HawkEye Lab

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

91-hawkeye (1).zip

Unzip the file with password cyberdefenders.org

Tactics:

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

Tools:

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

Scenario:

An accountant at your organization received an email regarding an invoice with a download link. Suspicious network traffic was observed shortly after opening the email. As a SOC analyst, investigate the network trace and analyze exfiltration attempts.

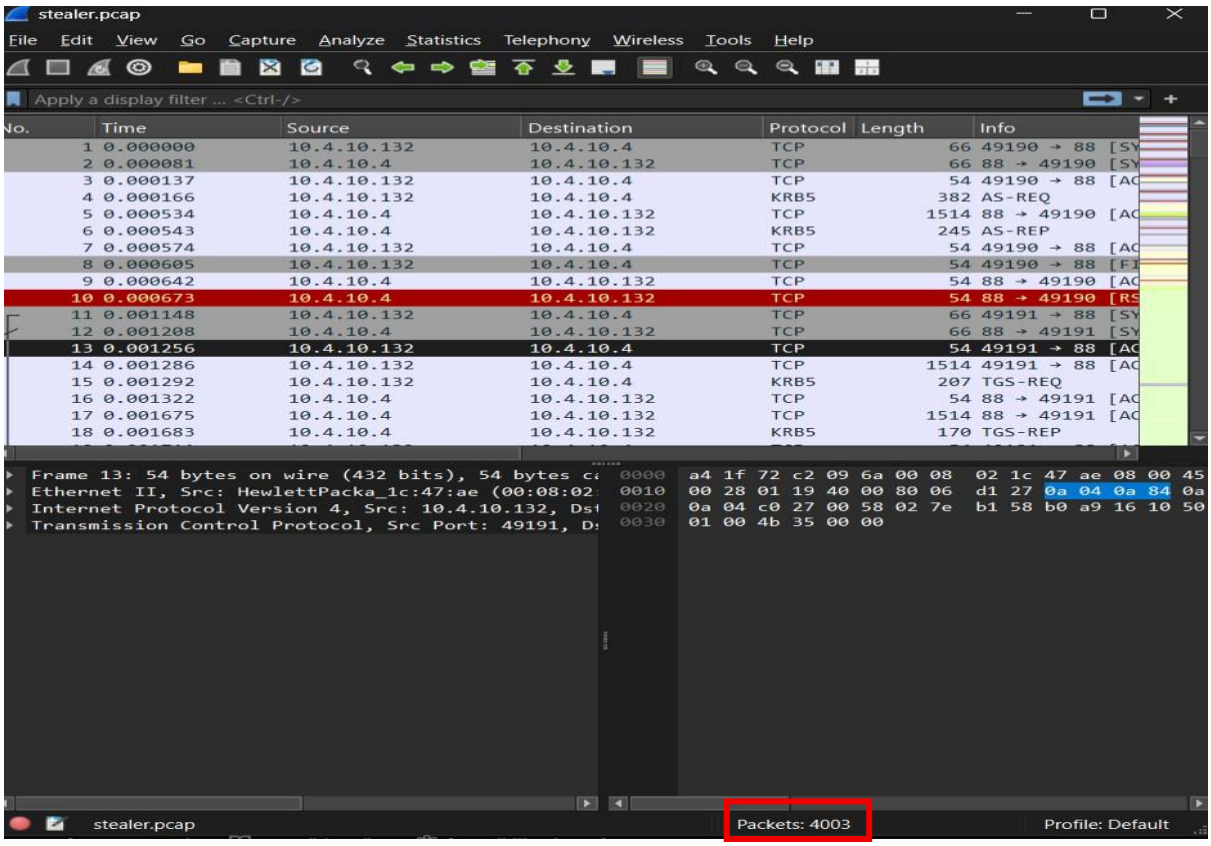
Achievement:

Blue team CTF Challenges | HawkEye - CyberDefenders

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

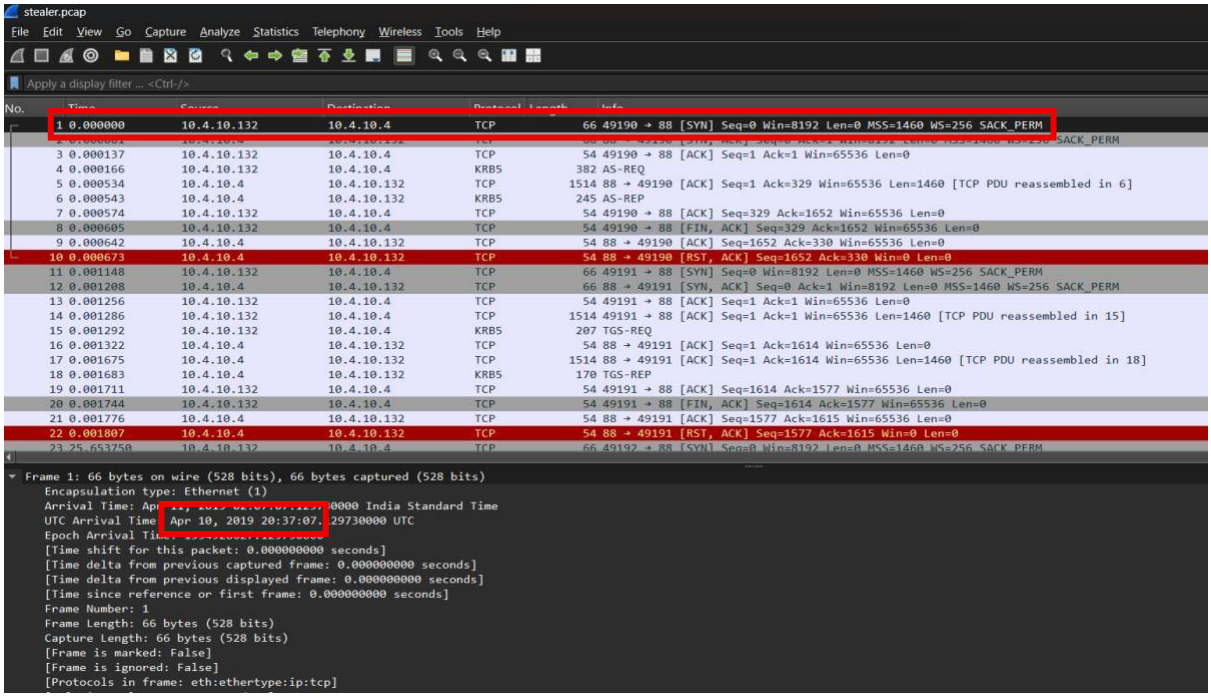
How many packets does the capture have?

4003



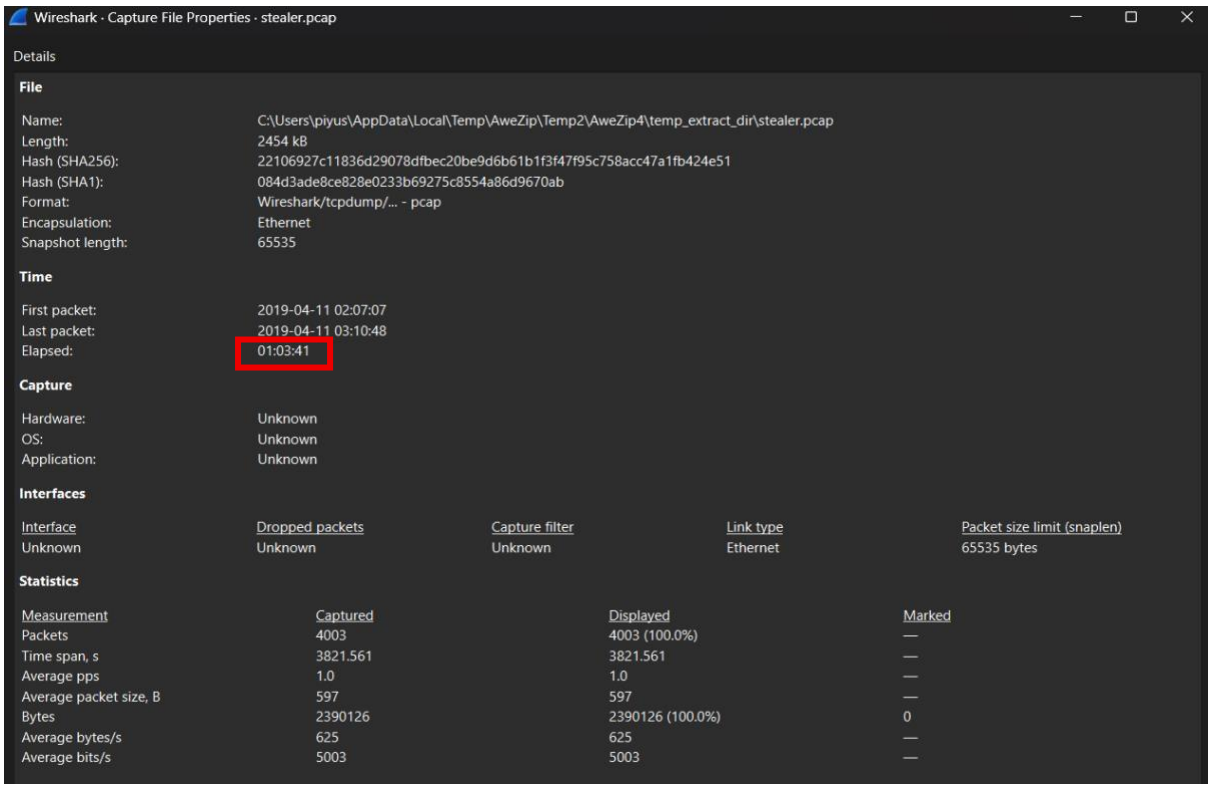
At what time was the first packet captured?

2019-04-10 20:37



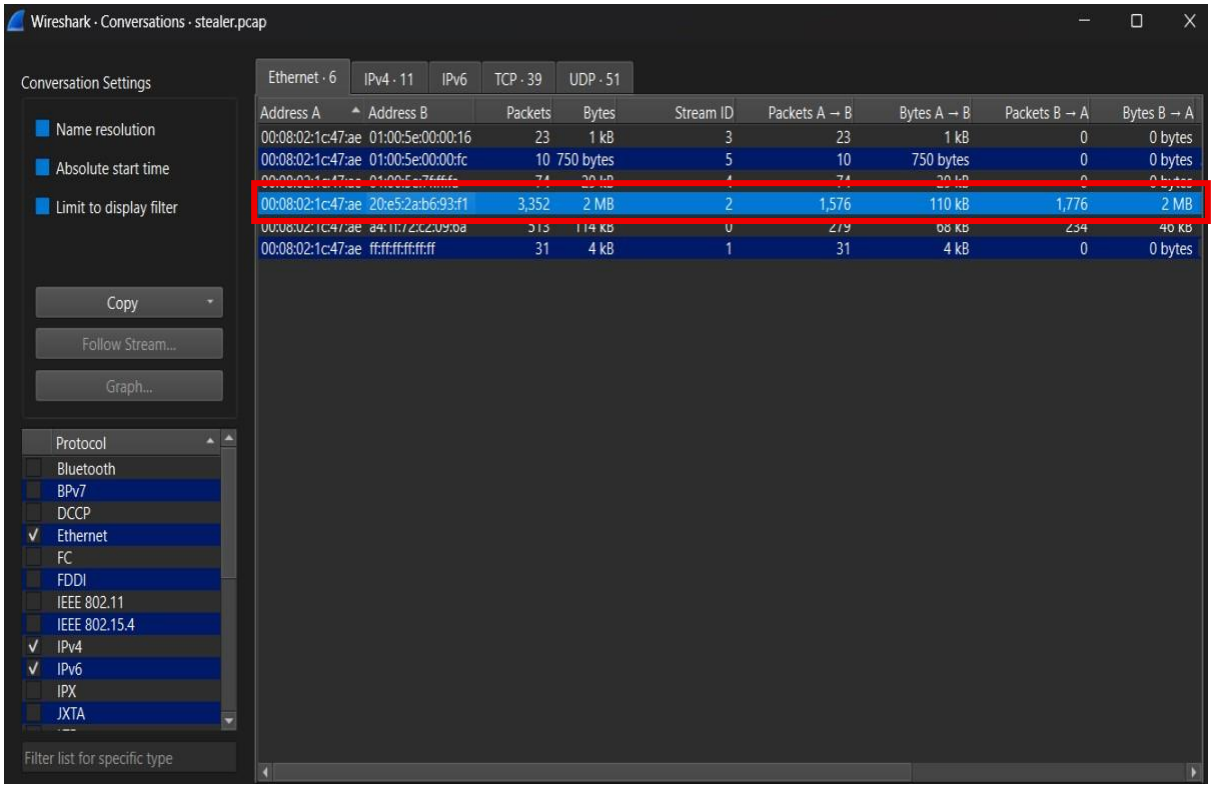
What is the duration of the capture?

01:03:41



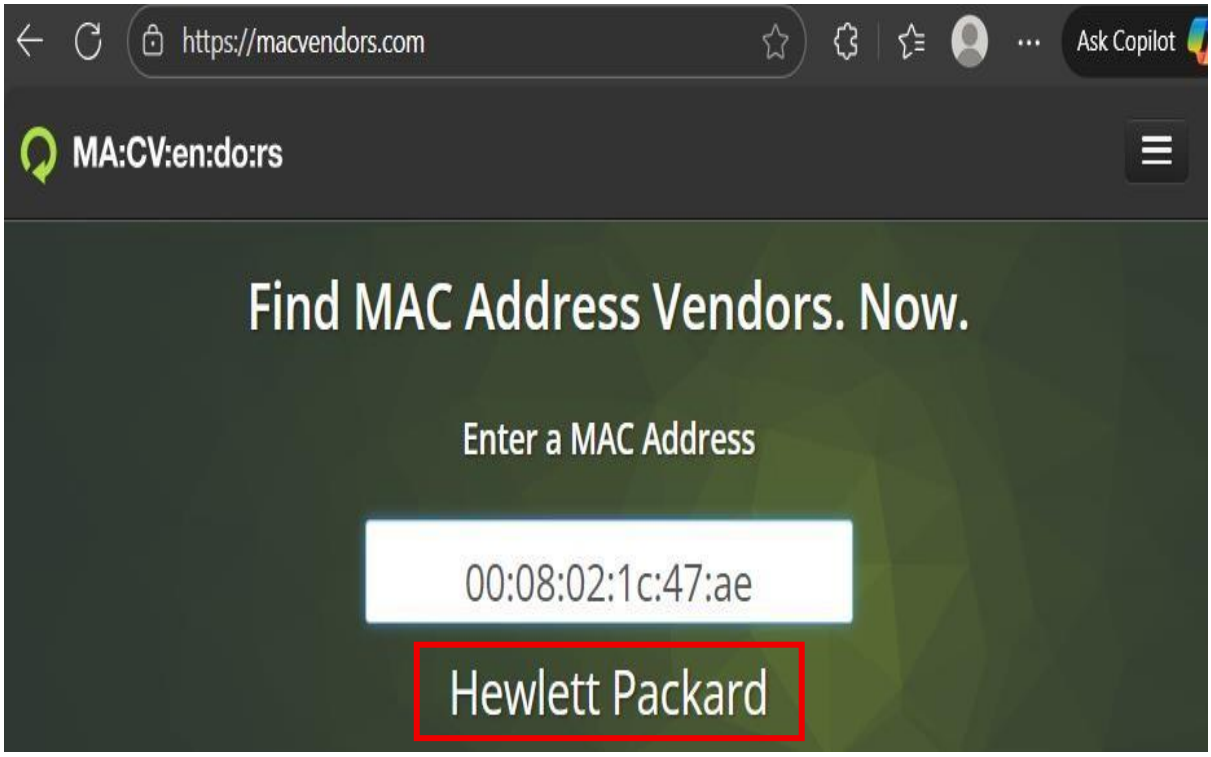
What is the most active computer at the link level?

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



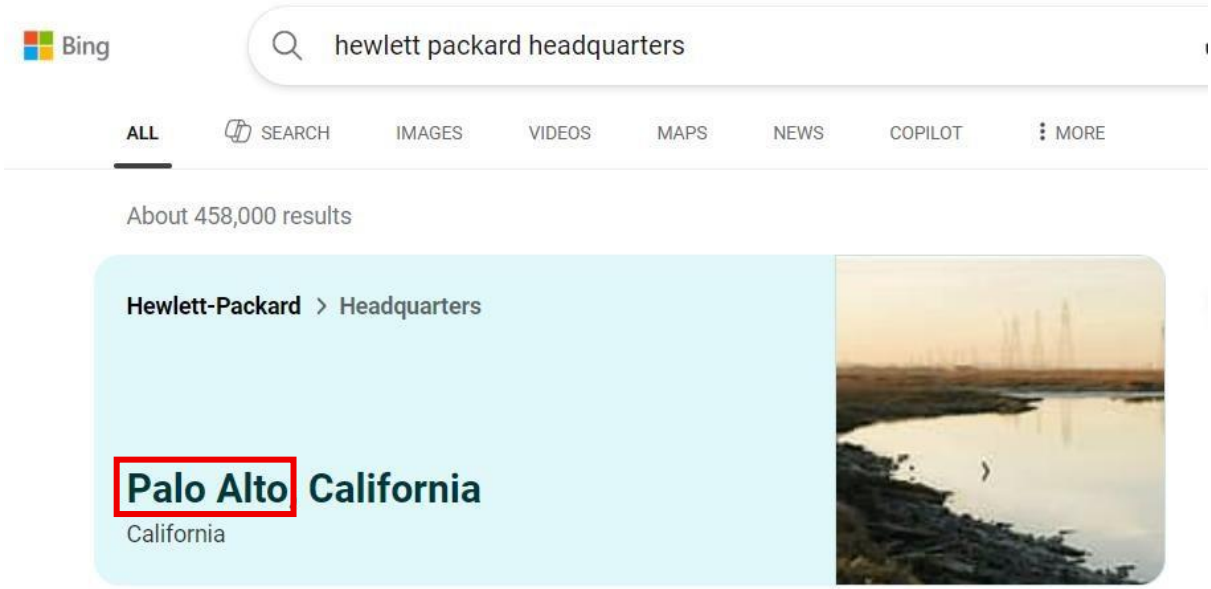
Manufacturer of the NIC of the most active system at the link level?

Hewlett-Packard



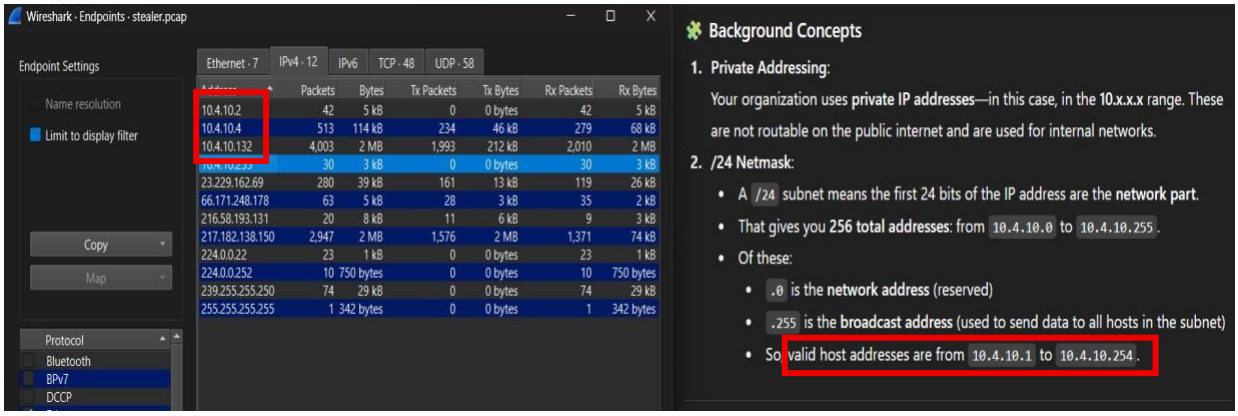
Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?

Pala Alto



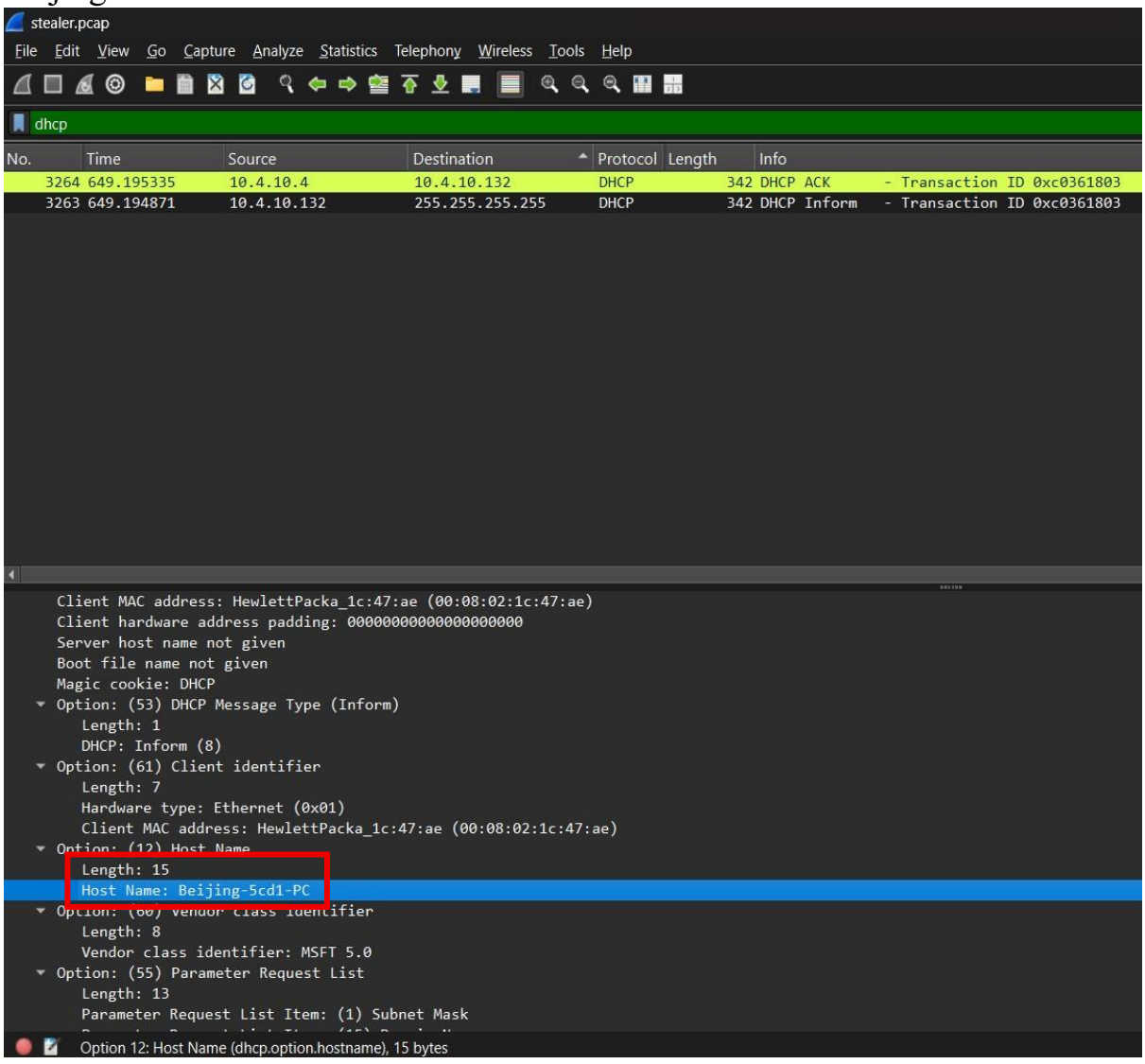
The organization works with private addressing and netmask /24. How many computers in the organization are involved in the capture?

3



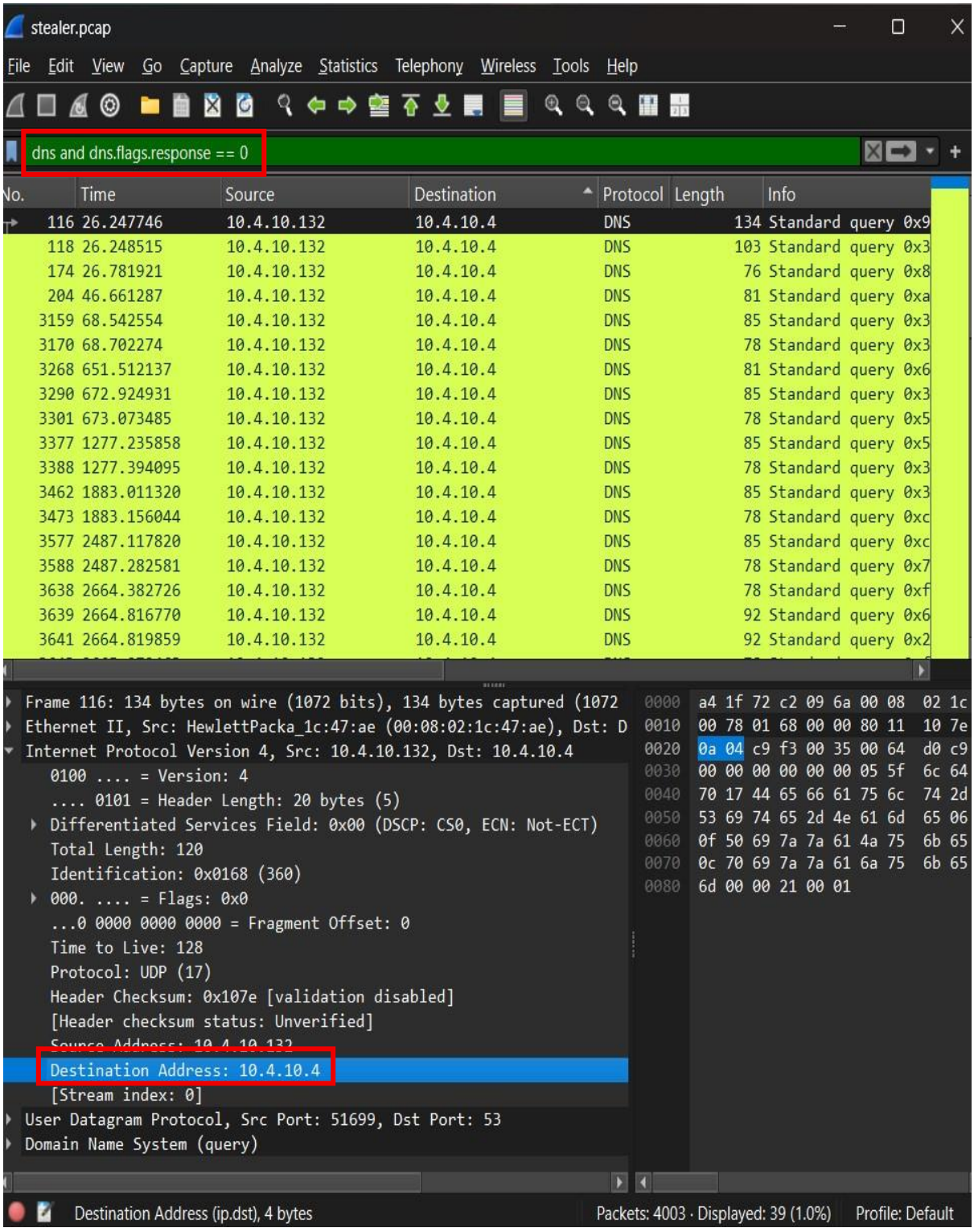
What is the name of the most active computer at the network level?

Beijing-5cd1-PC

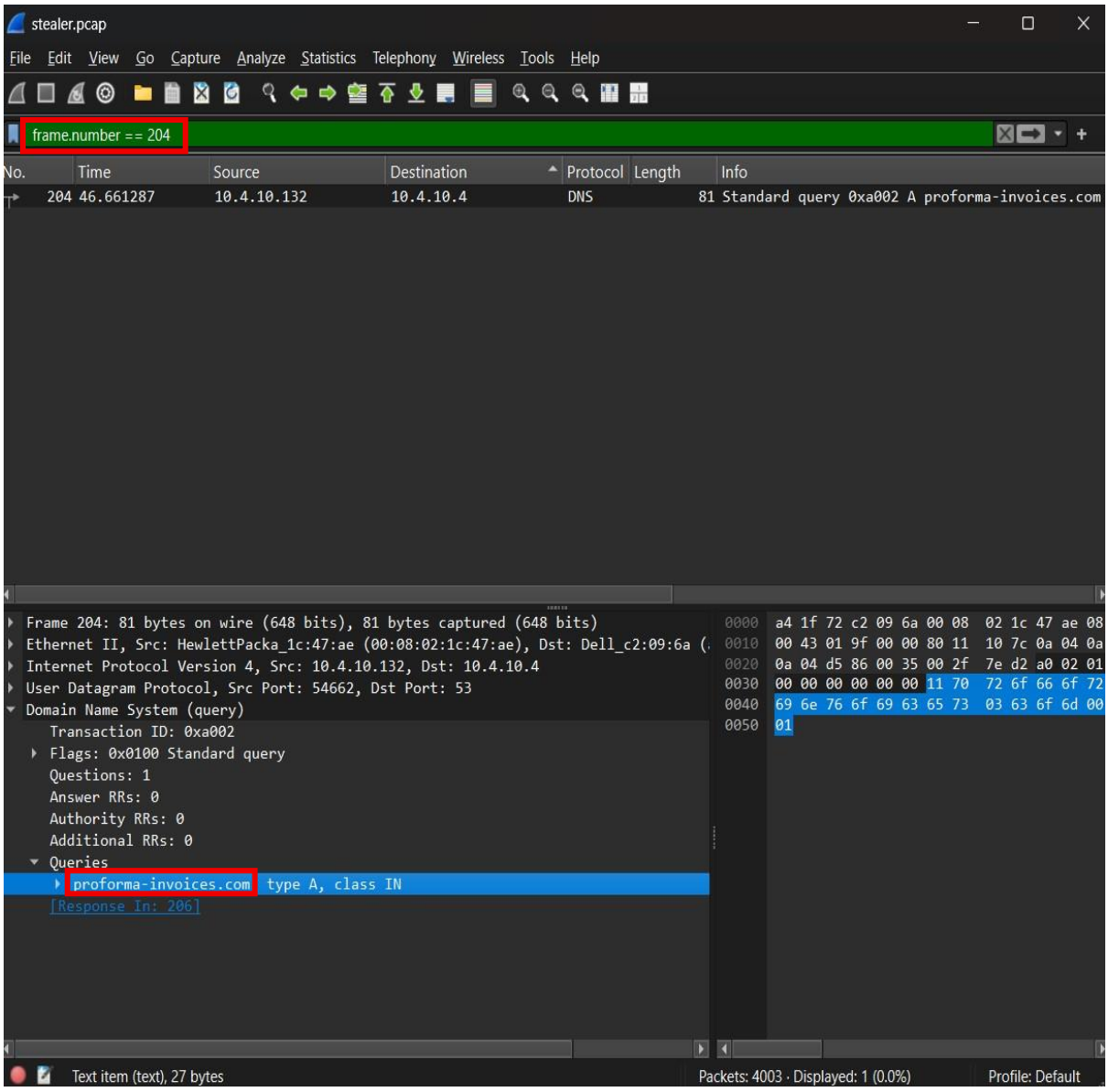


What is the IP of the organization's DNS server?

10.4.10.4

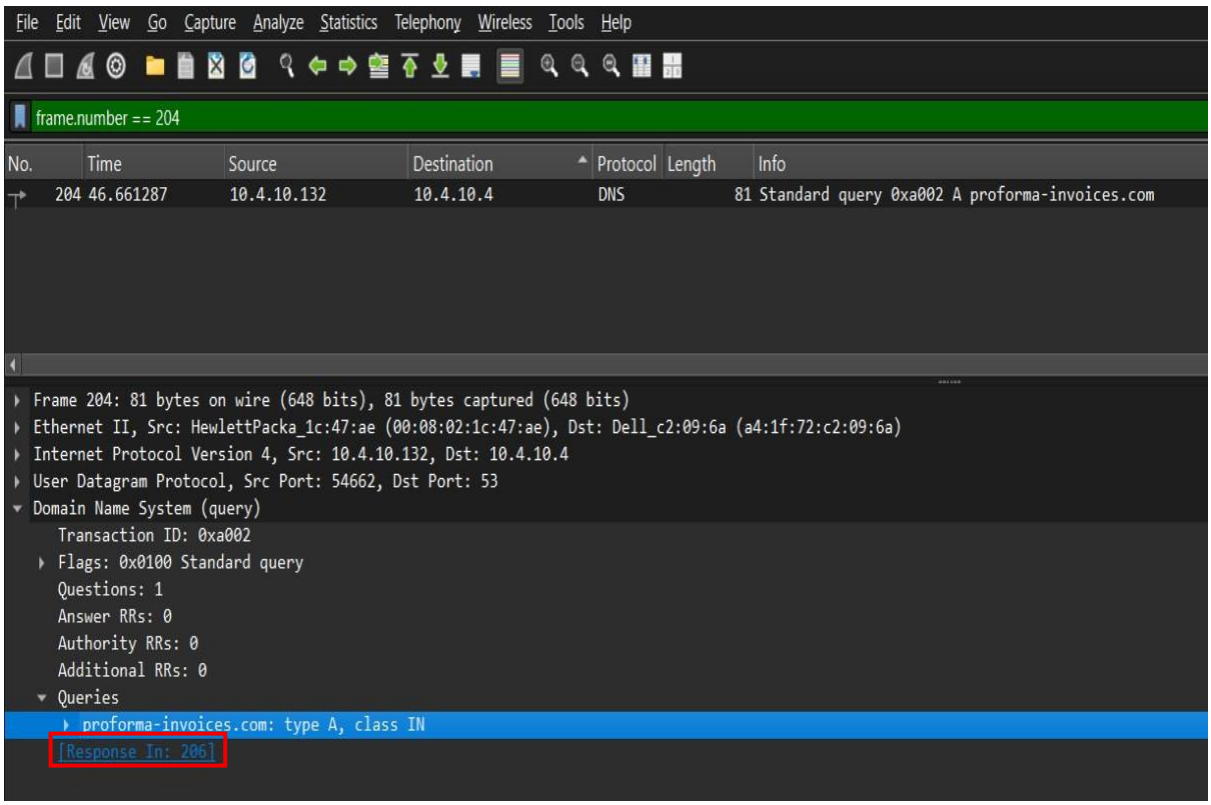


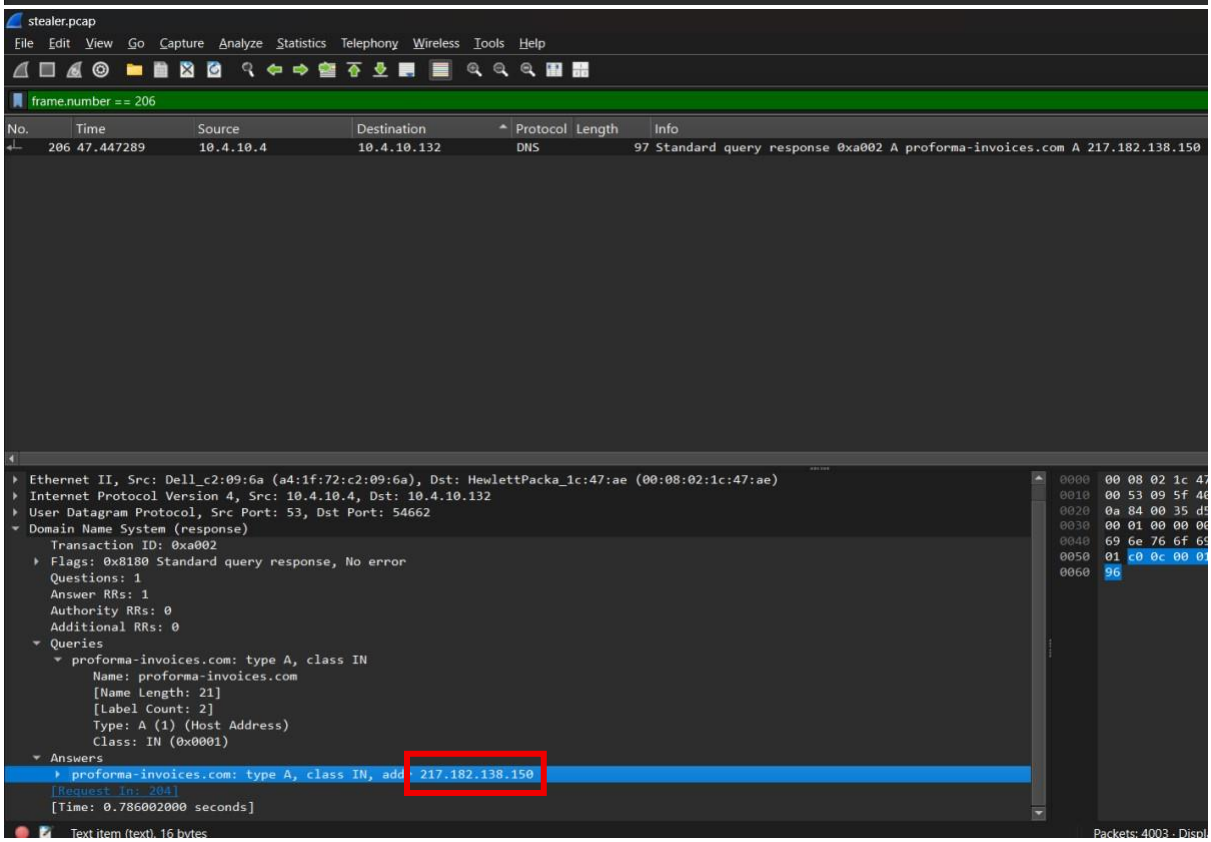
What domain is the victim asking about in packet 204? proforma-invoices.com



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

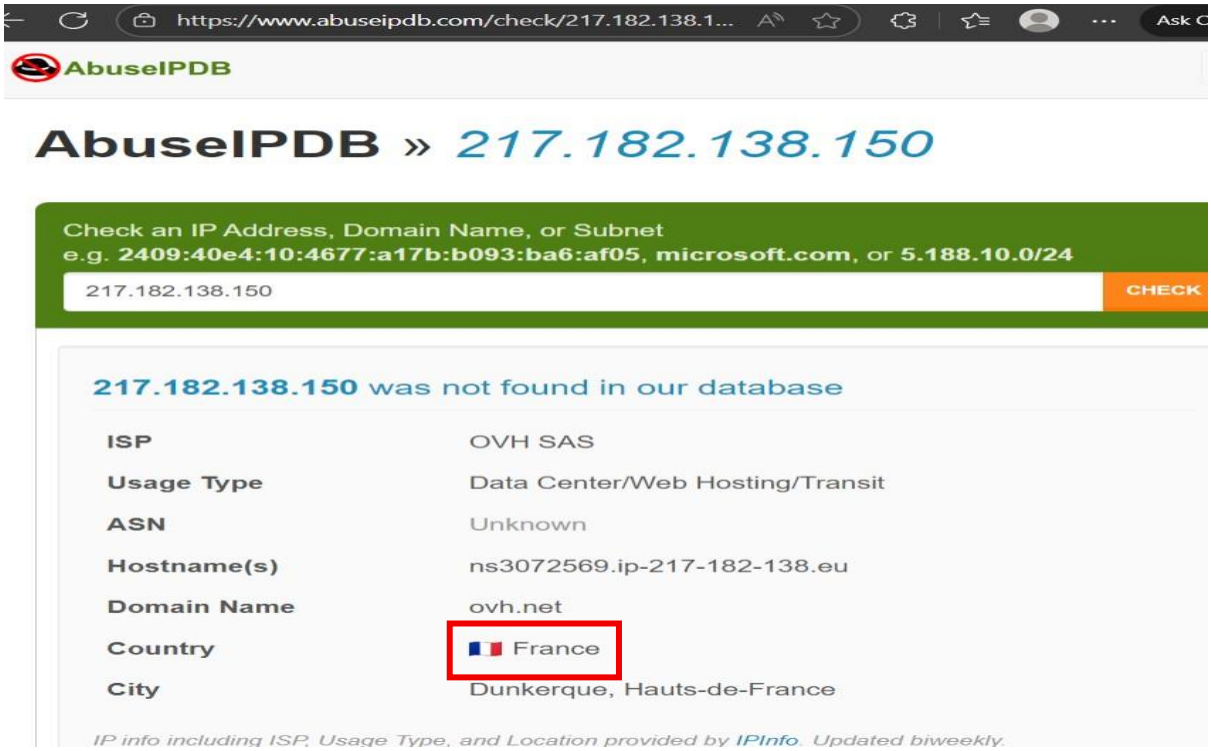
217.182.138.150





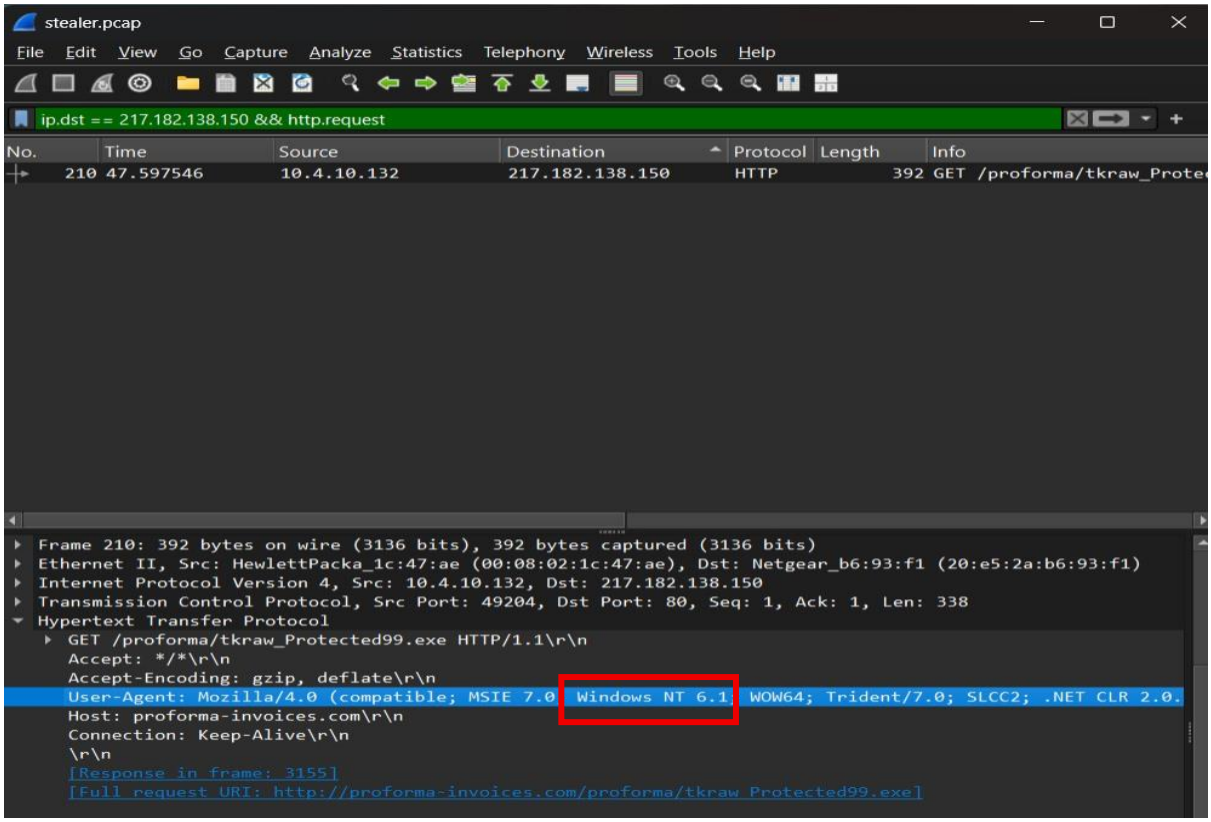
Indicate the country to which the IP in the previous section belongs.

France



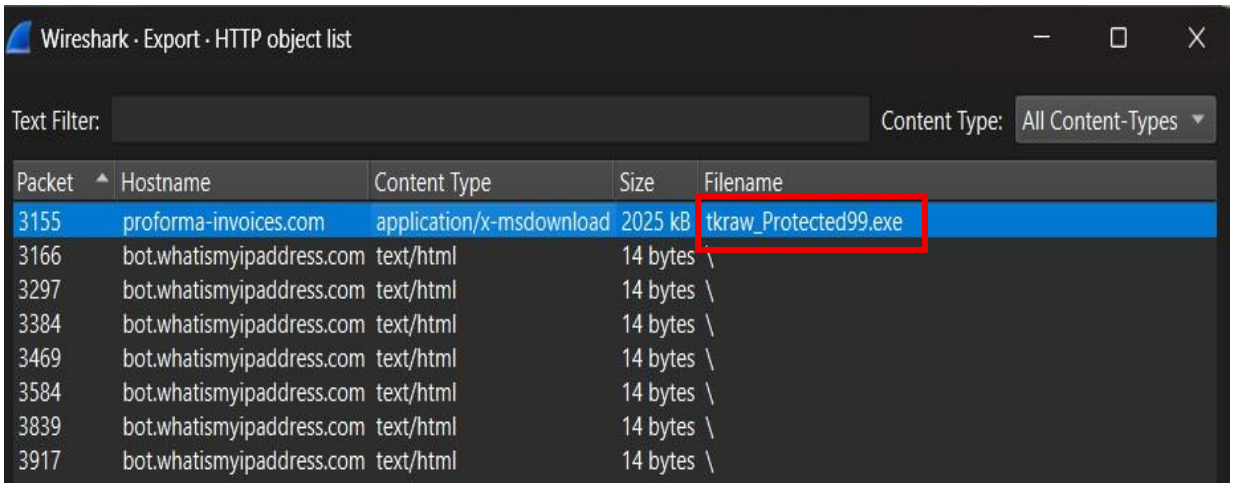
What operating system does the victim's computer run?

Windows NT 6.1



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

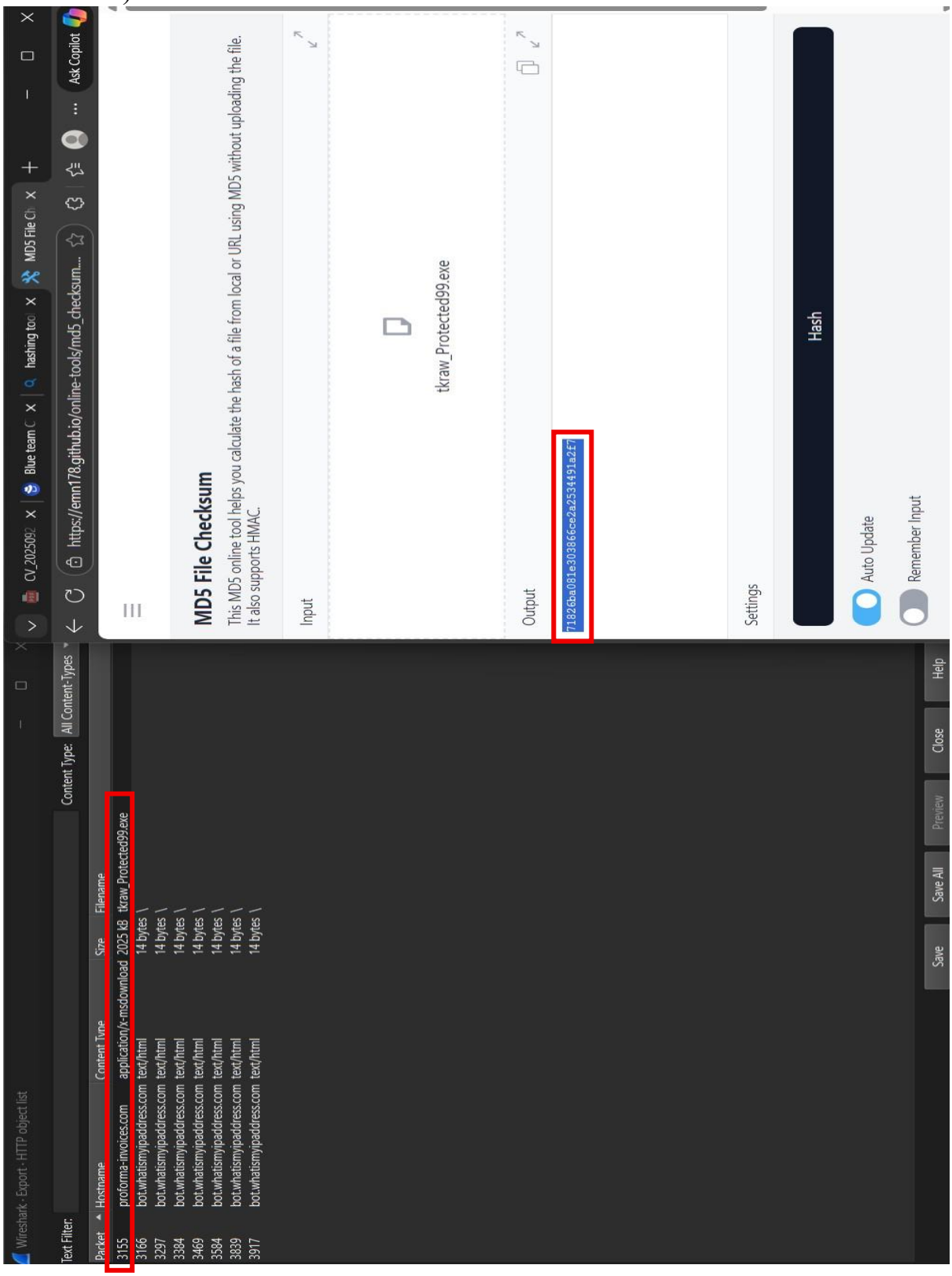
tkraw_Protected99.exe (Go to File > Export Objects > HTTP in Wireshark)



What is the md5 hash of the downloaded file?

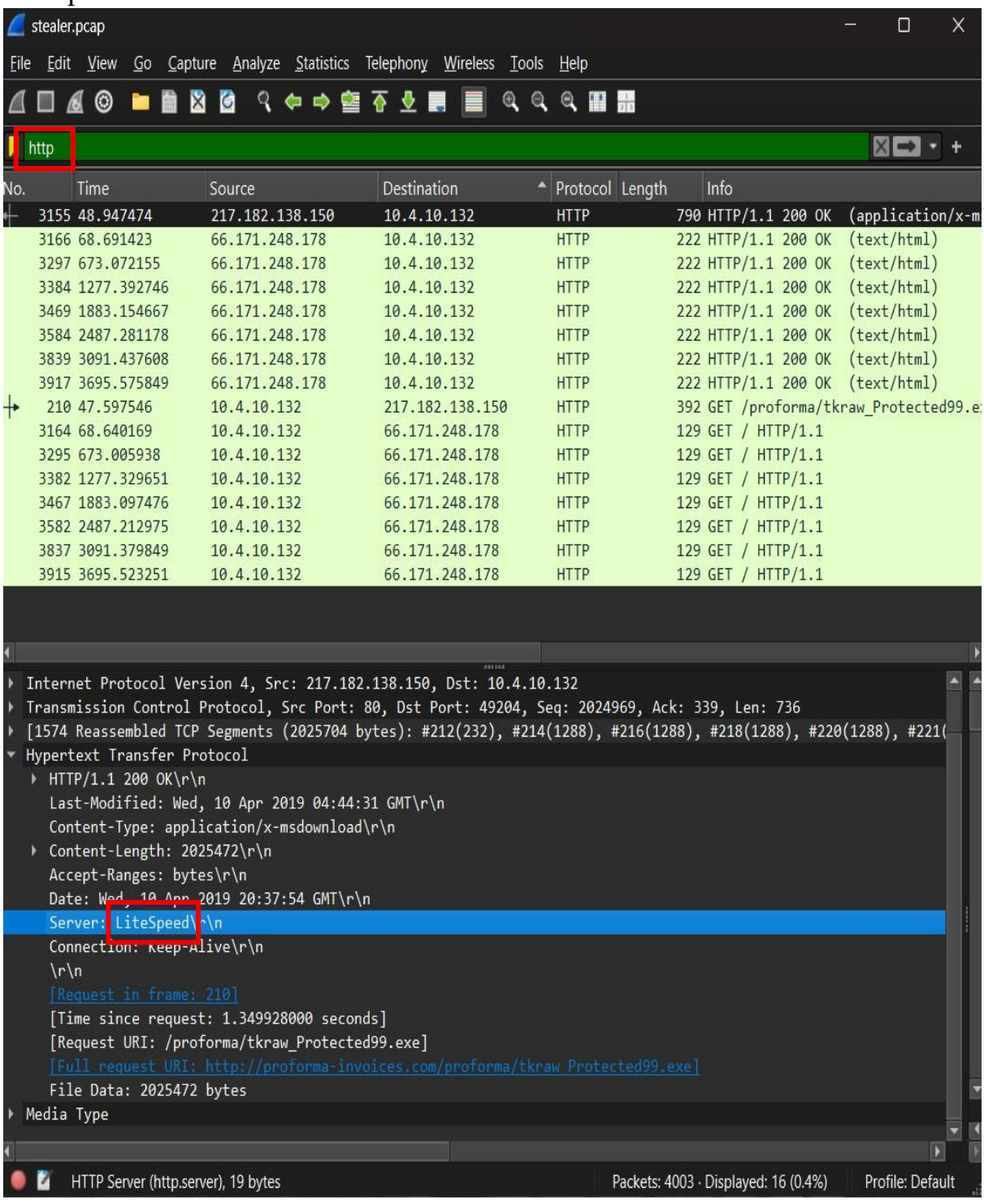
71826ba081e303866ce2a2534491a2f7

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



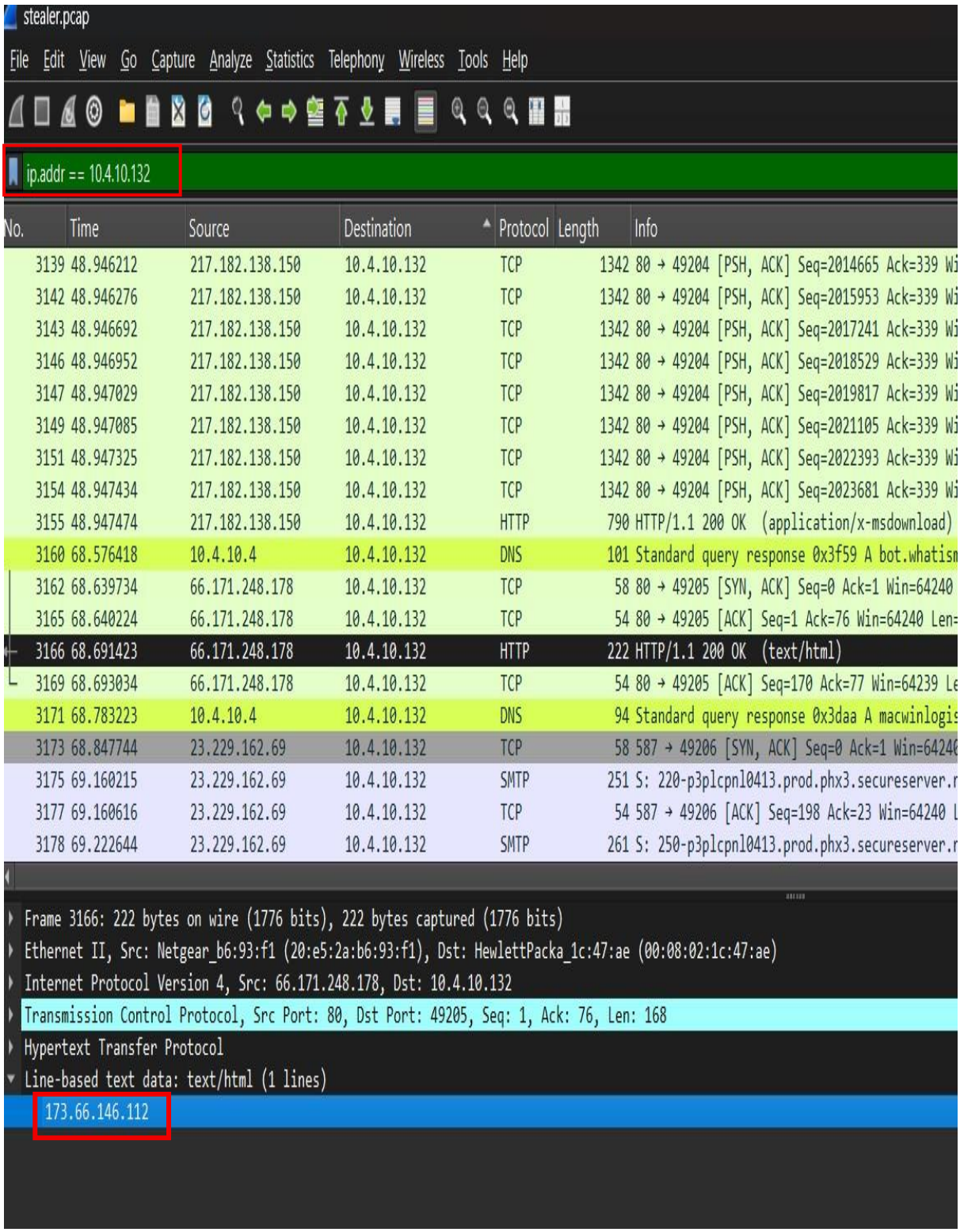
What software runs the webserver that hosts the malware?

LiteSpeed



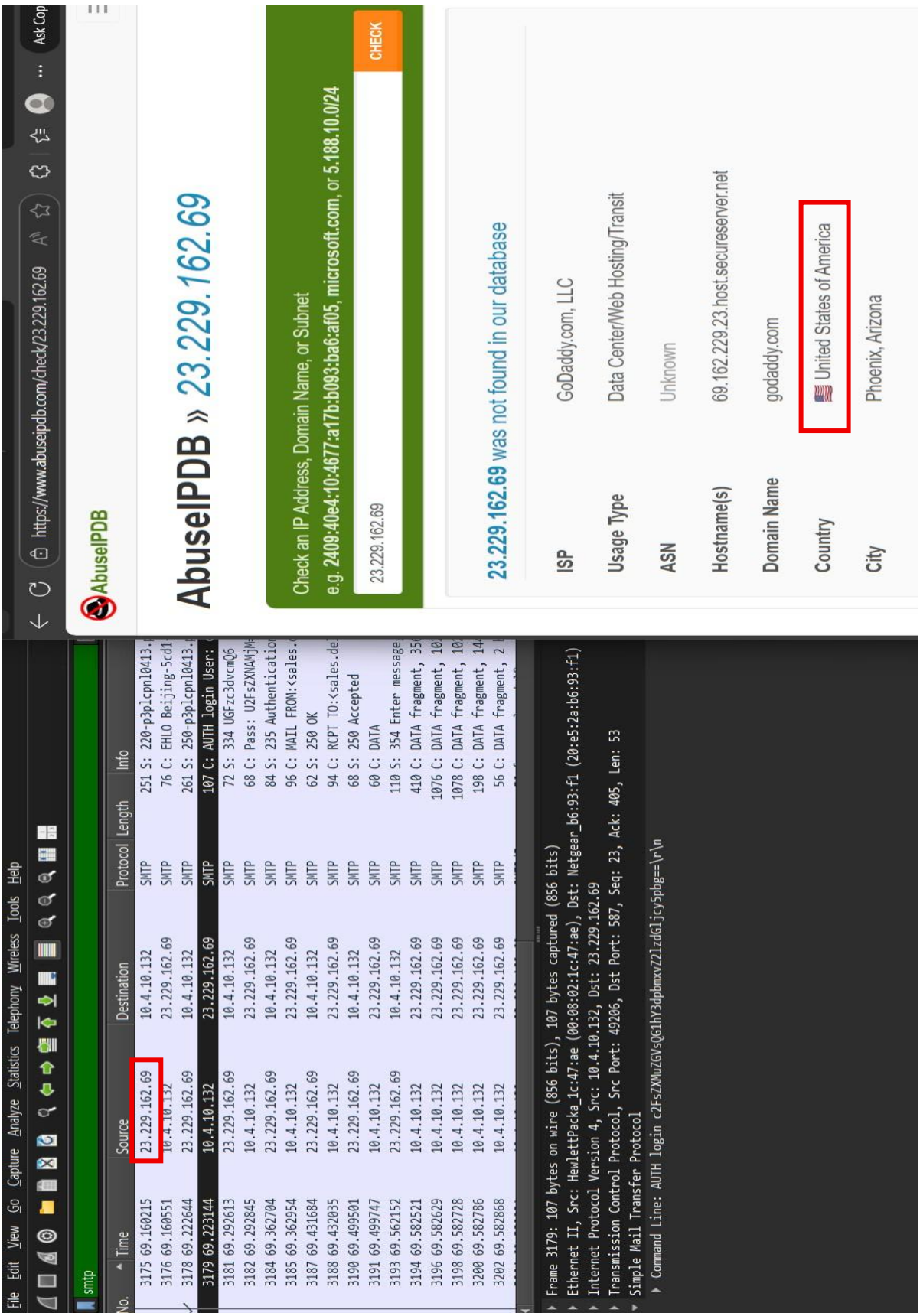
What is the public IP of the victim's computer?

173.66.146.112



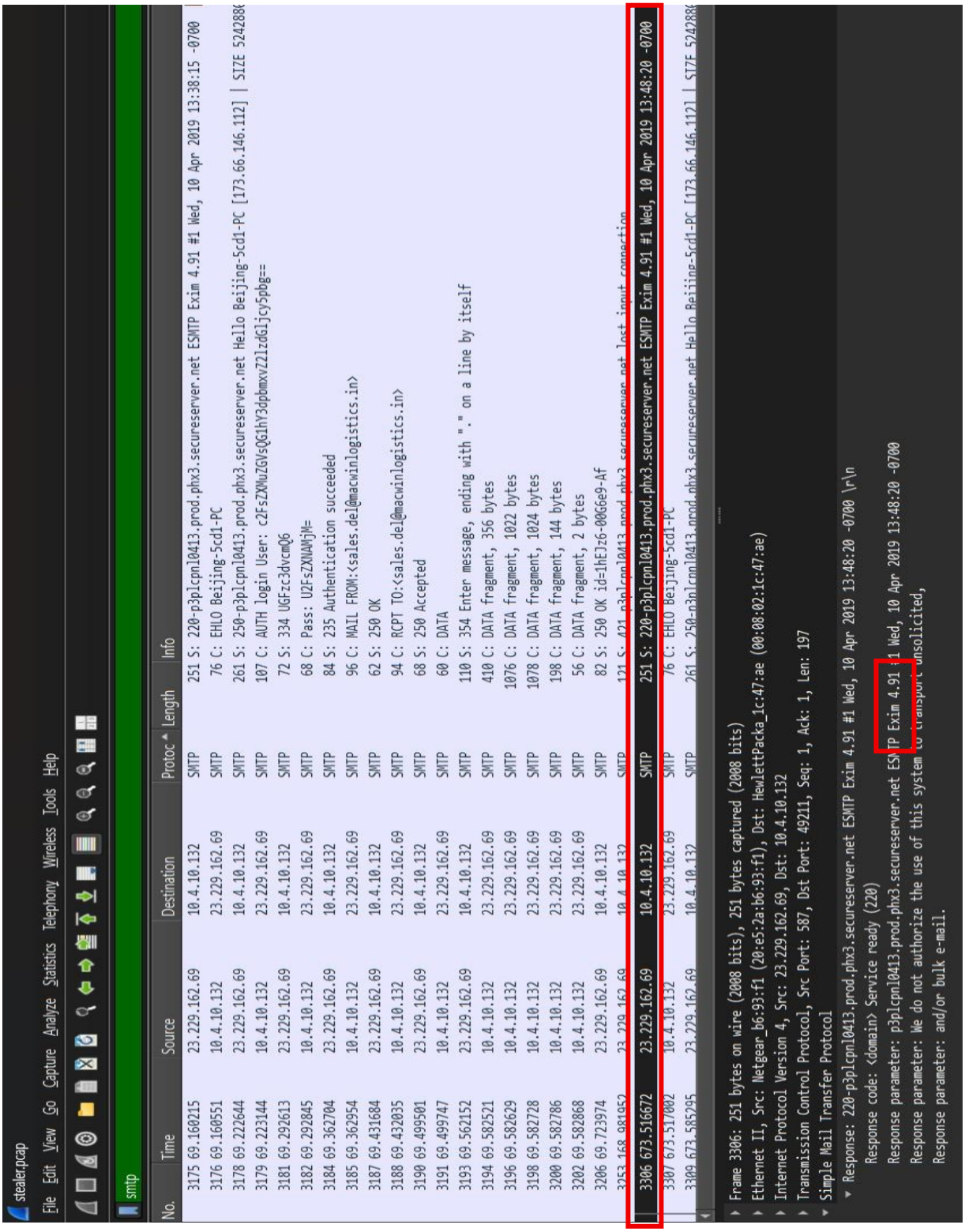
In which country is the email server to which the stolen information is sent?

United States



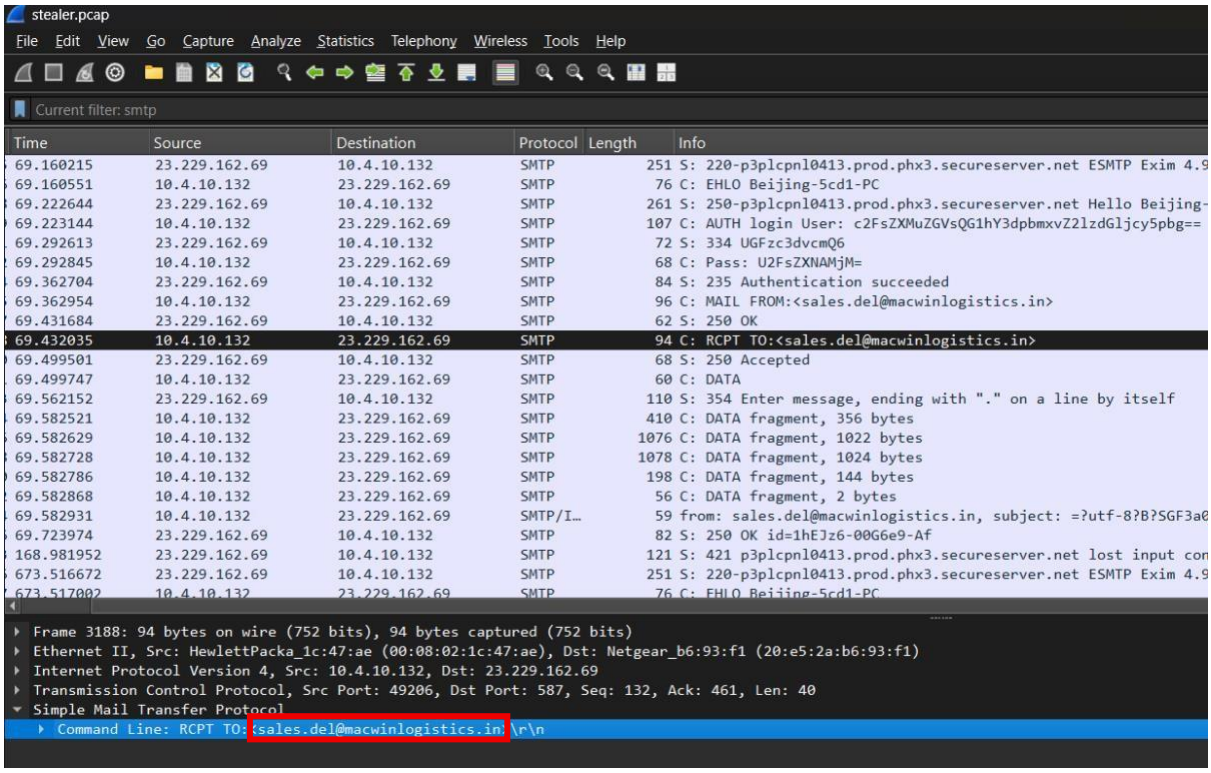
Analysing the first extraction of information. What software runs the email server to which the stolen data is sent?

EXIM 4.91



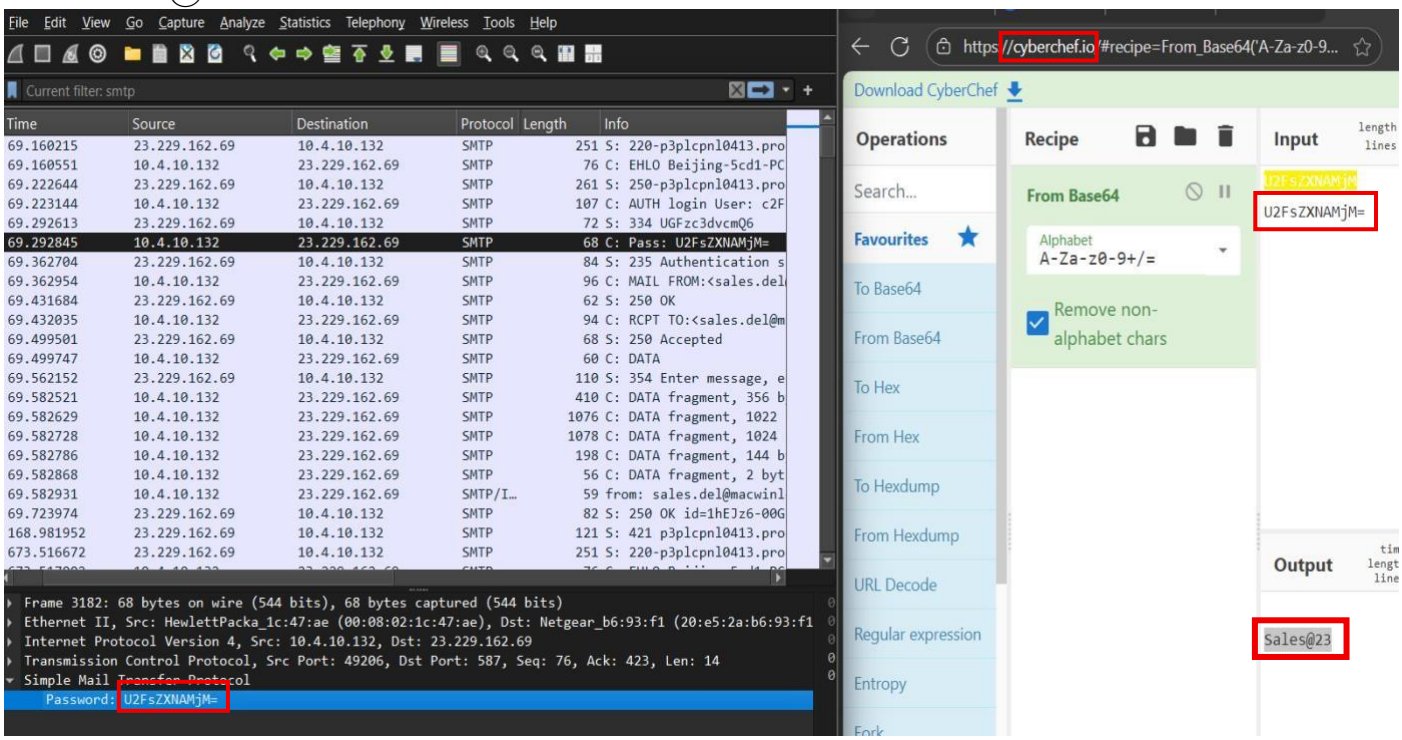
To which email account is the stolen information sent?

sales.del@macwinlogistics.in



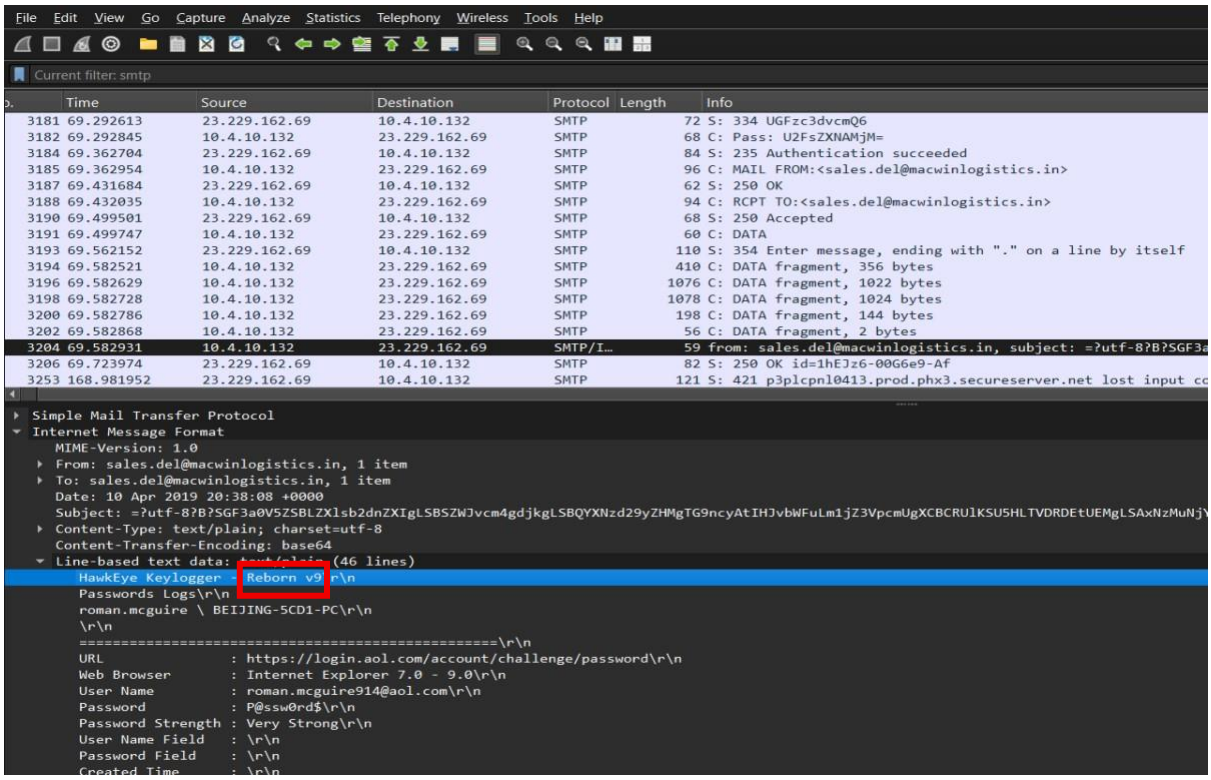
What is the password used by the malware to send the email?

sales@23



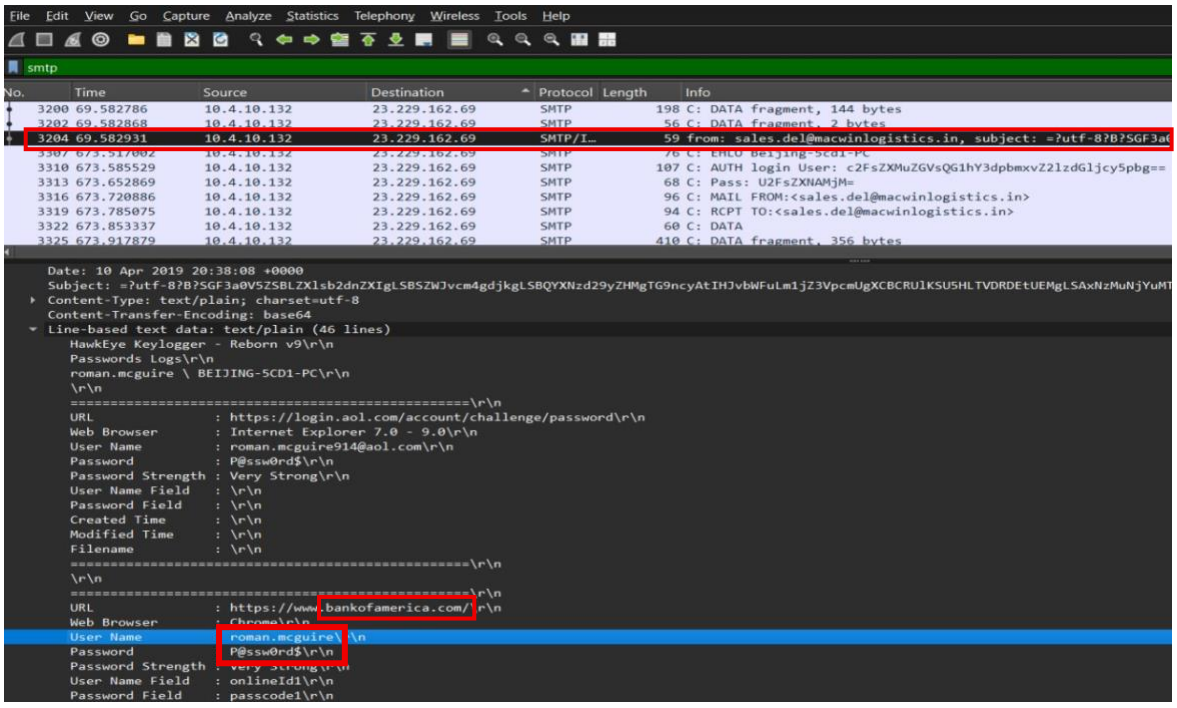
Which malware variant exfiltrated the data? reborn

v9



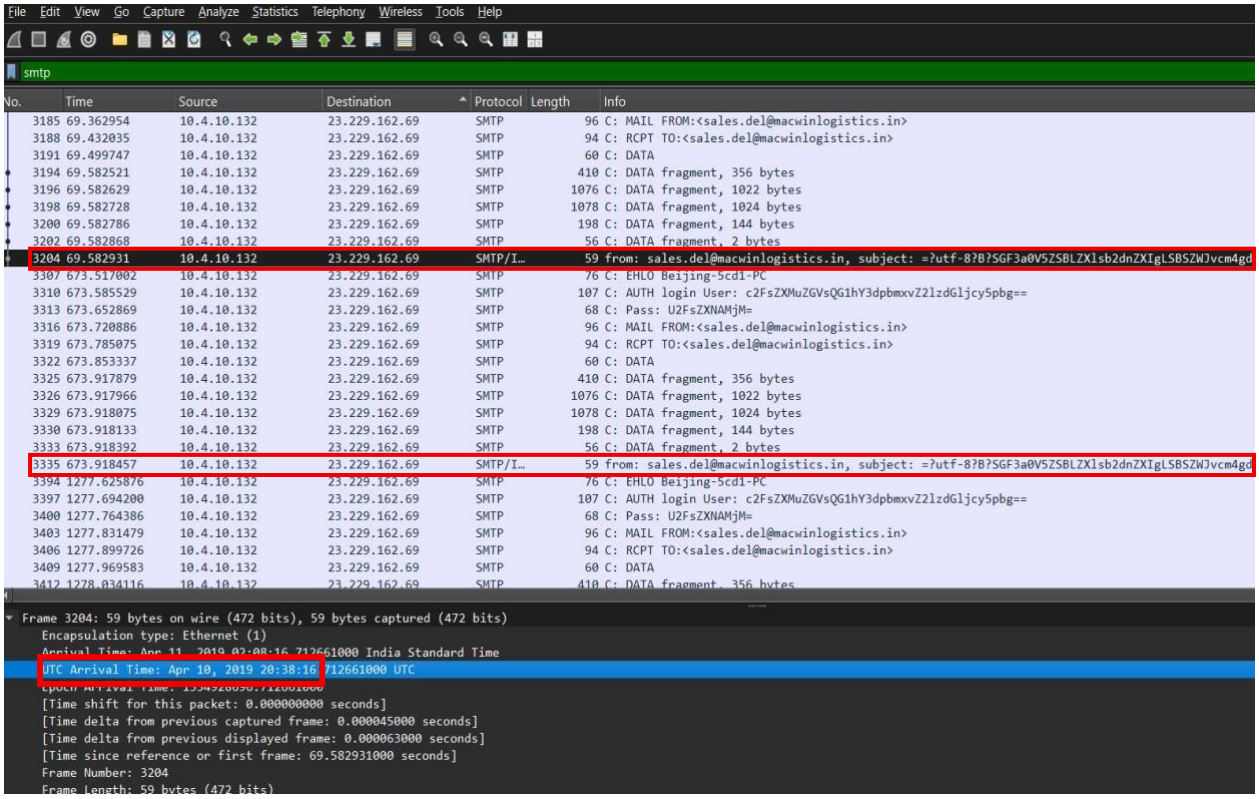
What are the bank of America access credentials? (username:password)

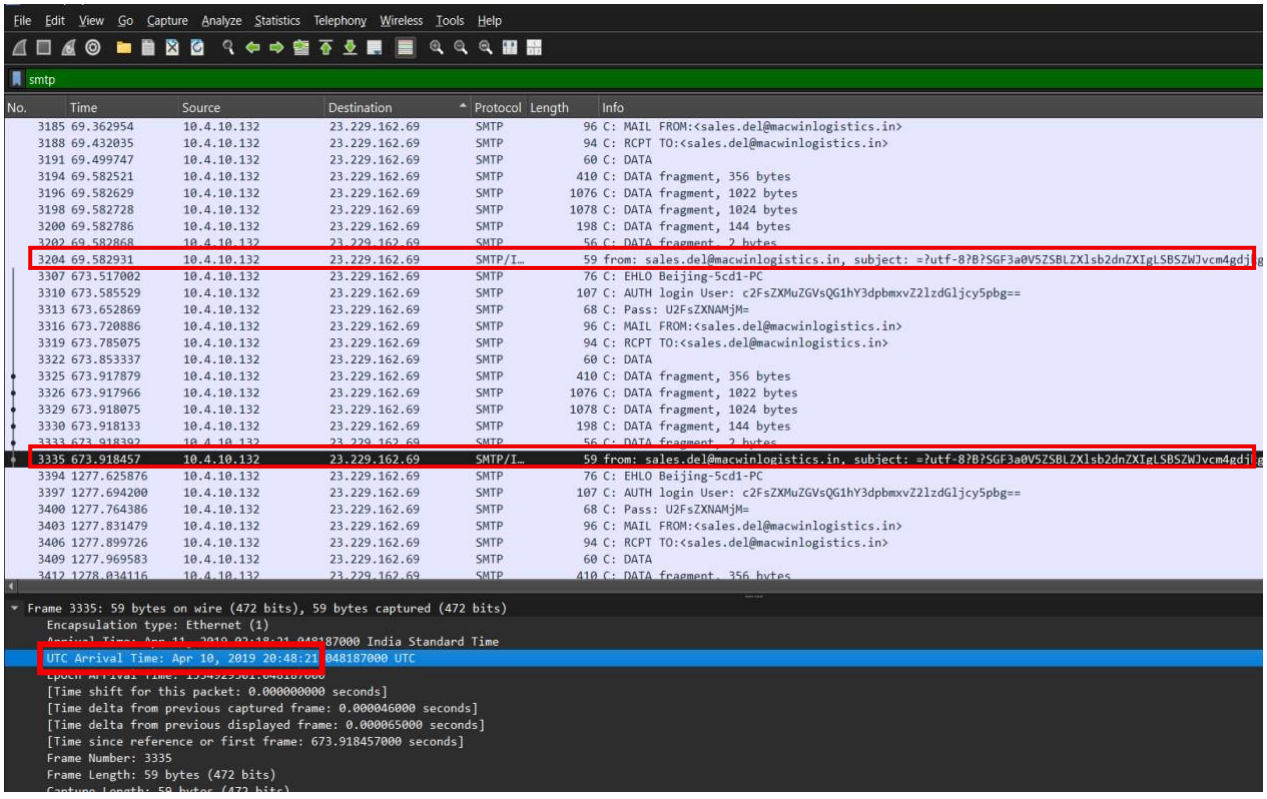
roman.mcguire:p@ssw0rd$



Every how many minutes does the collected data get exfiltrated?

10





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