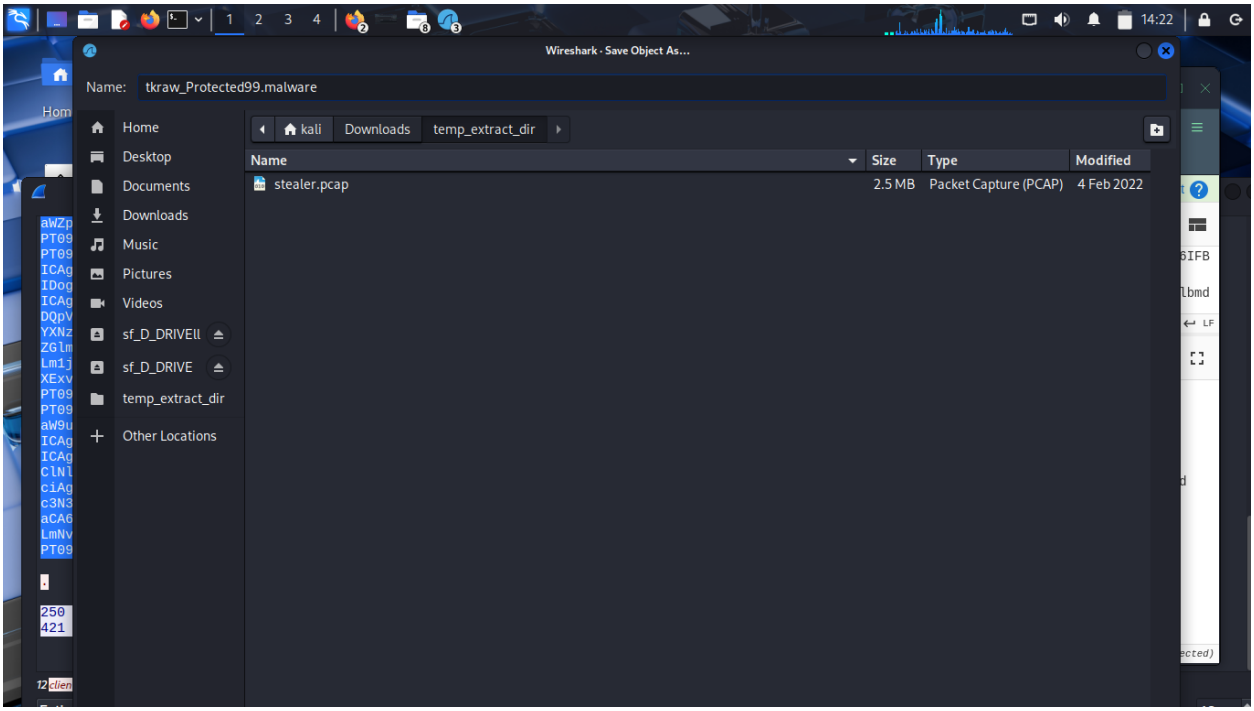
Malware File Extraction

Using `File > Export Objects > HTTP` in Wireshark, we extracted the malicious file:

- **File Name**: `TKraore_protected99.exe`
- **Delivery Domain**: `pro-invoices.com`

Defender was disabled temporarily in a sandboxed VM before export to avoid automatic detection or deletion.





File Hashing & VirusTotal Analysis

Generated hash via PowerShell:

```
powershell
Get-FileHash .\TKraore_protected99.exe -Algorithm SHA256
```

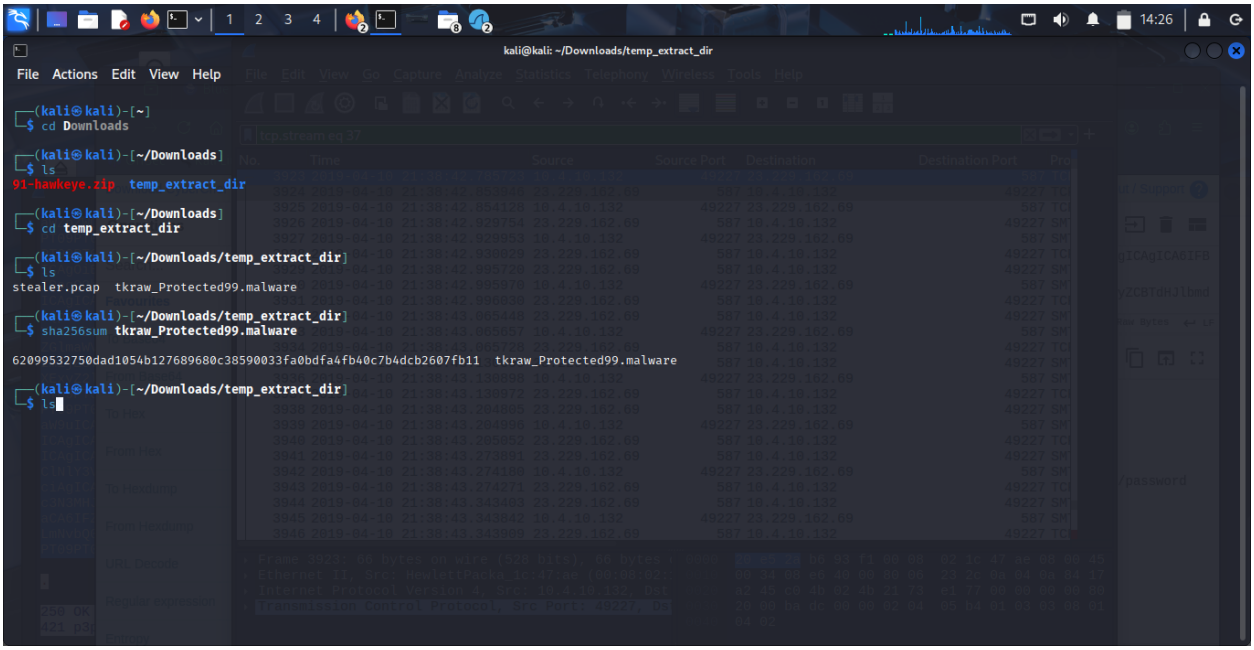
Submitted to VirusTotal:

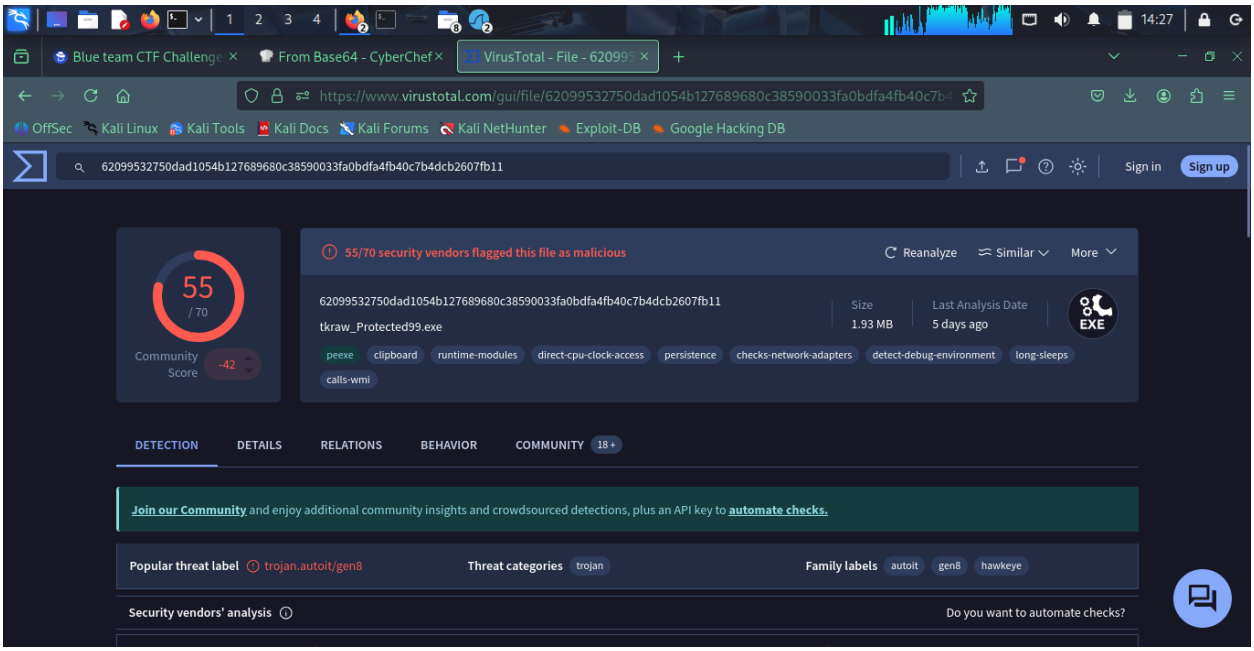
- **SHA256**: `[Redacted for brevity]`
- **Detections**: 57 vendors flagged the file as malicious
- **Label**: `Trojan.Autoit.Gen8` (associated with **Hawkeye** malware)
- **Threat Classification**: Remote Access Trojan (RAT) with keylogging

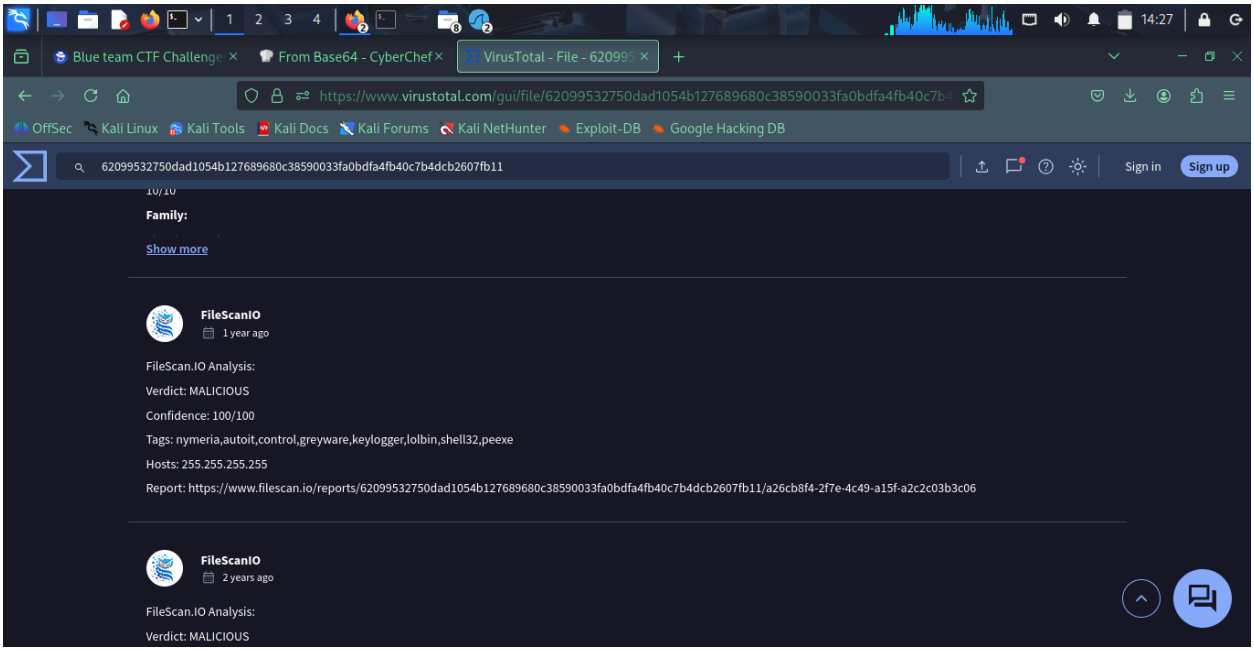
VirusTotal's **Relations** tab confirmed that the binary contacted:

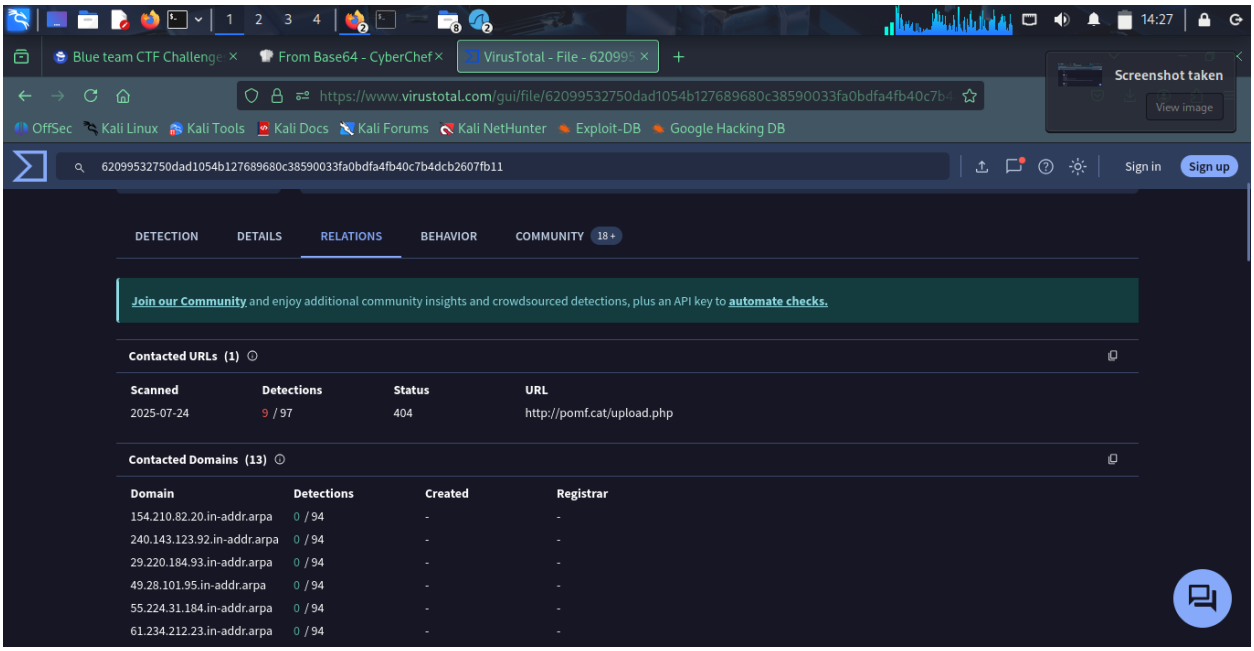
`bot.whatismyipaddress.com`

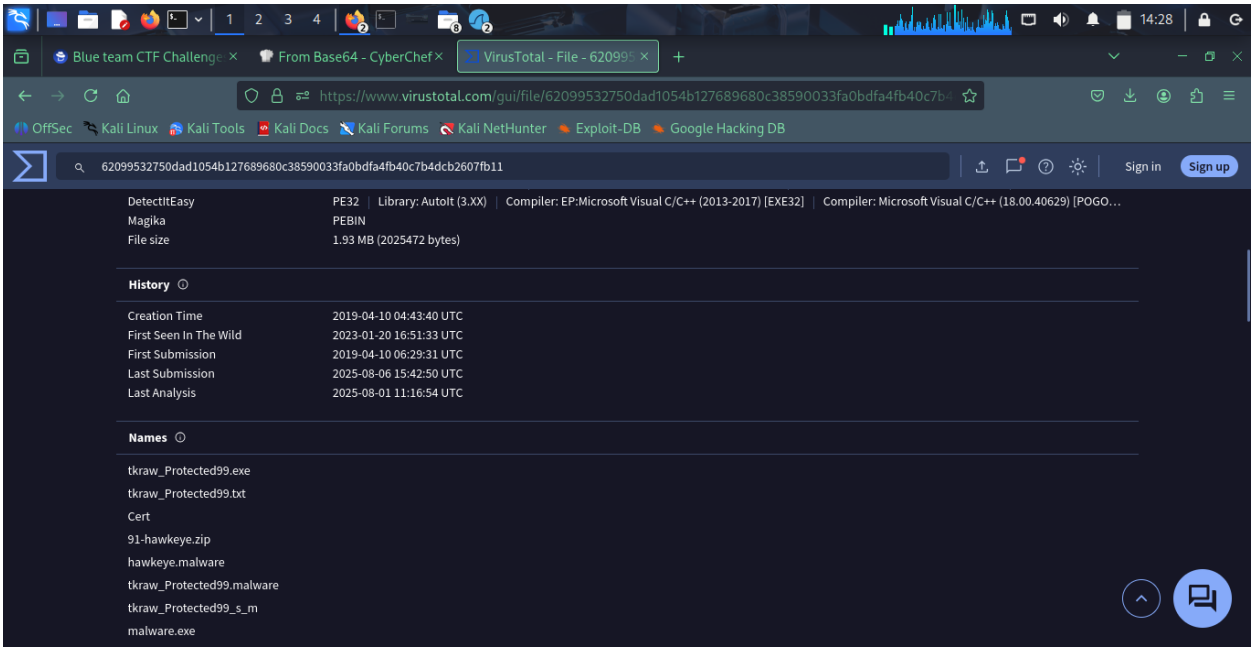
This aligns with the Wireshark findings, suggesting the malware performs periodic external IP checks post-installation.




Blue team CTF Challenge
From Base64 - CyberChef
VirusTotal - File - 620995
https://www.virustotal.com/gui/file/62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11
Sign in
Sign up
55
/ 70
Community Score
-42
55/70 security vendors flagged this file as malicious
Reanalyze
Similar
More
62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11
tkraw_Protected99.exe
Size
1.93 MB
Last Analysis Date
5 days ago
EXE
peexe
clipboard
runtime-modules
direct-cpu-clock-access
persistence
checks-network-adapters
detect-debug-environment
long-sleeps
calls-wmi
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 18+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.autoit/gen8
Threat categories trojan
Family labels autoit gen8 hawkeye
Security vendors' analysis
Do you want to automate checks?


Blue team CTF Challenge
From Base64 - CyberChef
VirusTotal - File - 620995
https://www.virustotal.com/gui/file/62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11
Sign in
Sign up
10/10
Family:
Show more
FileScanIO
1 year ago
FileScan.IO Analysis:
Verdict: MALICIOUS
Confidence: 100/100
Tags: nymeria,autoit,control,greyware,keylogger,lolbin,shell32,peexe
Hosts: 255.255.255.255
Report: https://www.filescan.io/reports/62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11/a26cb8f4-2f7e-4c49-a15f-a2c2c03b3c06
FileScanIO
2 years ago
FileScan.IO Analysis:
Verdict: MALICIOUS





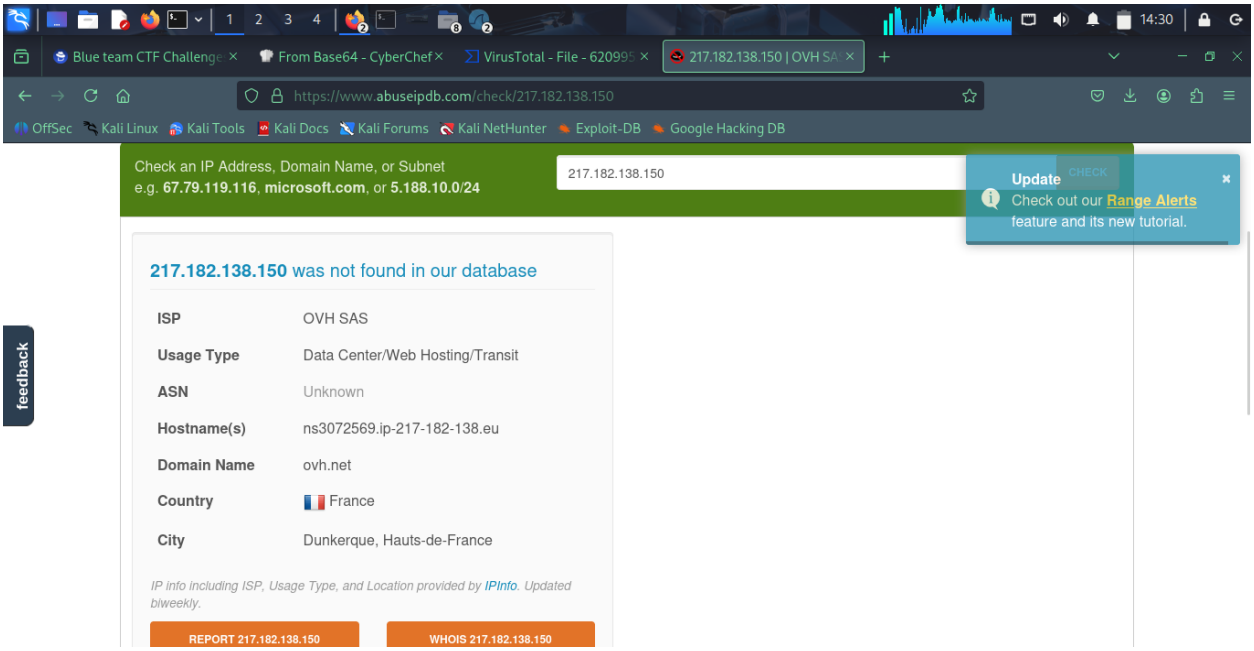
Threat Intelligence (OSINT)

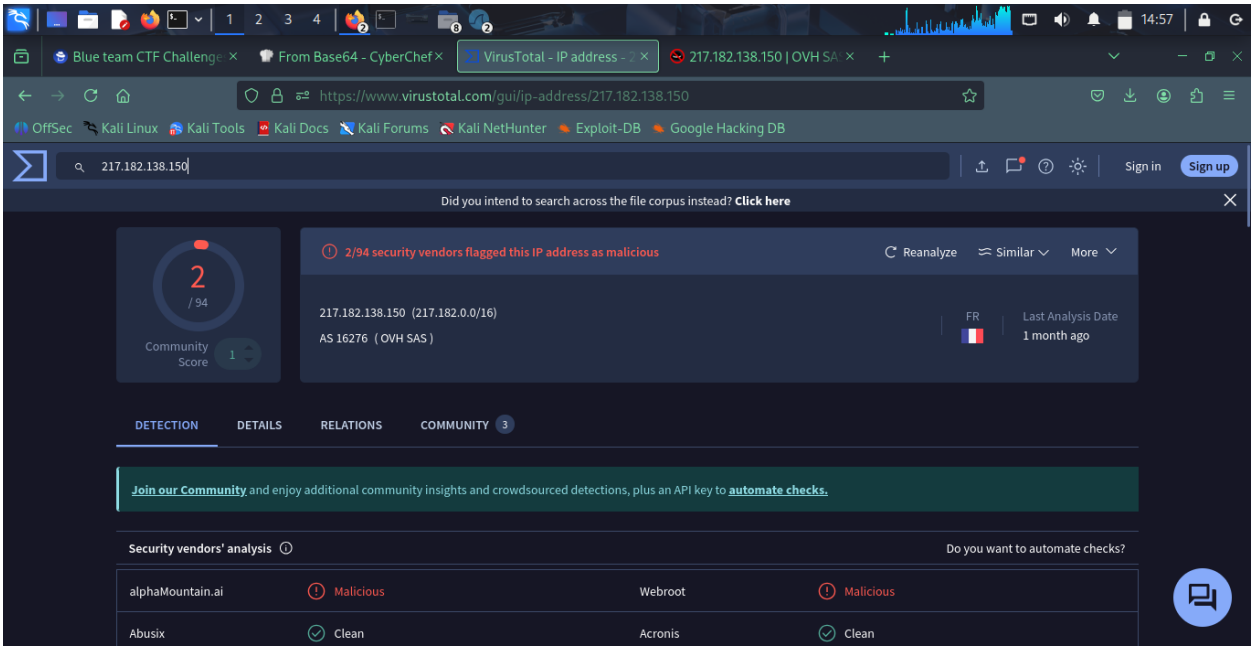
External IP Address: `217.11.182.38`

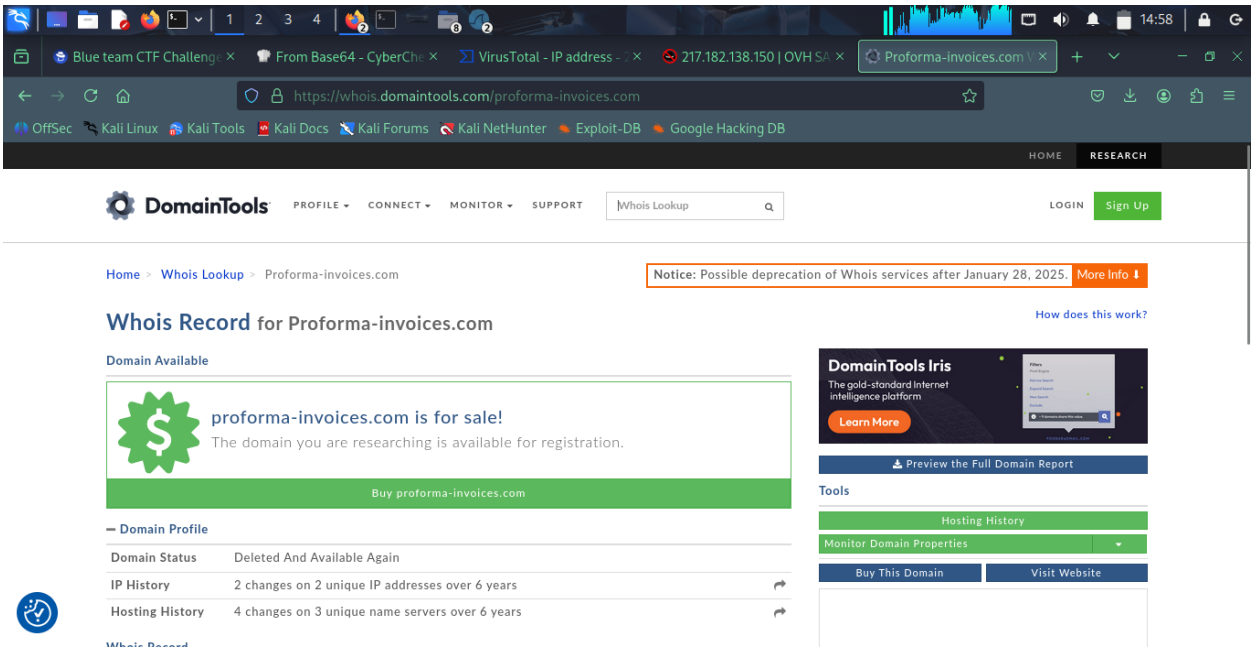
- Queried on AbuseIPDB
- ISP: OVH SAS (commonly abused by threat actors)
- Usage: Data center/web hosting
- Country: France
- VirusTotal: 4 security vendors flagged as malicious

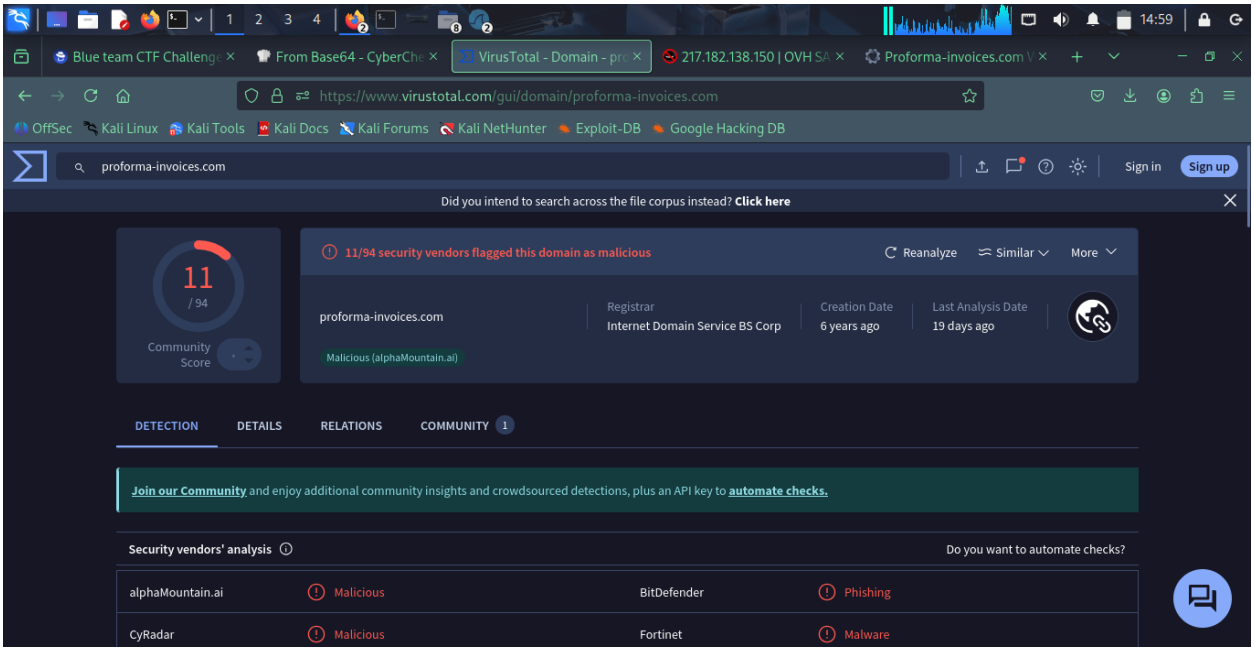
Malicious Domain: `pro-invoices.com`

- **WHOIS**: Domain is currently for sale (possible burner domain)
- **VirusTotal**: Flagged by 12 vendors, including phishing classifications
- **Domain History**: Two IP changes over 5 years, suspiciously minimal for legitimate domains



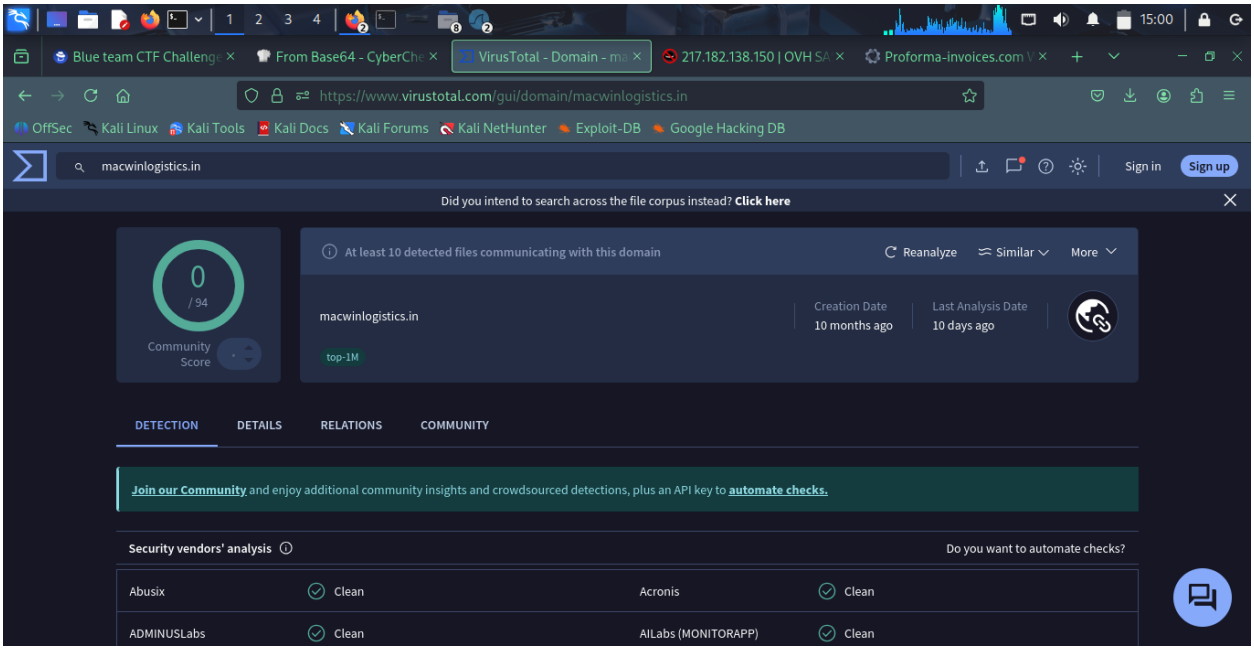


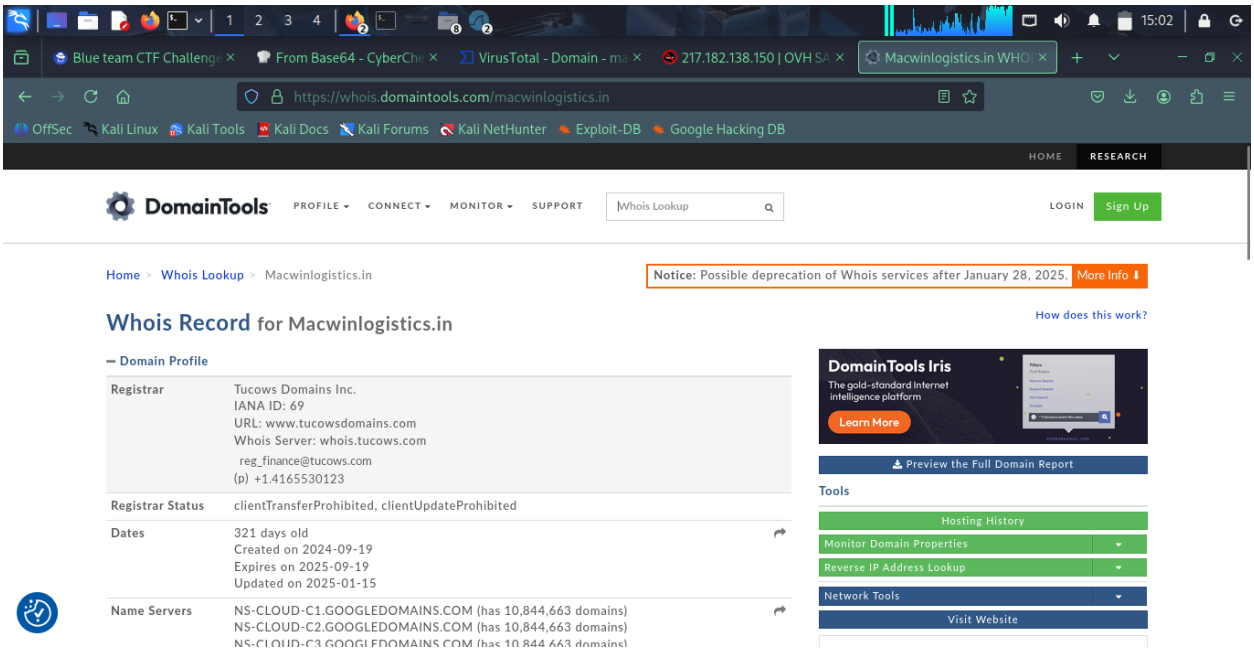


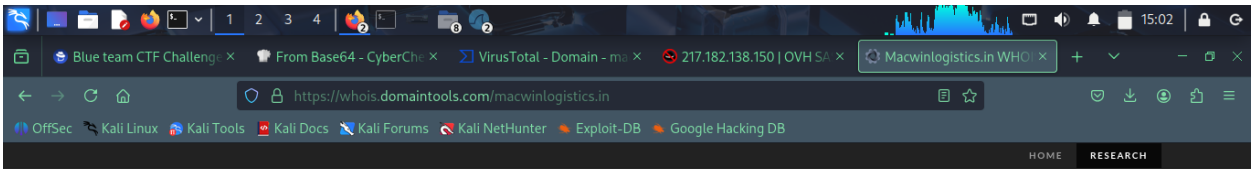


Email Domain: `macwinlogistics.com`

- VirusTotal shows:
  - No explicit flagging
  - 10+ files communicating with it, linked to Hawkeye
- WHOIS: Domain is also currently listed for sale


15:00
Blue team CTF Challenge
From Base64 - CyberChef
VirusTotal - Domain - ma
217.182.138.150 | OVH SA
Proforma-invoices.com
https://www.virustotal.com/gui/domain/macwinlogistics.in
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
macwinlogistics.in
Sign in
Sign up
Did you intend to search across the file corpus instead? Click here
0
/ 94
Community Score
At least 10 detected files communicating with this domain
Reanalyze
Similar
More
macwinlogistics.in
top-1M
Creation Date
10 months ago
Last Analysis Date
10 days ago
DETECTION
DETAILS
RELATIONS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Abusix
Clean
Acronis
Clean
ADMINUSLabs
Clean
AILabs (MONITORAPP)
Clean


15:02
Blue team CTF Challenge
From Base64 - CyberChef
VirusTotal - Domain - ma
217.182.138.150 | OVH SA
Macwinlogistics.in WHOIS
https://whois.domaintools.com/macwinlogistics.in
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Home > Whois Lookup > Macwinlogistics.in
Notice: Possible deprecation of Whois services after January 28, 2025. More Info
How does this work?
Whois Record for Macwinlogistics.in
Domain Profile
Registrar
Tucows Domains Inc.
IANA ID: 69
URL: www.tucowsdomains.com
Whois Server: whois.tucows.com
reg_finance@tucows.com
(p) +1.4165530123
Registrar Status
clientTransferProhibited, clientUpdateProhibited
Dates
321 days old
Created on 2024-09-19
Expires on 2025-09-19
Updated on 2025-01-15
Name Servers
NS-CLOUD-C1.GOOGLEDOMAINS.COM (has 10,844,663 domains)
NS-CLOUD-C2.GOOGLEDOMAINS.COM (has 10,844,663 domains)
DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website

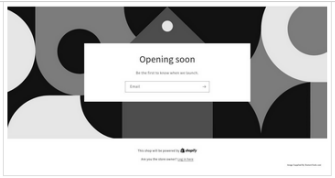


DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

IP Address	23.227.38.74 - 4,826,468 other sites hosted on this server
IP Location	- Ontario - Ottawa - Shopify Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
IP History	3 changes on 3 unique IP addresses over 2 years
Hosting History	3 changes on 3 unique name servers over 11 years

Whois Record (last updated on 2025-08-07)

```
Domain Name: macwinlogistics.in
Registry Domain ID: DFEEC8A4B4FBC467B901213ABB6A0C5F8-IN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: www.tucowsdomains.com
Updated Date: 2025-01-15T23:32:44.455Z
Creation Date: 2024-09-19T04:31:45.274Z
Registry Expiry Date: 2025-09-19T04:31:45.274Z
Registrar: Tucows Domains Inc.
Registrar IANA ID: 69
Registrar Abuse Contact Email: reg_finance@tucows.com
Registrar Abuse Contact Phone: +1.4165530123
Domain Status: clientTransferProhibited https://icann.org/
epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
```



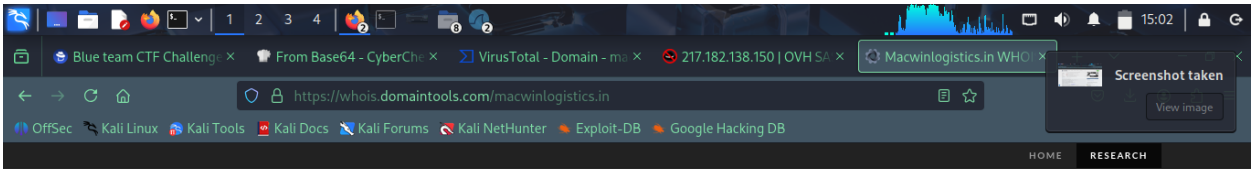
View Screenshot History

Available TLDs

General TLDs | Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- Taken domain.
- Available domain.
- Deleted previously owned domain.



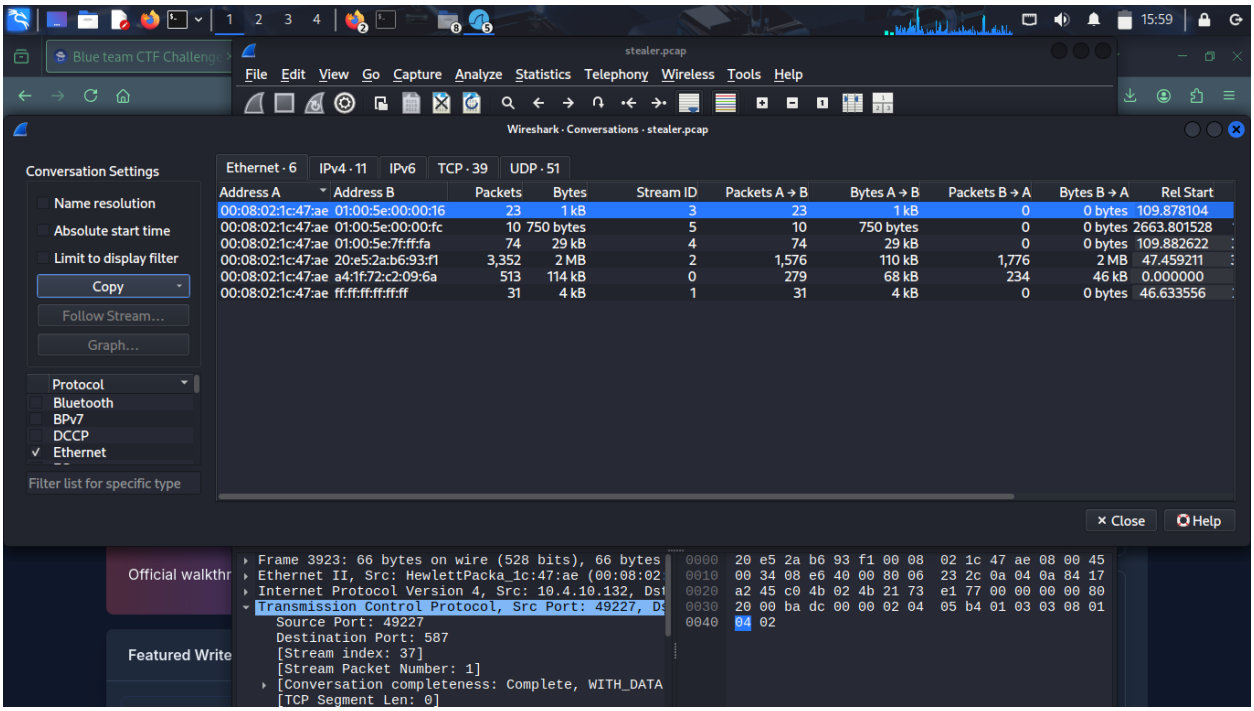
DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

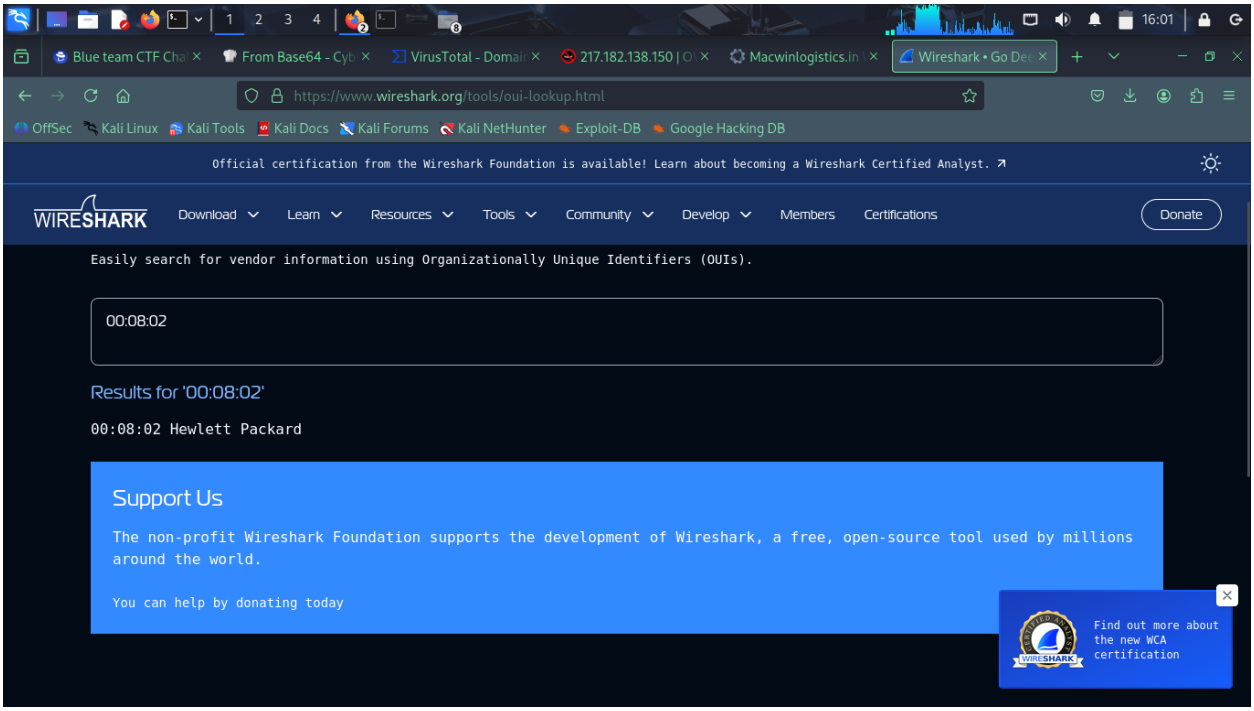
```
Registrar IANA ID: 69
Registrar Abuse Contact Email: reg_finance@tucows.com
Registrar Abuse Contact Phone: +1.4165530123
Domain Status: clientTransferProhibited https://icann.org/
epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: My Store
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: N/A
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: TW
Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identifie
d in this
output for information on how to contact the Registrant, Admin, or Tech contact of t
he queried
domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
```

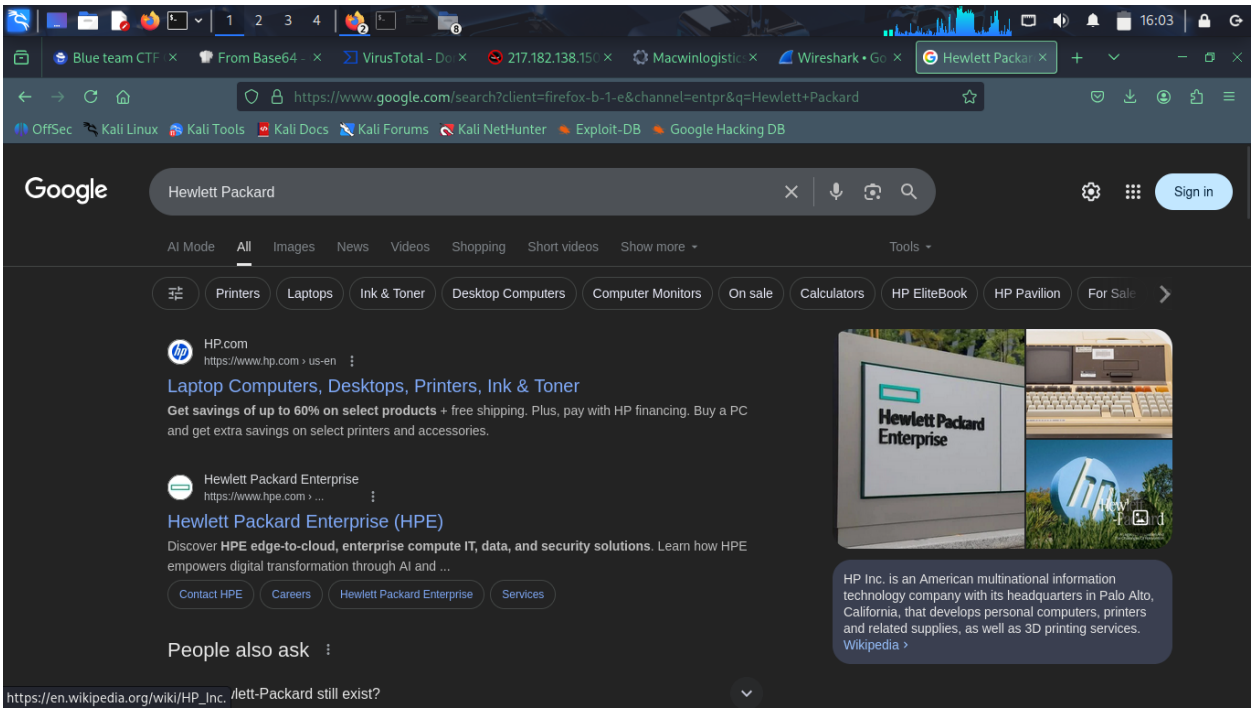
information. (3rd party site)

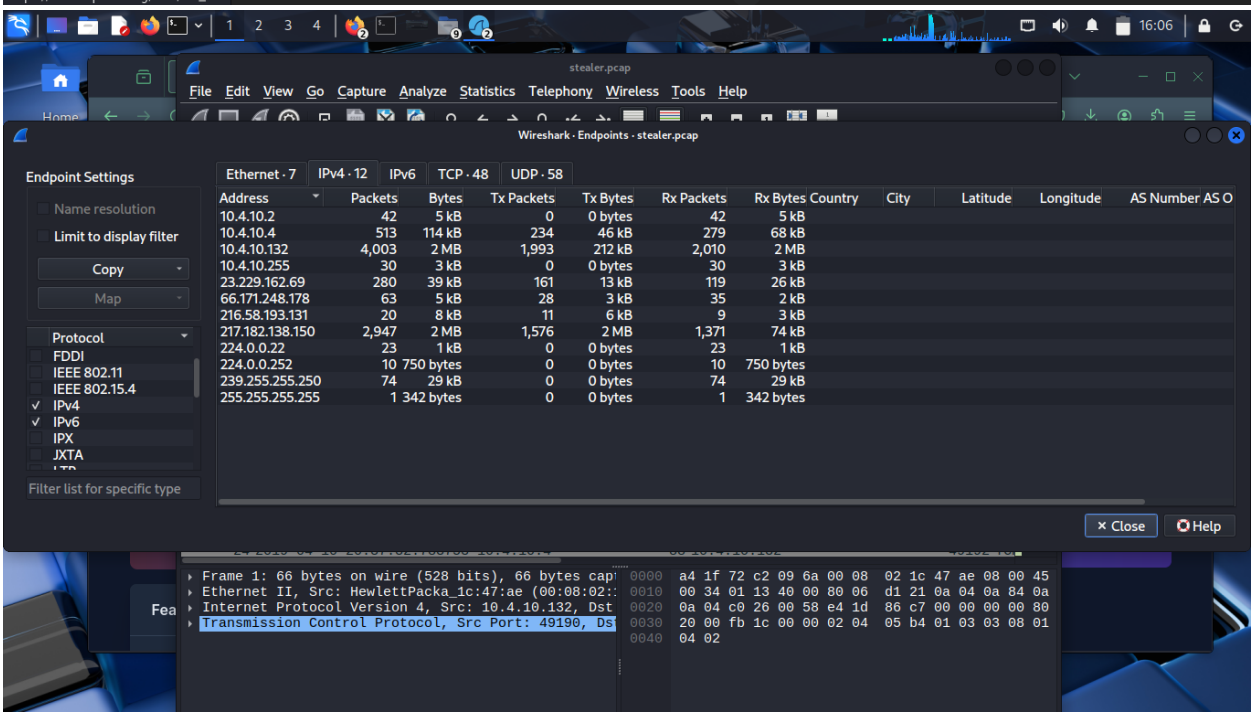
- Taken domain.
- Available domain.
- Deleted previously owned domain.

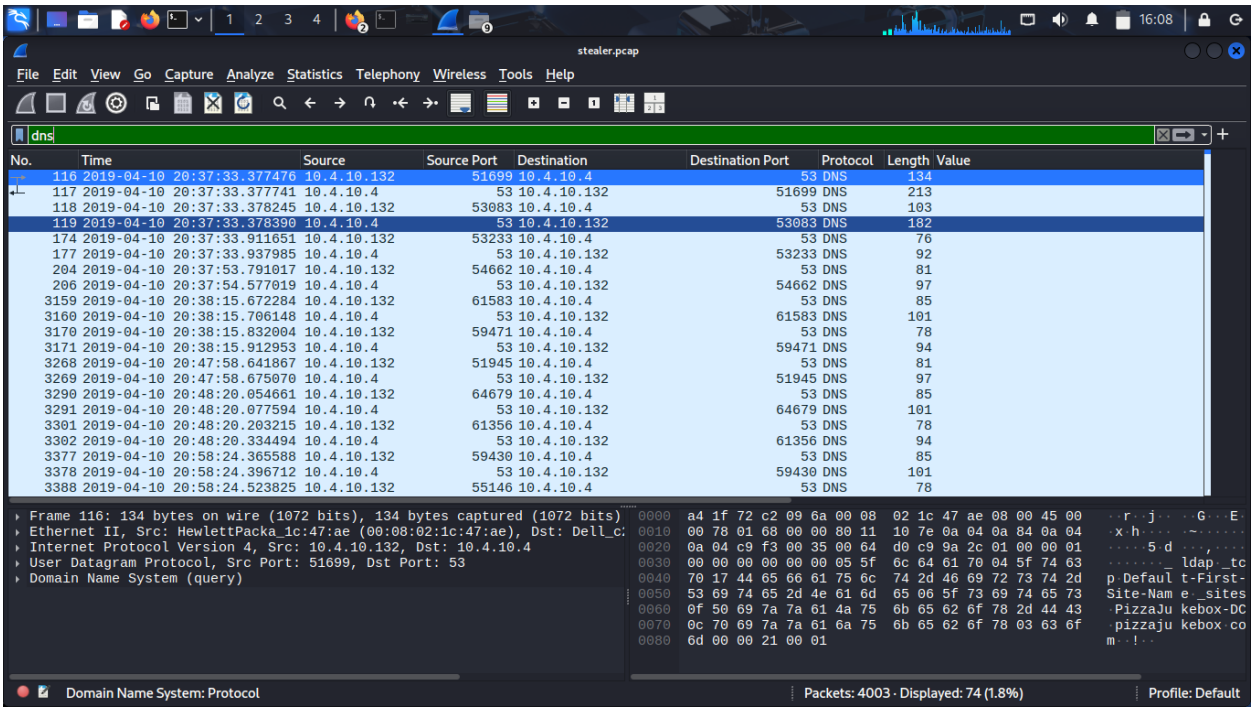
MacWinLogistics.com	View Whois
MacWinLogistics.net	Buy Domain
MacWinLogistics.org	Buy Domain
MacWinLogistics.info	Buy Domain
MacWinLogistics.biz	Buy Domain
MacWinLogistics.us	Buy Domain

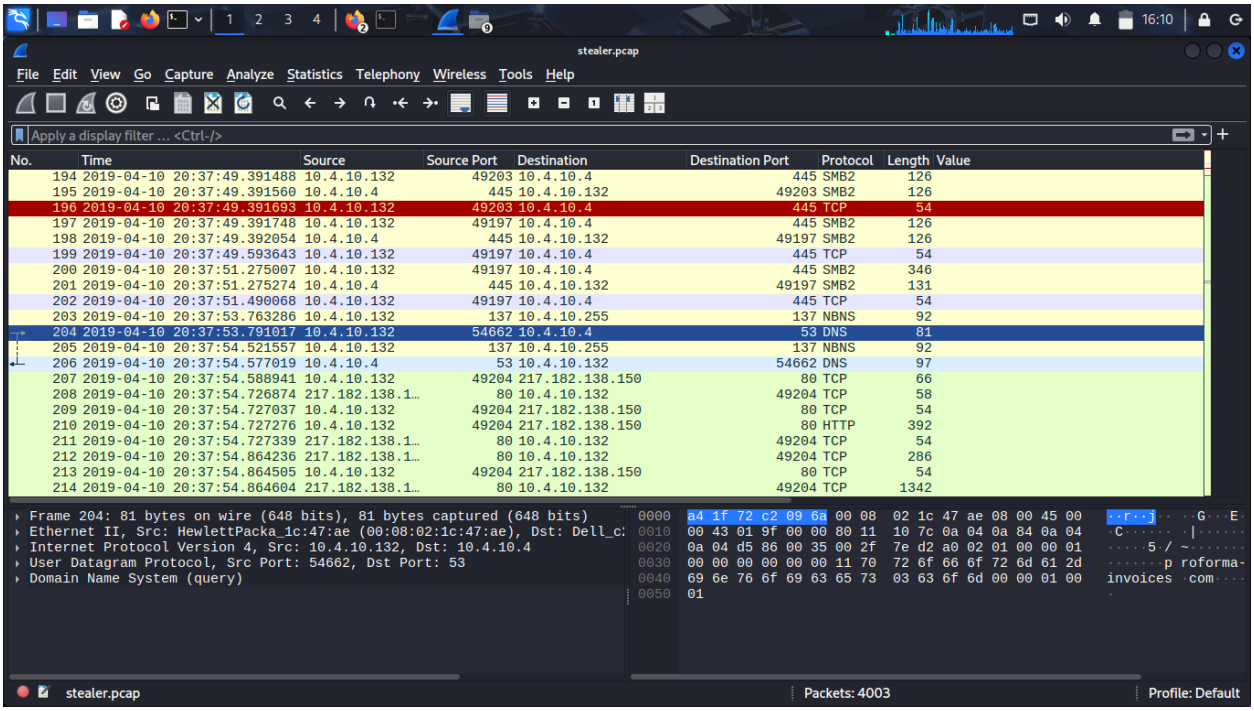

stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · stealer.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
BPv7
DCCP
Ethernet
Filter list for specific 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 Rel Start
00:08:02:1c:47:ae 01:00:5e:00:00:16 23 1 kB 3 23 1 kB 0 0 bytes 109.878104
00:08:02:1c:47:ae 01:00:5e:00:00:fc 10 750 bytes 5 10 750 bytes 0 0 bytes 2663.801528
00:08:02:1c:47:ae 01:00:5e:7f:ff:fa 74 29 kB 4 74 29 kB 0 0 bytes 109.882622
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 47.459211
00:08:02:1c:47:ae a4:1f:72:c2:09:6a 513 114 kB 0 279 68 kB 234 46 kB 0.000000
00:08:02:1c:47:ae ff:ff:ff:ff:ff:ff 31 4 kB 1 31 4 kB 0 0 bytes 46.633556
× Close
Help
Official walkthr
Featured Write
Frame 3923: 66 bytes on wire (528 bits), 66 bytes
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02
Internet Protocol Version 4, Src: 10.4.10.132, Ds
Transmission Control Protocol, Src Port: 49227, D
Source Port: 49227
Destination Port: 587
[Stream index: 37]
[Stream Packet Number: 1]
[Conversation completeness: Complete, WITH_DATA
[TCP Segment Len: 0]
0000 20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45
0010 00 34 08 e6 40 00 80 06 23 2c 0a 04 0a 84 17
0020 a2 45 c0 4b 02 4b 21 73 e1 77 00 00 00 00 80
0030 20 00 ba dc 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02

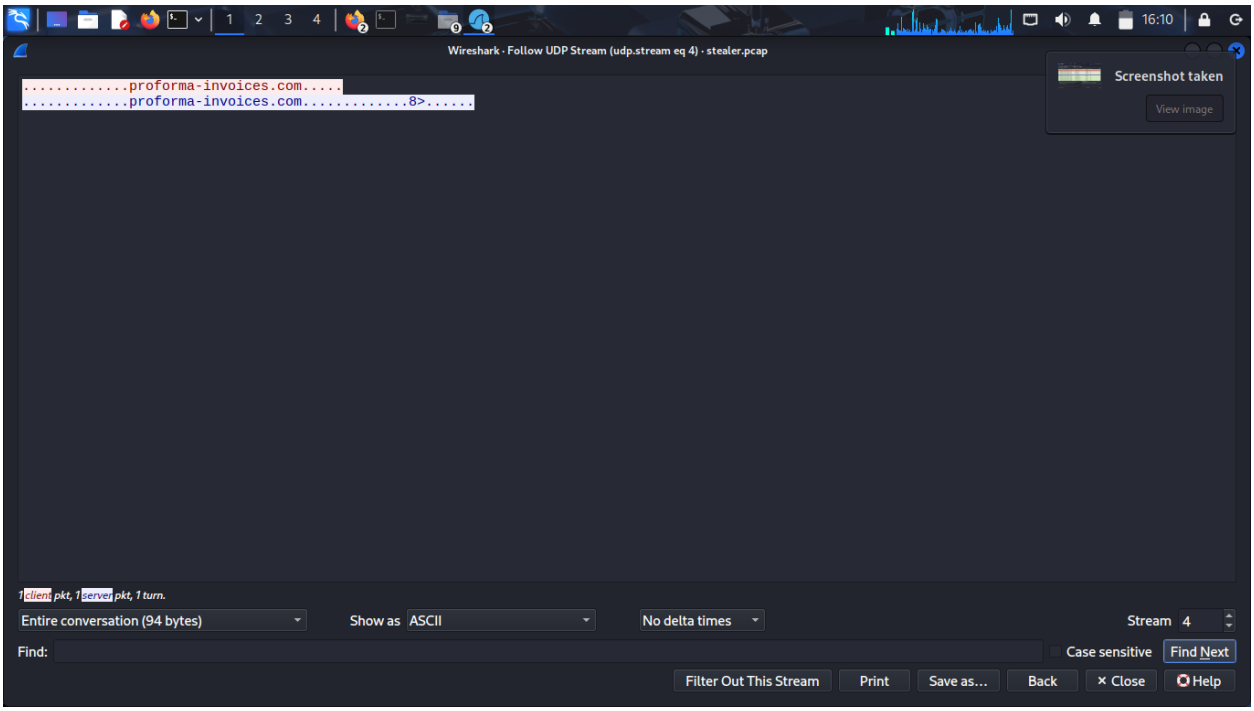

Blue team CTF Cha
From Base64 - Cyb
VirusTotal - Domai
217.182.138.150 | O
Macwinlogistics.in
Wireshark • Go Dee
https://www.wireshark.org/tools/oui-lookup.html
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Official certification from the Wireshark Foundation is available! Learn about becoming a Wireshark Certified Analyst. ↗
WIRESHARK
Download Learn Resources Tools Community Develop Members Certifications
Donate
Easily search for vendor information using Organizationally Unique Identifiers (OUIs).
00:08:02
Results for '00:08:02'
00:08:02 Hewlett Packard
Support Us
The non-profit Wireshark Foundation supports the development of Wireshark, a free, open-source tool used by millions around the world.
You can help by donating today
Find out more about the new WCA certification

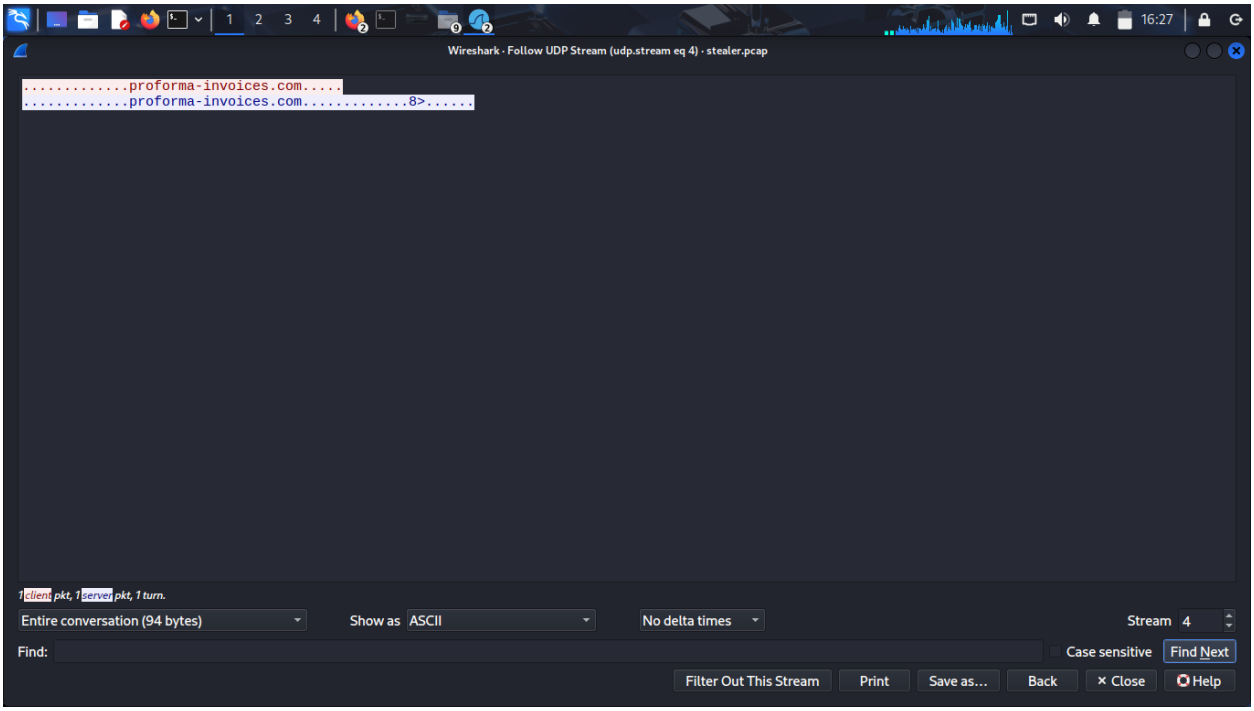

Blue team CTF
From Base64
VirusTotal - Do
217.182.138.150
Macwinlogistics
Wireshark • Go
Hewlett Packar
https://www.google.com/search?client=firefox-b-1-e&channel=entpr&q=Hewlett+Packard
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Google
Hewlett Packard
Sign in
AI Mode
All
Images
News
Videos
Shopping
Short videos
Show more
Tools
Printers
Laptops
Ink & Toner
Desktop Computers
Computer Monitors
On sale
Calculators
HP EliteBook
HP Pavilion
HP.com
https://www.hp.com › us-en
Laptop Computers, Desktops, Printers, Ink & Toner
Get savings of up to 60% on select products + free shipping. Plus, pay with HP financing. Buy a PC and get extra savings on select printers and accessories.
Hewlett Packard Enterprise
https://www.hpe.com › ...
Hewlett Packard Enterprise (HPE)
Discover HPE edge-to-cloud, enterprise compute IT, data, and security solutions. Learn how HPE empowers digital transformation through AI and ...
Contact HPE
Careers
Hewlett Packard Enterprise
Services
People also ask
Hewlett Packard Enterprise
HP Inc. is an American multinational information technology company with its headquarters in Palo Alto, California, that develops personal computers, printers and related supplies, as well as 3D printing services.
Wikipedia ›
https://en.wikipedia.org/wiki/HP_Inc. /lett-Packard still exist?

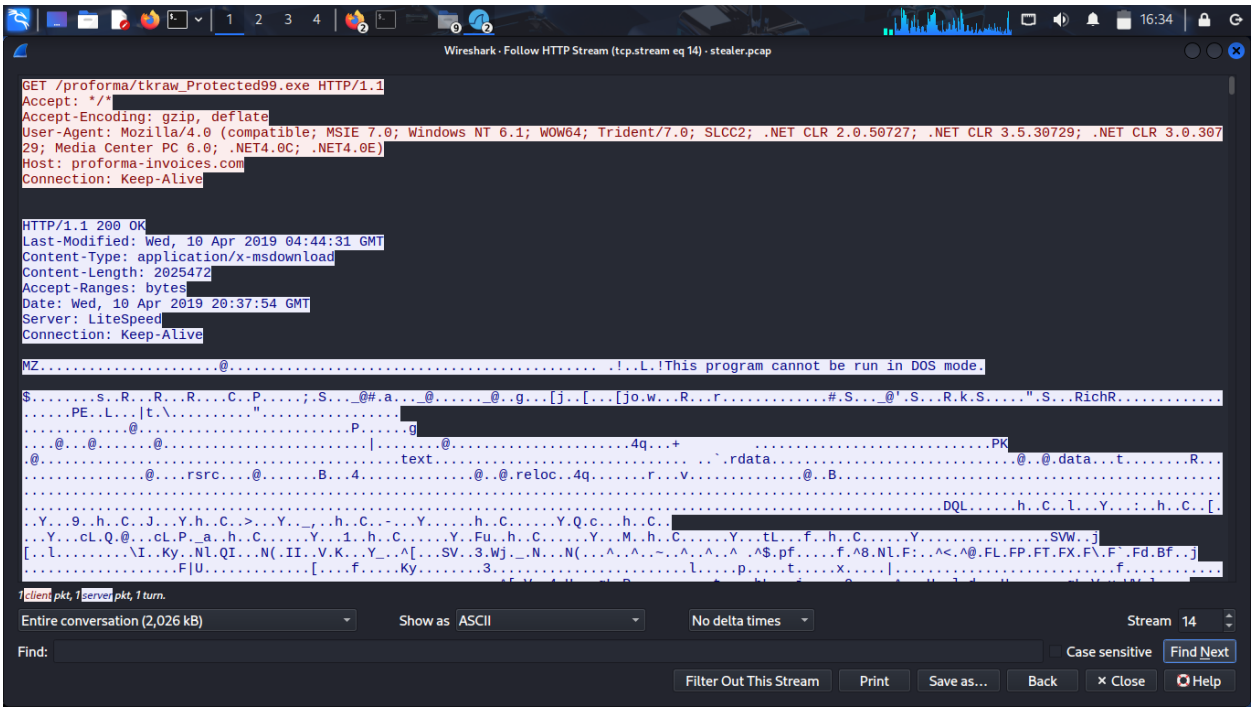

stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Endpoints · stealer.pcap
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Protocol
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
Filter list for specific type
Ethernet · 7
IPv4 · 12
IPv6
TCP · 48
UDP · 58
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City Latitude Longitude AS Number AS O
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
Close
Help
Frame 1: 66 bytes on wire (528 bits), 66 bytes cap
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:
Internet Protocol Version 4, Src: 10.4.10.132, Dst
Transmission Control Protocol, Src Port: 49190, Ds
0000 a4 1f 72 c2 09 6a 00 08 02 1c 47 ae 08 00 45
0010 00 34 01 13 40 00 80 06 d1 21 0a 04 0a 84 0a
0020 0a 04 c0 26 00 58 e4 1d 86 c7 00 00 00 00 80
0030 20 00 fb 1c 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02

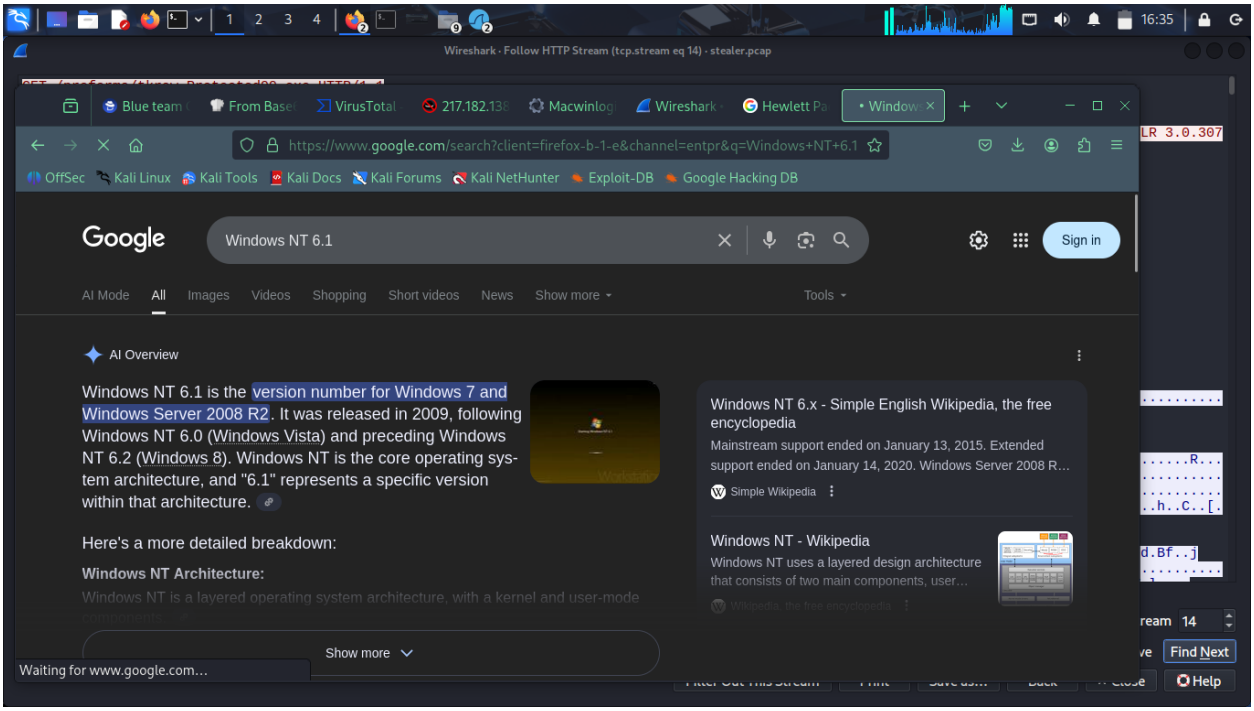

stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Source Port Destination Destination Port Protocol Length Value
116 2019-04-10 20:37:33.377476 10.4.10.132 51699 10.4.10.4 53 DNS 134
117 2019-04-10 20:37:33.377741 10.4.10.4 53 10.4.10.132 51699 DNS 213
118 2019-04-10 20:37:33.378245 10.4.10.132 53083 10.4.10.4 53 DNS 103
119 2019-04-10 20:37:33.378390 10.4.10.4 53 10.4.10.132 53083 DNS 182
174 2019-04-10 20:37:33.911651 10.4.10.132 53233 10.4.10.4 53 DNS 76
177 2019-04-10 20:37:33.937985 10.4.10.4 53 10.4.10.132 53233 DNS 92
204 2019-04-10 20:37:53.791017 10.4.10.132 54662 10.4.10.4 53 DNS 81
206 2019-04-10 20:37:54.577019 10.4.10.4 53 10.4.10.132 54662 DNS 97
3159 2019-04-10 20:38:15.672284 10.4.10.132 61583 10.4.10.4 53 DNS 85
3160 2019-04-10 20:38:15.706148 10.4.10.4 53 10.4.10.132 61583 DNS 101
3170 2019-04-10 20:38:15.832004 10.4.10.132 59471 10.4.10.4 53 DNS 78
3171 2019-04-10 20:38:15.912953 10.4.10.4 53 10.4.10.132 59471 DNS 94
3268 2019-04-10 20:47:58.641867 10.4.10.132 51945 10.4.10.4 53 DNS 81
3269 2019-04-10 20:47:58.675070 10.4.10.4 53 10.4.10.132 51945 DNS 97
3290 2019-04-10 20:48:20.054661 10.4.10.132 64679 10.4.10.4 53 DNS 85
3291 2019-04-10 20:48:20.077594 10.4.10.4 53 10.4.10.132 64679 DNS 101
3301 2019-04-10 20:48:20.203215 10.4.10.132 61356 10.4.10.4 53 DNS 78
3302 2019-04-10 20:48:20.334494 10.4.10.4 53 10.4.10.132 61356 DNS 94
3377 2019-04-10 20:58:24.365588 10.4.10.132 59430 10.4.10.4 53 DNS 85
3378 2019-04-10 20:58:24.396712 10.4.10.4 53 10.4.10.132 59430 DNS 101
3388 2019-04-10 20:58:24.523825 10.4.10.132 55146 10.4.10.4 53 DNS 78
Frame 116: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c
Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4
User Datagram Protocol, Src Port: 51699, Dst Port: 53
Domain Name System (query)
0000 a4 1f 72 c2 09 6a 00 08 02 1c 47 ae 08 00 45 00
0010 00 78 01 68 00 00 80 11 10 7e 0a 04 0a 84 0a 04
0020 0a 04 c9 f3 00 35 00 64 d0 c9 9a 2c 01 00 00 01
0030 00 00 00 00 00 00 05 5f 6c 64 61 70 04 5f 74 63
0040 70 17 44 65 66 61 75 6c 74 2d 46 69 72 73 74 2d
0050 53 69 74 65 2d 4e 61 6d 65 06 5f 73 69 74 65 73
0060 0f 50 69 7a 7a 61 4a 75 6b 65 62 6f 78 2d 44 43
0070 0c 70 69 7a 7a 61 6a 75 6b 65 62 6f 78 03 63 6f
0080 6d 00 00 21 00 01
Domain Name System: Protocol
Packets: 4003 · Displayed: 74 (1.8%)
Profile: Default

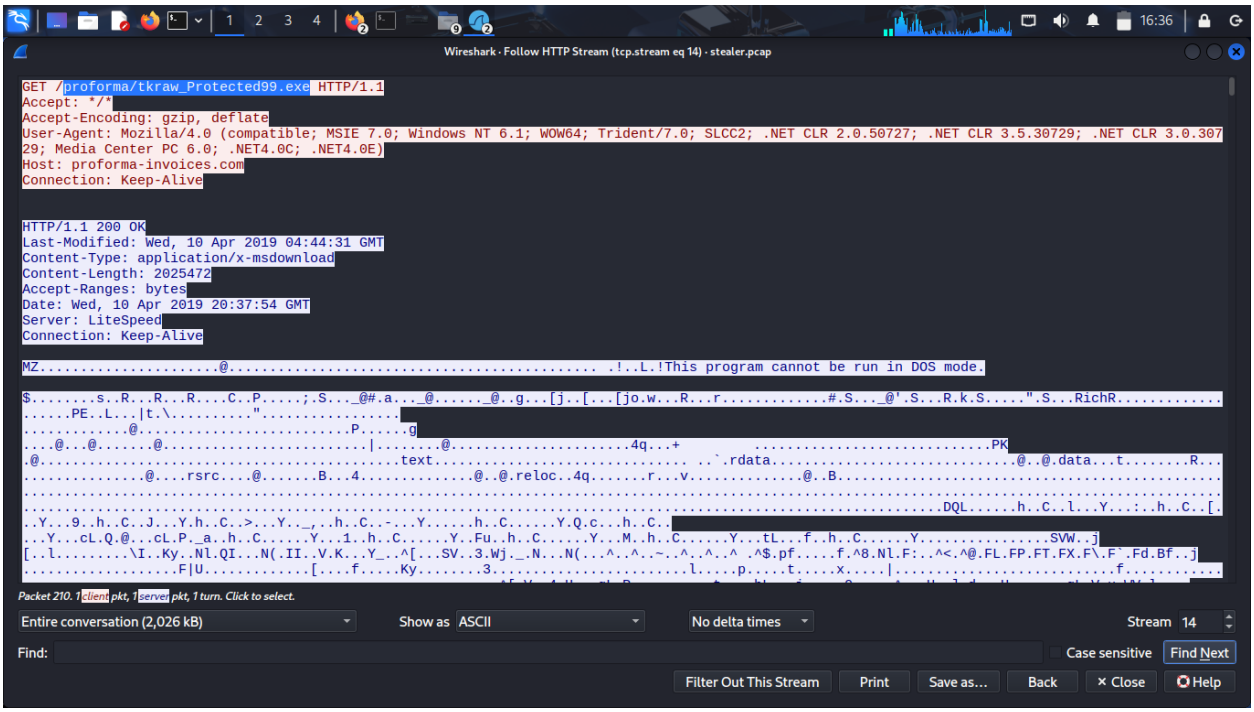

stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Source Port Destination Destination Port Protocol Length Value
194 2019-04-10 20:37:49.391488 10.4.10.132 49203 10.4.10.4 445 SMB2 126
195 2019-04-10 20:37:49.391560 10.4.10.4 445 10.4.10.132 49203 SMB2 126
196 2019-04-10 20:37:49.391693 10.4.10.132 49203 10.4.10.4 445 TCP 54
197 2019-04-10 20:37:49.391748 10.4.10.132 49197 10.4.10.4 445 SMB2 126
198 2019-04-10 20:37:49.392054 10.4.10.4 445 10.4.10.132 49197 SMB2 126
199 2019-04-10 20:37:49.593643 10.4.10.132 49197 10.4.10.4 445 TCP 54
200 2019-04-10 20:37:51.275007 10.4.10.132 49197 10.4.10.4 445 SMB2 346
201 2019-04-10 20:37:51.275274 10.4.10.4 445 10.4.10.132 49197 SMB2 131
202 2019-04-10 20:37:51.490068 10.4.10.132 49197 10.4.10.4 445 TCP 54
203 2019-04-10 20:37:53.763286 10.4.10.132 137 10.4.10.255 137 NBNS 92
204 2019-04-10 20:37:53.791017 10.4.10.132 54662 10.4.10.4 53 DNS 81
205 2019-04-10 20:37:54.521557 10.4.10.132 137 10.4.10.255 137 NBNS 92
206 2019-04-10 20:37:54.577019 10.4.10.4 53 10.4.10.132 54662 DNS 97
207 2019-04-10 20:37:54.588941 10.4.10.132 49204 217.182.138.150 80 TCP 66
208 2019-04-10 20:37:54.726874 217.182.138.1… 80 10.4.10.132 49204 TCP 58
209 2019-04-10 20:37:54.727037 10.4.10.132 49204 217.182.138.150 80 TCP 54
210 2019-04-10 20:37:54.727276 10.4.10.132 49204 217.182.138.150 80 HTTP 392
211 2019-04-10 20:37:54.727339 217.182.138.1… 80 10.4.10.132 49204 TCP 54
212 2019-04-10 20:37:54.864236 217.182.138.1… 80 10.4.10.132 49204 TCP 286
213 2019-04-10 20:37:54.864505 10.4.10.132 49204 217.182.138.150 80 TCP 54
214 2019-04-10 20:37:54.864604 217.182.138.1… 80 10.4.10.132 49204 TCP 1342
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_c
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)
0000 a4 1f 72 c2 09 6a 00 08 02 1c 47 ae 08 00 45 00
0010 00 43 01 9f 00 00 80 11 10 7c 0a 04 0a 84 0a 04
0020 0a 04 d5 86 00 35 00 2f 7e d2 a0 02 01 00 00 01
0030 00 00 00 00 00 00 11 70 72 6f 66 6f 72 6d 61 2d
0040 69 6e 76 6f 69 63 65 73 03 63 6f 6d 00 00 01 00
0050 01
stealer.pcap
Packets: 4003
Profile: Default

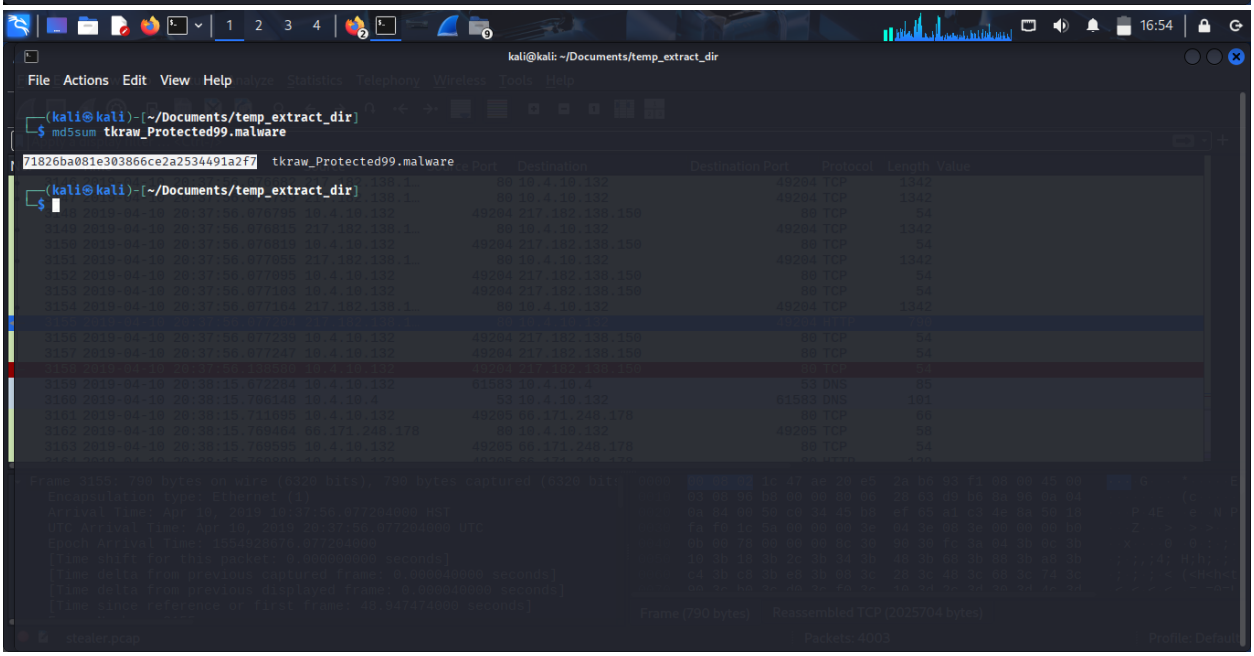

16:10
Wireshark · Follow UDP Stream (udp.stream eq 4) · stealer.pcap
.....proforma-invoices.com.....
.....proforma-invoices.com.....8>.....
Screenshot taken
View image
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (94 bytes)
Show as ASCII
No delta times
Stream 4
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
× Close
Help


16:27
Wireshark · Follow UDP Stream (udp.stream eq 4) · stealer.pcap
.....proforma-invoices.com.....
.....proforma-invoices.com.....8>.....
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (94 bytes)
Show as ASCII
No delta times
Stream 4
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
× Close
Help


16:34
Wireshark · Follow HTTP Stream (tcp.stream eq 14) · stealer.pcap
GET /proforma/tkraw_Protected99.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.307
29; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: proforma-invoices.com
Connection: Keep-Alive
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
MZ.....@..... .!..L.!This program cannot be run in DOS mode.
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (2,026 kB)
Show as ASCII
No delta times
Stream 14
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
× Close
Help


16:35
Wireshark · Follow HTTP Stream (tcp.stream eq 14) · stealer.pcap
https://www.google.com/search?client=firefox-b-1-e&channel=entpr&q=Windows+NT+6.1
Google
Windows NT 6.1
Sign in
AI Mode
All
Images
Videos
Shopping
Short videos
News
Show more
Tools
AI Overview
Windows NT 6.1 is the version number for Windows 7 and Windows Server 2008 R2. It was released in 2009, following Windows NT 6.0 (Windows Vista) and preceding Windows NT 6.2 (Windows 8). Windows NT is the core operating system architecture, and "6.1" represents a specific version within that architecture.
Here's a more detailed breakdown:
Windows NT Architecture:
Windows NT is a layered operating system architecture, with a kernel and user-mode
Show more
Windows NT 6.x - Simple English Wikipedia, the free encyclopedia
Mainstream support ended on January 13, 2015. Extended support ended on January 14, 2020. Windows Server 2008 R...
Simple Wikipedia
Windows NT - Wikipedia
Windows NT uses a layered design architecture that consists of two main components, user...
Waiting for www.google.com...

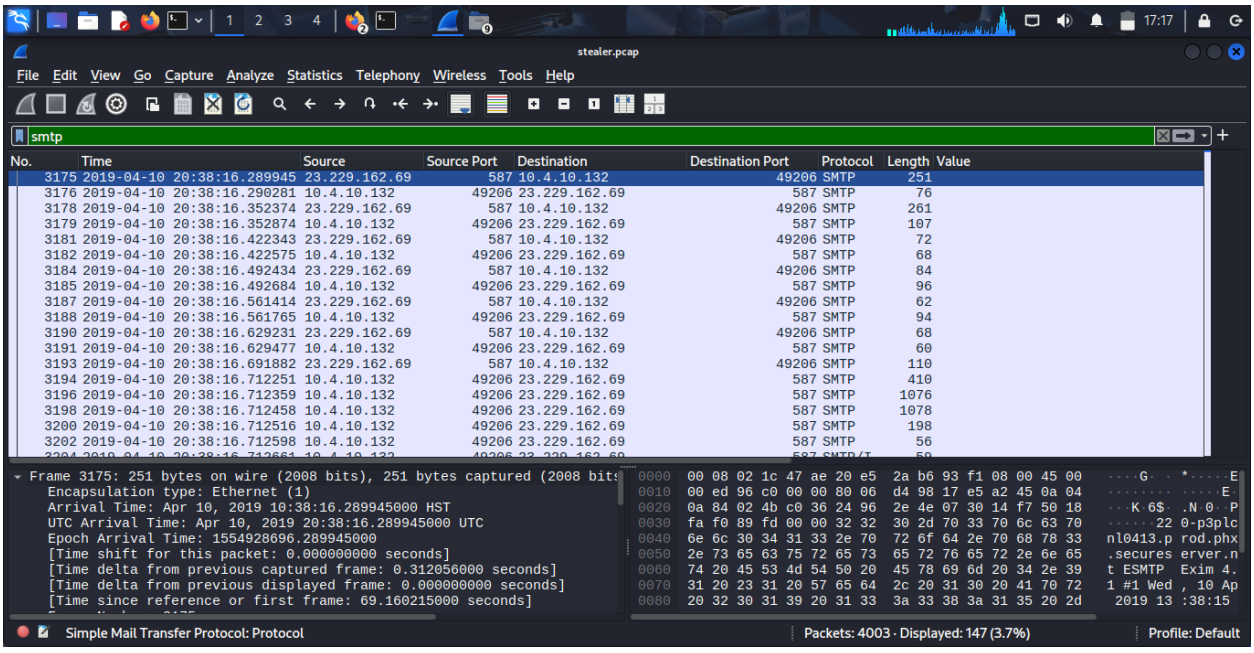


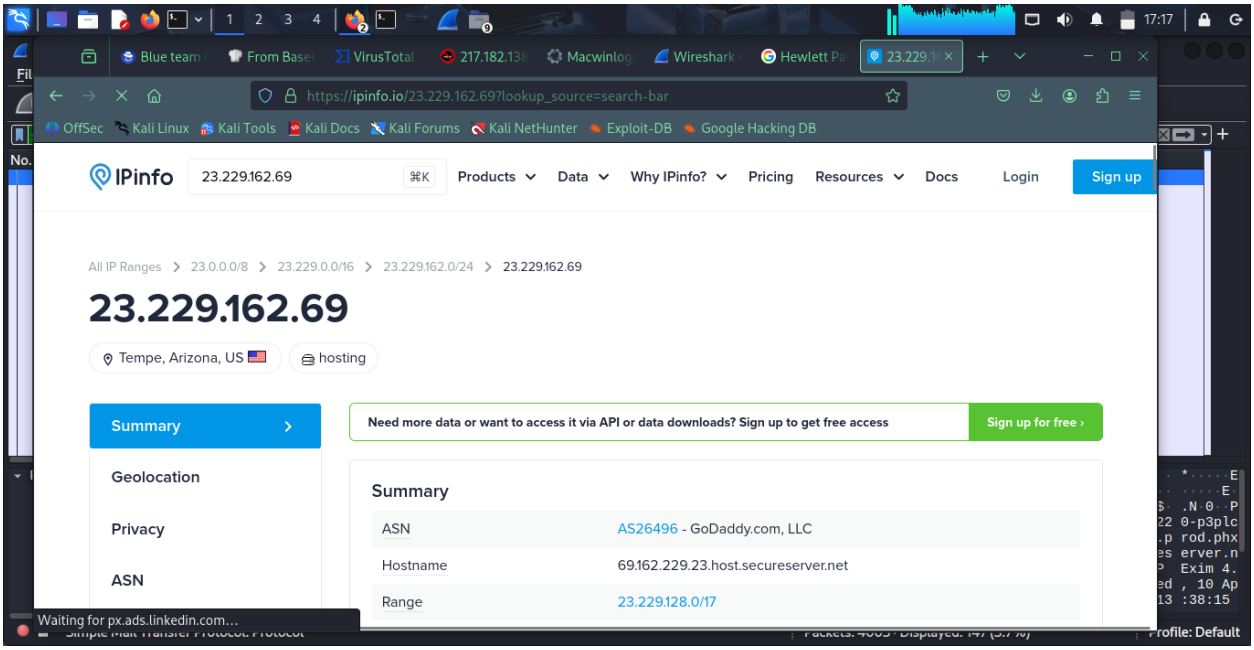


DNS Activity

- **DNS Server IP**: `10.4.104.104`
  Identified by observing responses from port 53 to the internal host.
- **Queried Domain (Packet #204)**: `pro-invoices.com`
- **Resolved IP for Domain**: `217.182.138.150`

- **Domain Geolocation**: France 🇫🇷 (via IP lookup tools)



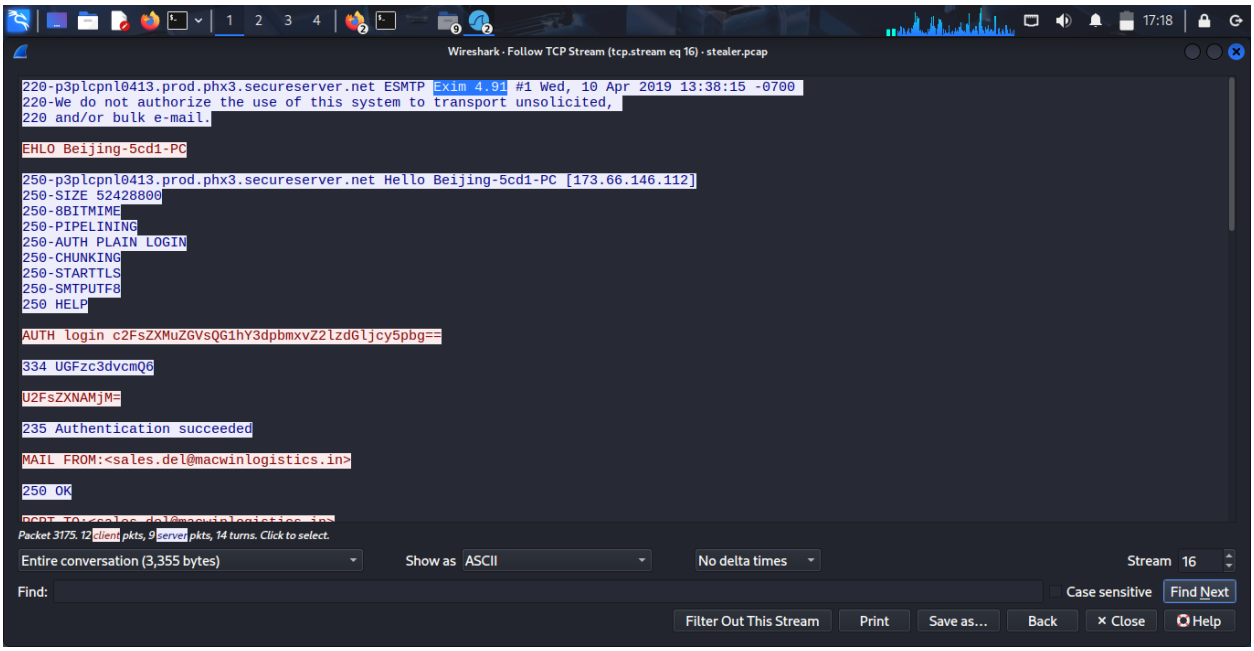


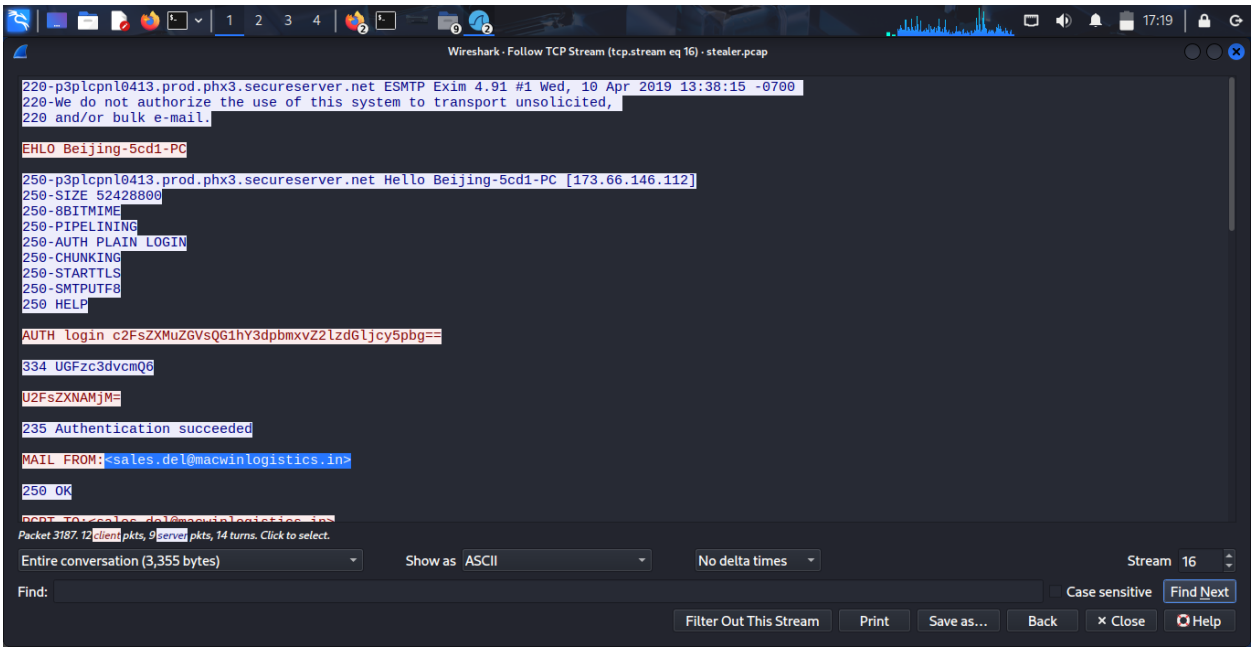
Host Identification

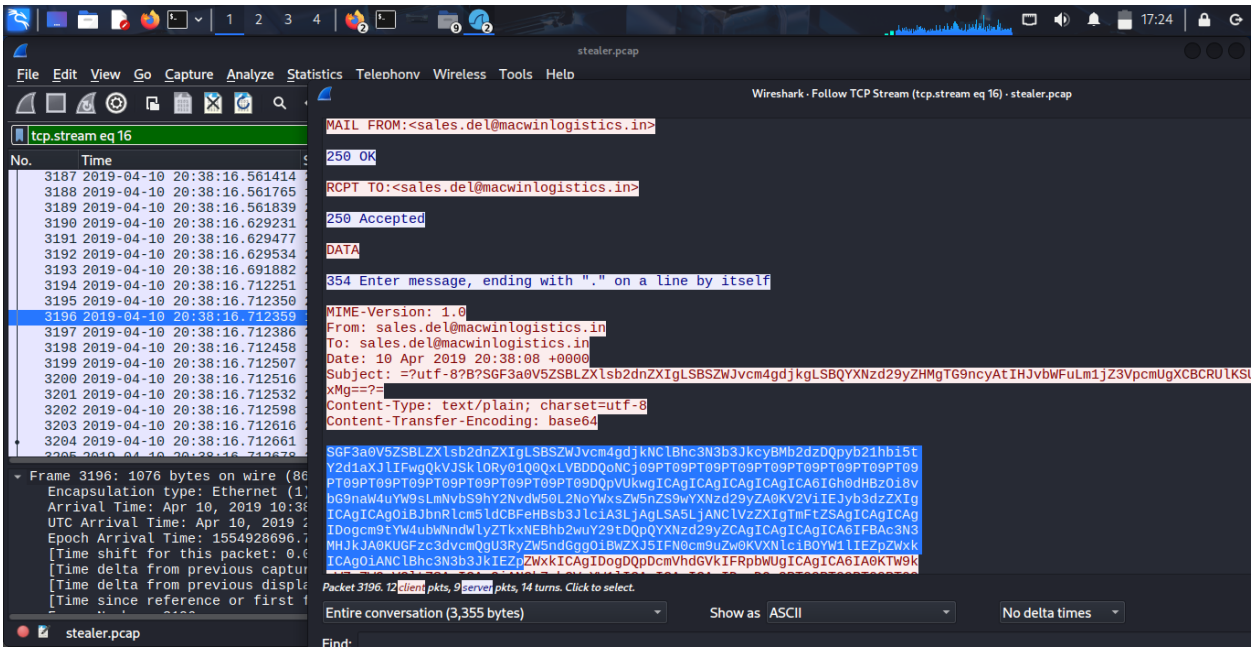
- **Hostname**: `BEIJING-D5CD1-PC`
- **Internal IP**: `10.4.104.132`
- **Public IP**: `173.66.146.12`

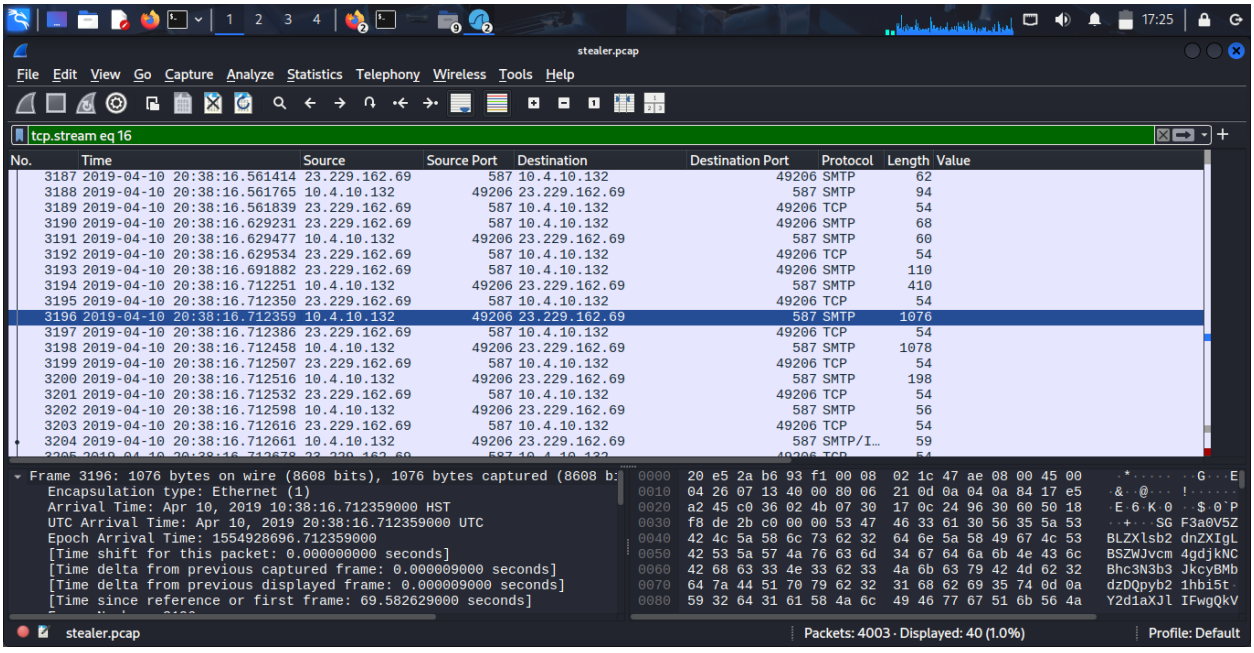
Target Email Address

- sales@dellmacwinlogistics.com









Conclusion:

This investigation successfully reconstructed a simulated credential exfiltration attack using deep PCAP analysis. By following a structured SOC workflow, the Hawkeye malware was identified as the primary actor. The timeline of activity was determined, sensitive data exfiltration paths were confirmed, and multiple internal hosts were identified as potentially affected.

This lab sharpened real-world forensics skills such as:

- Layer 2–Layer 7 analysis

- SMTP payload decoding
- IOC extraction
- Timeline reconstruction
- Cross-verification using OSINT and malware intelligence