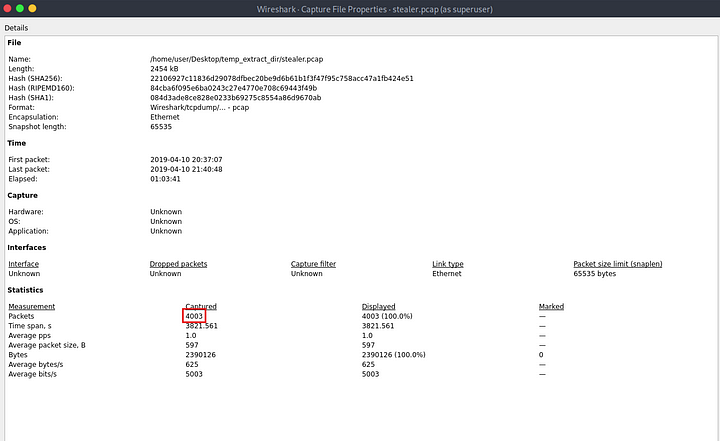
### **HawkEye Lab — CyberDefenders**

**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.

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

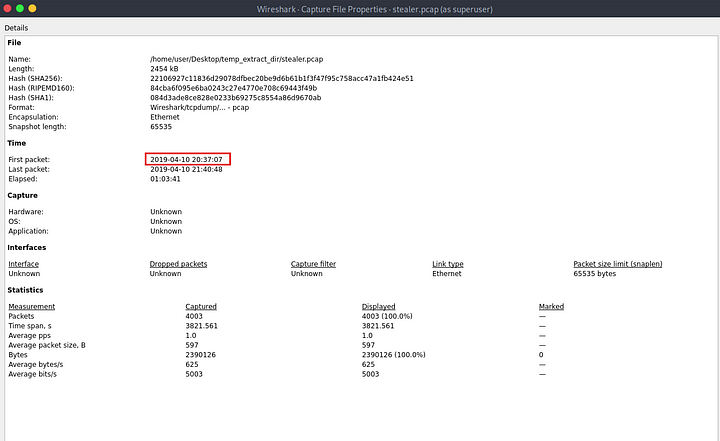
Go to Statistics -> Capture File Properties.



**Answer:** 4003

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

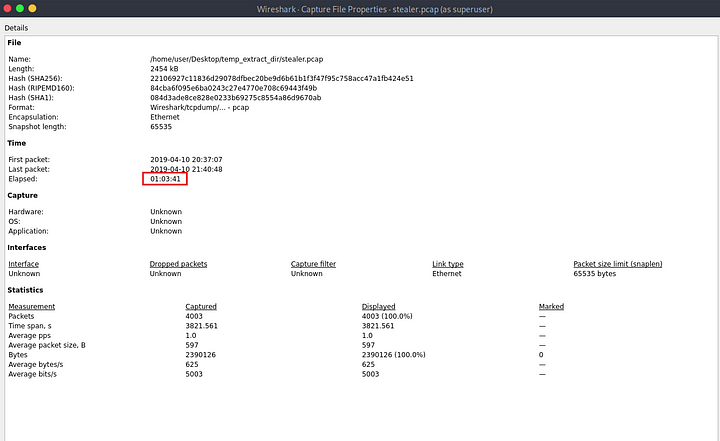
This can also be found in the capture file properties.



Answer: 2019–04–10 20:37:07 UTC

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

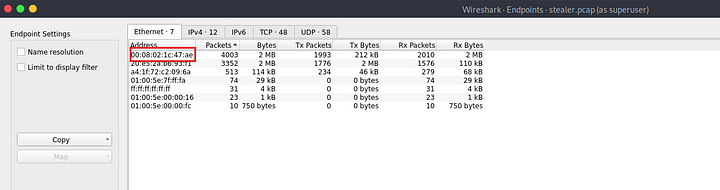
This can also be found in the capture file properties.



**Answer:** 01:03:41

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

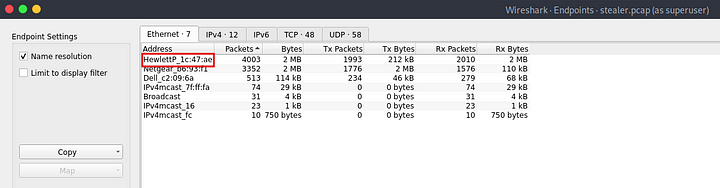
Go to Statistics -> Endpoints. Then sort by number of packets. The MAC address with most number of packets is the answer.



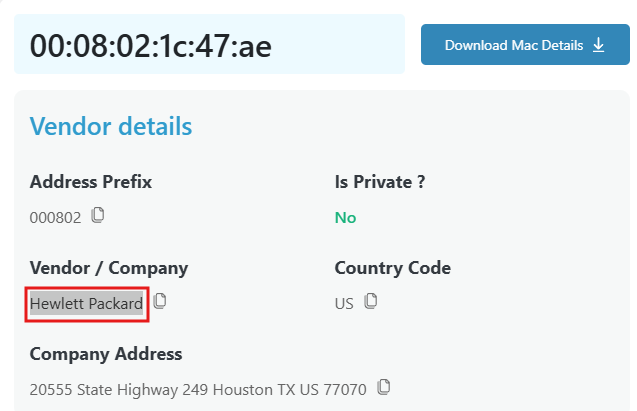
**Answer:** 00:08:02:1c:47:ae

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

In the Endpoints tab, select Name resolution on the left.



We can see it belongs to HP — Hewlett-Packard. We can also find this out online with tools like MAC lookup.



**Answer:** Hewlett-Packard

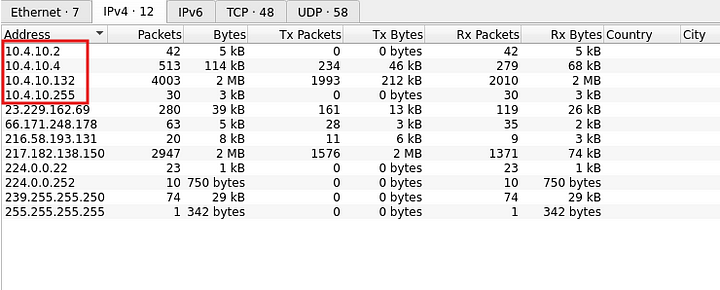
**6. Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?**

The headquarters of HP is in Palo Alto, California.

Answer: Palo Alto.

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

Under Endpoints, go to IPV4 tab.

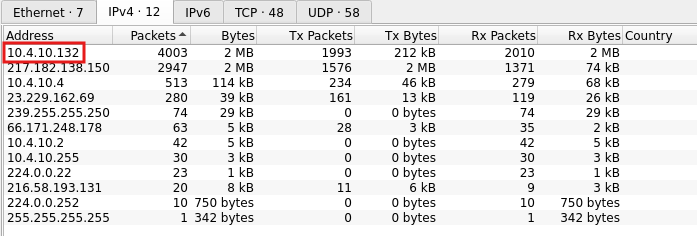


There are 4 private IP addresses. One of them 10.4.10.255 is a broadcast address, so the total number of computer is 3.

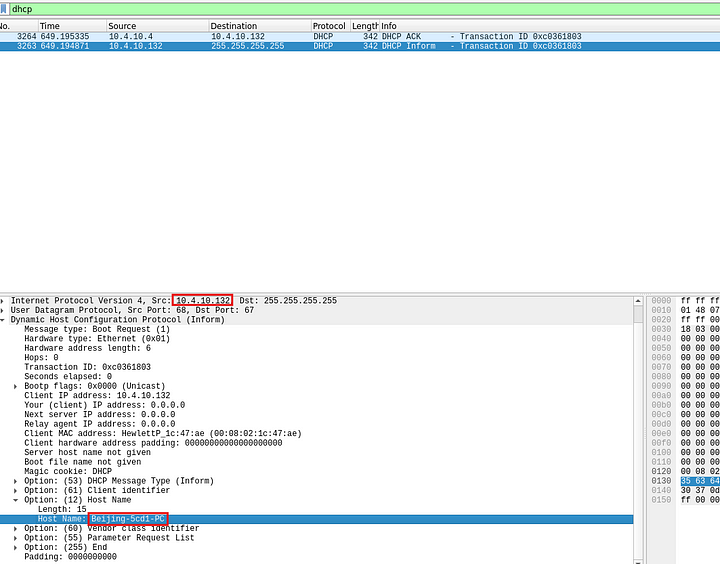
**Answer:** 3

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

In the same IPv4 tab sort the IP addresses based on the number of packets.



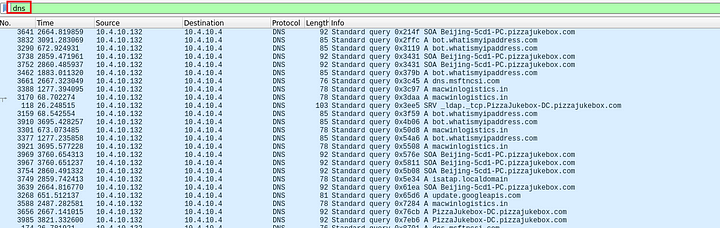
We need to find the name of this computer. For this we can search for the DHCP packets.



Answer: Beijing-5cd1-PC

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

Filter the dns packets.

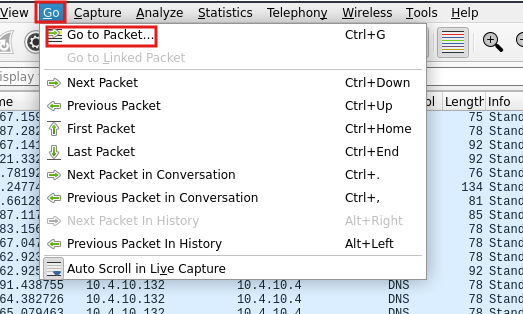


We can see above, all the dns queries are directed to the same IP address.

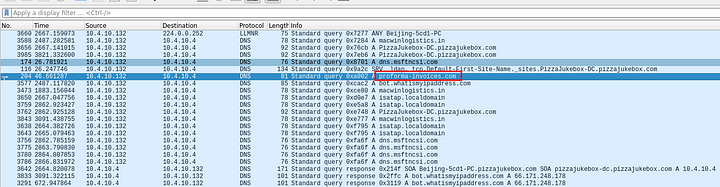
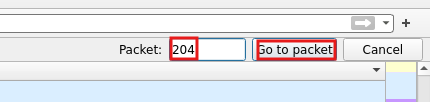
**Answer:** 10.4.10.4

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

Click on Go -> Go to Packet.



Then enter the packet number and click go to packet.

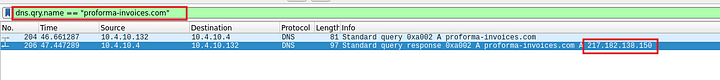


**Answer:** proforma-invoices.com

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

We can search for the DNS queries for the above domain.

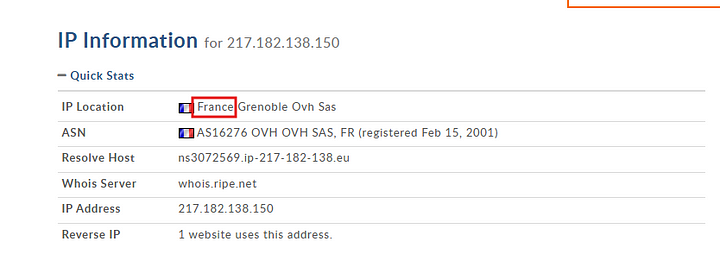
dns.qry.name == "proforma-invoices.com"



**Answer:** 217.182.138.150

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

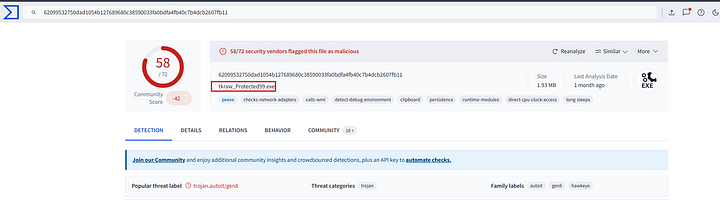
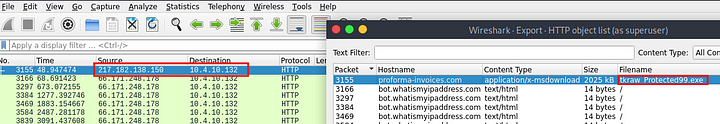
We can use online tools like whois.domaintools.com to find the country of origin of this IP address.



**Answer:** France

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

So far, the endpoint with the IP address 10.4.10.132 seems to be the victim, but to confirm this I checked for any http objects. I found that an executable was downloaded by this machine. Upon uploading the hash of this executable to VirusTotal it came out to be malicious.



So it is clear that 10.4.10.132 is indeed the victim. We can find the Operating system of this machine by checking the User agent string in the HTTP requests sent by the above host.

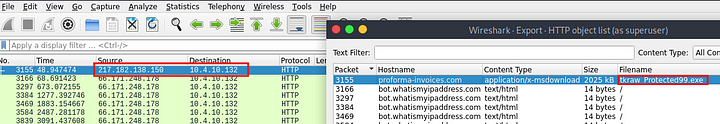
http.request && ip.src == 10.4.10.132



**Answer:** Windows NT 6.1

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

We saw this in the question 13.



**Answer:** tkraw\_Protected99.exe

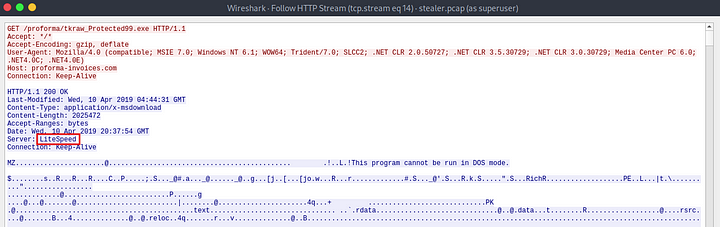
**15. What is the md5 hash of the downloaded file?**

****

**Answer:** 71826ba081e303866ce2a2534491a2f7

**16. What software runs the webserver that hosts the malware?**

Let us examine the http request from the question 13. Select the packet and click on follow http stream.

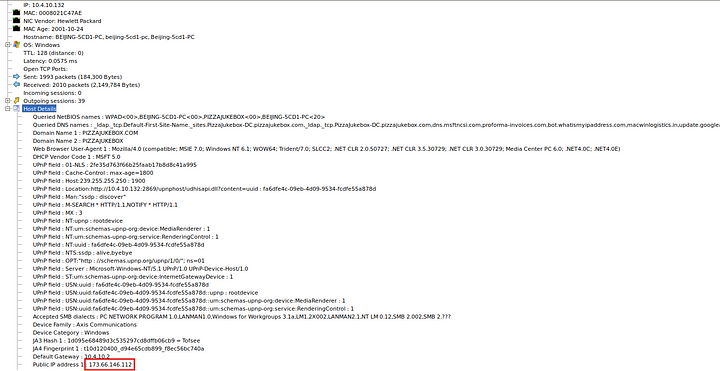


As we can see from the response, the server used by the malicious actor to host the malware is LiteSpeed.

Answer: LiteSpeed

**17.What is the public IP of the victim’s computer?**

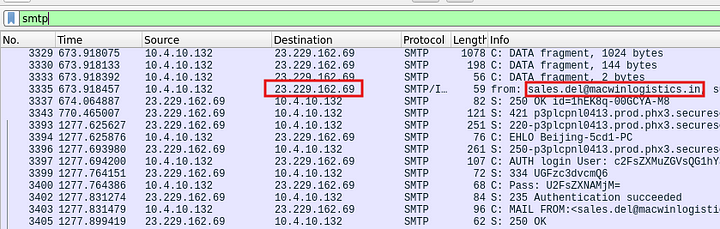
This is easier o find in the Network Miner. Open the capture file in network miner and go to hosts tab and select eh victim and check the host details.



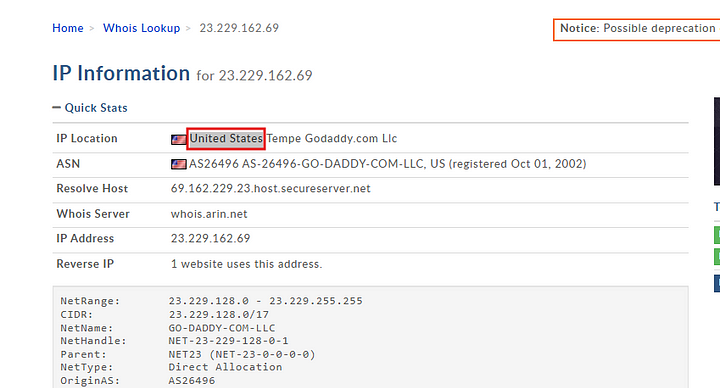
Answer: 173.66.146.112

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

Let us look for SMTP traffic.



We can see that the data is being sent to sales.del@macwinlogistics.in. Let us take the IP address and check online for the country.

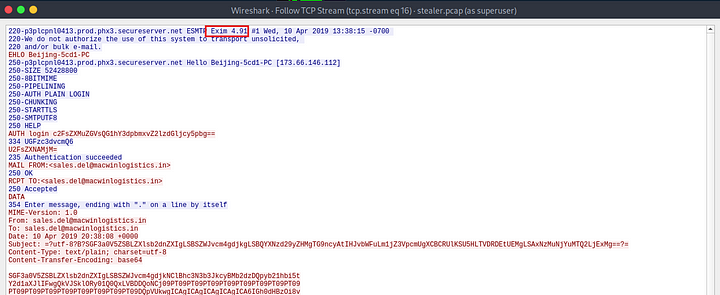
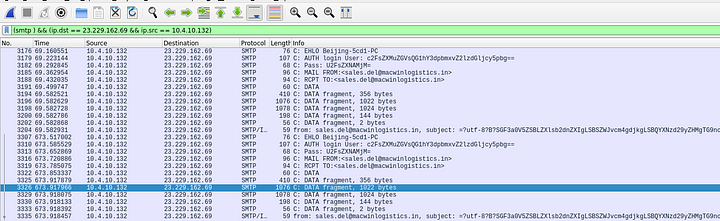


**Answer:** United States

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

Let us first filter these smtp traffic to show the smtp traffic sent from the victim to the attacker.

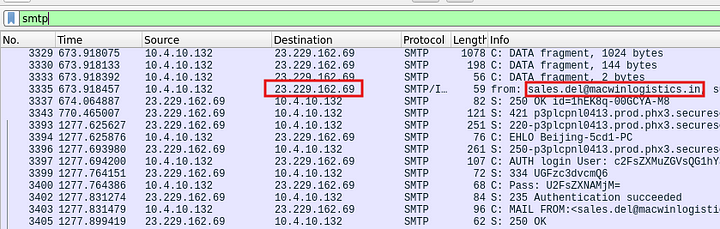
(smtp ) && (ip.dst == 23.229.162.69 && ip.src == 10.4.10.132)



Now follow TCP stream on any packet.  
**Answer:** Exim 4.91

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

We saw this in the question 18.

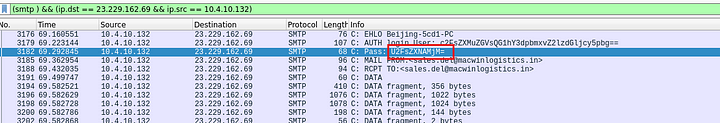


**Answer:** sales.del@macwinlogistics.in

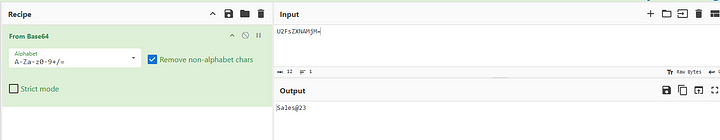
**21. What is the password used by the malware to send the email?**

In the question 19 we filtered the SMTP traffic between the victim and the attacker.

(smtp ) && (ip.dst == 23.229.162.69 && ip.src == 10.4.10.132)



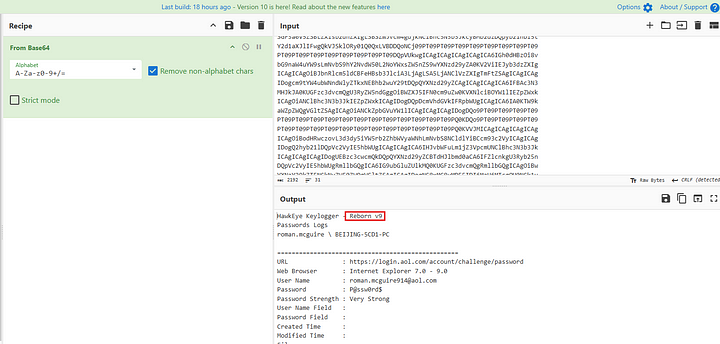
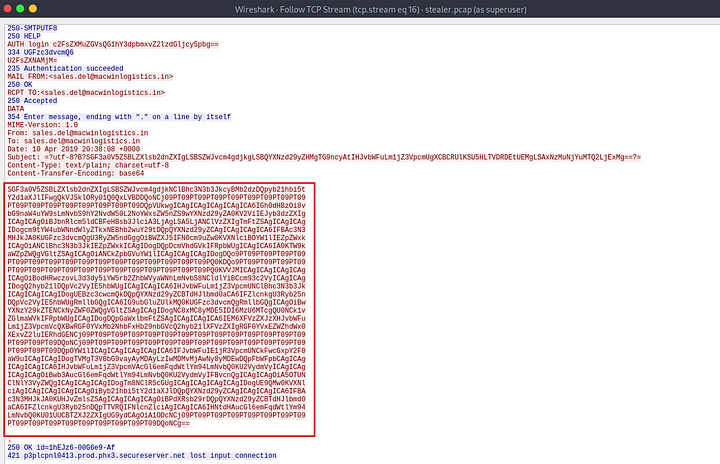
As we can see in the third packet there is a Password which is encoded. If we copy this and paste it to cyberchef, we can see the password.



Answer: Sales@23

**22. Which malware variant exfiltrated the data?**

Let us decode the data in the SMTP packets.



As we can see above this is a keylogger and the name is Reborn v9

**Answer:** Reborn v9

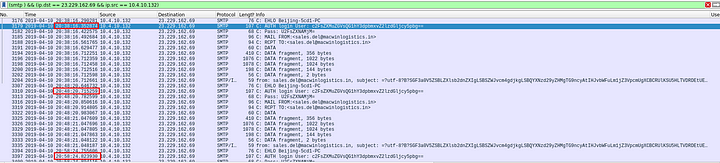
**23. What are the bankofamerica access credentials? (username:password)**

In the same packet, which we decoded, we can see the credentials belonging to bankofamerica.com.



**Answer:** roman.mcguire:P@ssw0rd$

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

****

We can see the time difference above.

**Answer:** 10

This is the end of this lab.