Challenge: WireDive Lab

Platform: CyberDefenders

Category: Network Forensics

Difficulty: Medium

Tools Used: Wireshark

Summary: This lab involved investigating a series of PCAPs, covering a variety of different topics. In all honesty, this lab is great at practicing your Wireshark skills for a variety of protocols, other than that, it isn't that enjoyable. Nonetheless, I still recommend it, especially for those new to network forensics.

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.

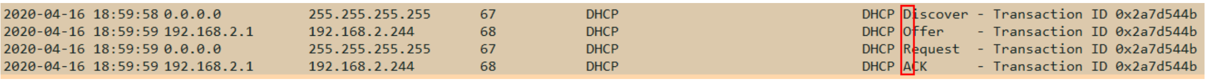
File: dhcp.pcapng

What IP address is requested by the client?

As a little refresher, Dynamic Host Configuration Protocol (DHCP) is used to automate assigning IP addresses and other configuration details to hosts within a network. Without DHCP, you would need to manually configure each device on a network. DHCP uses a four-step process called DORA (Discover, Offer, Request, and Acknowledge). A device sends a broadcast to find a DHCP server, the server offers an IP address and configuration settings, the device accepts the offer, and the server acknowledges the assignment, giving the device a temporary lease for the IP address.

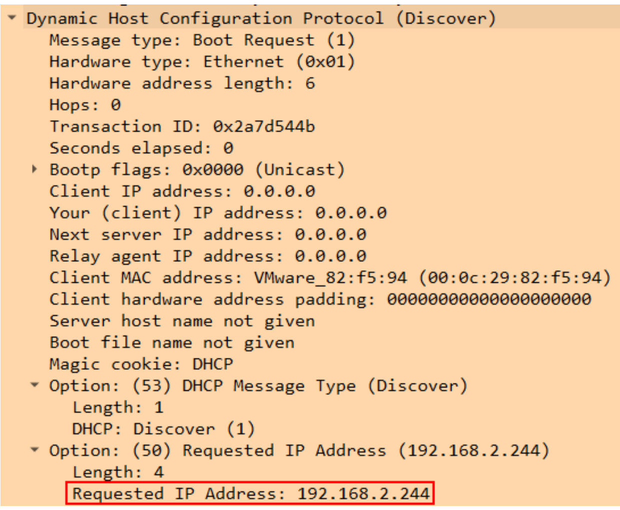
To find the IP requested by the client, we can use the following display filter:

- dhcp



```
2020-04-16 18:59:58 0.0.0.0         255.255.255.255    67          DHCP                                  DHCP Discover - Transaction ID 0x2a7d544b
2020-04-16 18:59:59 192.168.2.1     192.168.2.244      68          DHCP                                  DHCP Offer    - Transaction ID 0x2a7d544b
2020-04-16 18:59:59 0.0.0.0         255.255.255.255    67          DHCP                                  DHCP Request  - Transaction ID 0x2a7d544b
2020-04-16 18:59:59 192.168.2.1     192.168.2.244      68          DHCP                                  DHCP ACK      - Transaction ID 0x2a7d544b
```

If you view the DHCP Discover packet, we can see that the client requests 192.168.2.244:



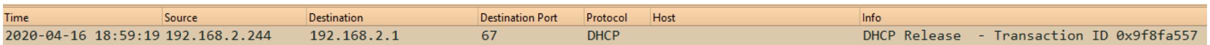
```
▾ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x2a7d544b
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: VMware_82:f5:94 (00:0c:29:82:f5:94)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
  ▾ Option: (50) Requested IP Address (192.168.2.244)
      Length: 4
      Requested IP Address: 192.168.2.244
```

Note! Make sure to expand the DHCP section in the packet details pane to find the answer.

Answer: 192.168.2.244

What is the transaction ID for the DHCP release?

Using the same dhcp display filter as before, we can see that packet number 176 is a DHCP Release packet, you can find the transaction ID within the info column as well as in the packet details pane:

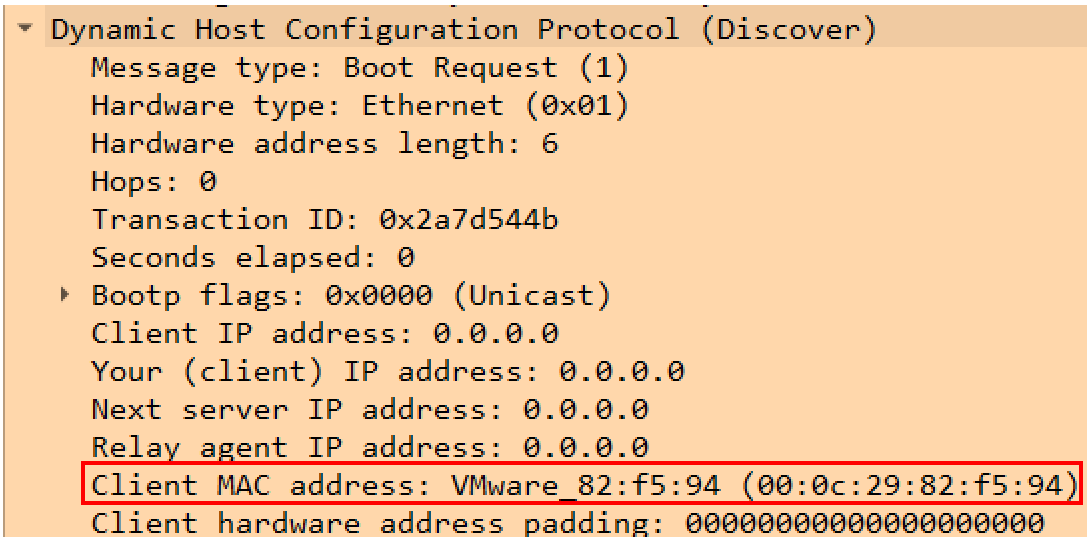


```
Time                Source         Destination    Destination Port  Protocol  Host                 Info
2020-04-16 18:59:19 192.168.2.244  192.168.2.1    67                DHCP                           DHCP Release  - Transaction ID 0x9f8fa557
```

Answer: 0x9f8fa557

What is the MAC address of the client?

If you look at any of the DHCP requests, you can find the client MAC address in the packet details pane:



```
▾ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x2a7d544b
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: VMware_82:f5:94 (00:0c:29:82:f5:94)
    Client hardware address padding: 00000000000000000000
```

Answer: 00:0c:29:82:f5:94

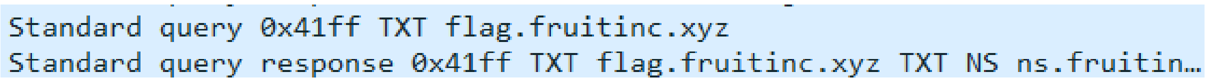
File: dns.pcapng

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

The Domain Name System (DNS) is responsible for resolving domain names, like google.com, to IP addresses like 172.253.63.100. To filter for DNS traffic within the pcap, we can use the following display filter:

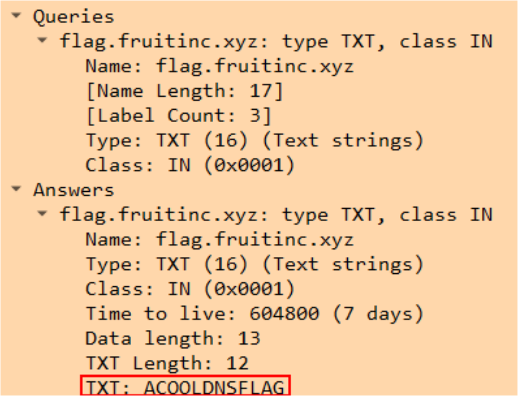
- dns

If you looking through the displayed packets, we can see a request being made to flag.fruitinc.xyz, followed by a response:



```
Standard query 0x41ff TXT flag.fruitinc.xyz
Standard query response 0x41ff TXT flag.fruitinc.xyz TXT NS ns.fruitin…
```

If you view the query response packet, you can find the answer given by the DNS server:



```
▾ Queries
  ▾ flag.fruitinc.xyz: type TXT, class IN
      Name: flag.fruitinc.xyz
      [Name Length: 17]
      [Label Count: 3]
      Type: TXT (16) (Text strings)
      Class: IN (0x0001)
▾ Answers
  ▾ flag.fruitinc.xyz: type TXT, class IN
      Name: flag.fruitinc.xyz
      Type: TXT (16) (Text strings)
      Class: IN (0x0001)
      Time to live: 604800 (7 days)
      Data length: 13
      TXT Length: 12
      TXT: ACOOLDNSFLAG
```

Answer: ACOOLDNSFLAG

Which root server responds to the google.com query? Hostname.

Answer: e.root-servers.net

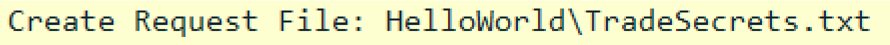
File: smb.pcapng

What is the path of the file that is opened?

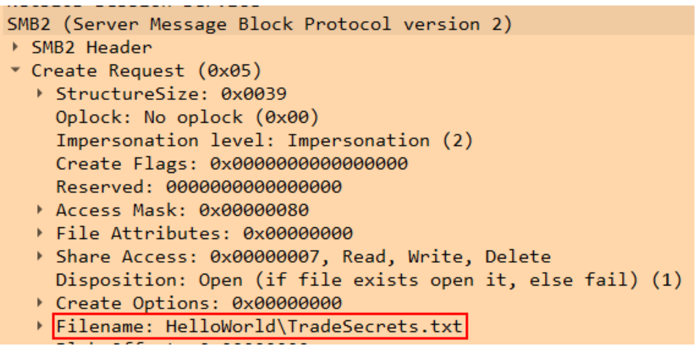
Create request file is a command sent by a client to a server to either create a new file or access an existing file over a network using SMB. We can look for this command using the following display filter:

- smb2.tree

If you view the packets, we can see that a file called TradeSecrets.txt is opened within the HelloWorld directory:

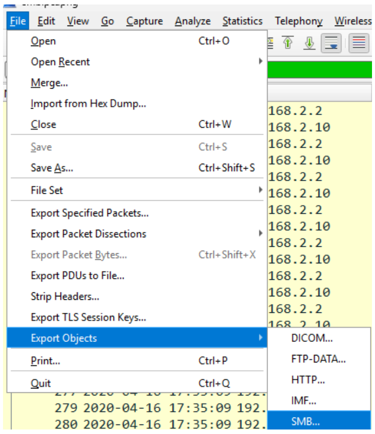


```
Create Request File: HelloWorld\TradeSecrets.txt
```



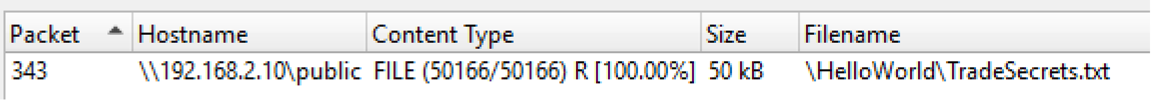
```
SMB2 (Server Message Block Protocol version 2)
 ▸ SMB2 Header
 ▾ Create Request (0x05)
   ▸ StructureSize: 0x0039
     Oplock: No oplock (0x00)
     Impersonation level: Impersonation (2)
     Create Flags: 0x0000000000000000
     Reserved: 0000000000000000
   ▸ Access Mask: 0x00000080
   ▸ File Attributes: 0x00000000
   ▸ Share Access: 0x00000007, Read, Write, Delete
     Disposition: Open (if file exists open it, else fail) (1)
   ▸ Create Options: 0x00000000
   ▸ Filename: HelloWorld\TradeSecrets.txt
```

Alternatively, if you navigate to File > Export Objects > SMB:



```
168.2.2
168.2.10
168.2.2
168.2.10
168.2.2
168.2.10
168.2.2
168.2.10
168.2.2
168.2.10
168.2.2
168.2.10
168.2.2
279 2020-04-16 17:35:09 192.
280 2020-04-16 17:35:09 192.
```

We can see that there is only one object extracted from the SMB traffic:



Packet	Hostname	Content Type	Size	Filename
343	\\192.168.2.10\public	FILE (50166/50166) R [100.00%]	50 kB	\HelloWorld\TradeSecrets.txt

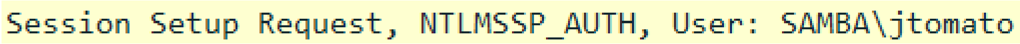
Answer: HelloWorld\TradeSecrets.txt

What was the hex status code when the user SAMBA\jtomato logs in?

Through using the following filter:

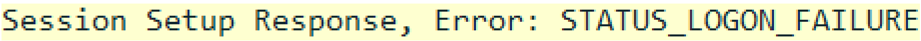
- smb or smb2

We can find the session setup request for SAMBA\jtomato:



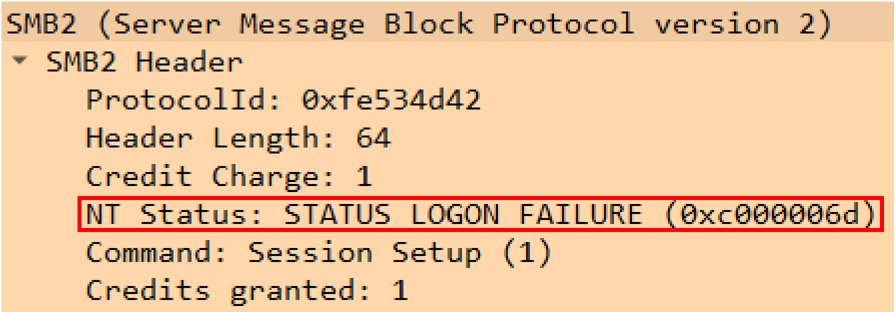
```
Session Setup Request, NTLMSSP_AUTH, User: SAMBA\jtomato
```

Following this request, there is a STATUS_LOGON_FAILURE response:



```
Session Setup Response, Error: STATUS_LOGON_FAILURE
```

If you view the packet details pane for this response, you can find the hex status code:



```
SMB2 (Server Message Block Protocol version 2)
▾ SMB2 Header
    ProtocolId: 0xfe534d42
    Header Length: 64
    Credit Charge: 1
    NT Status: STATUS_LOGON_FAILURE (0xc000006d)
    Command: Session Setup (1)
    Credits granted: 1
```

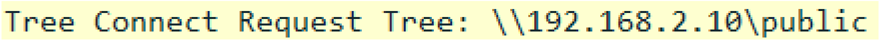
Answer: 0xc000006d

What is the tree that is being browsed?

In SMB, a tree is essentially a session-level connection to a specific share on the server. If you use the following display filter:

- smb2.tree

We can see a tree connection requesting being made to \\192.168.2.10\public:

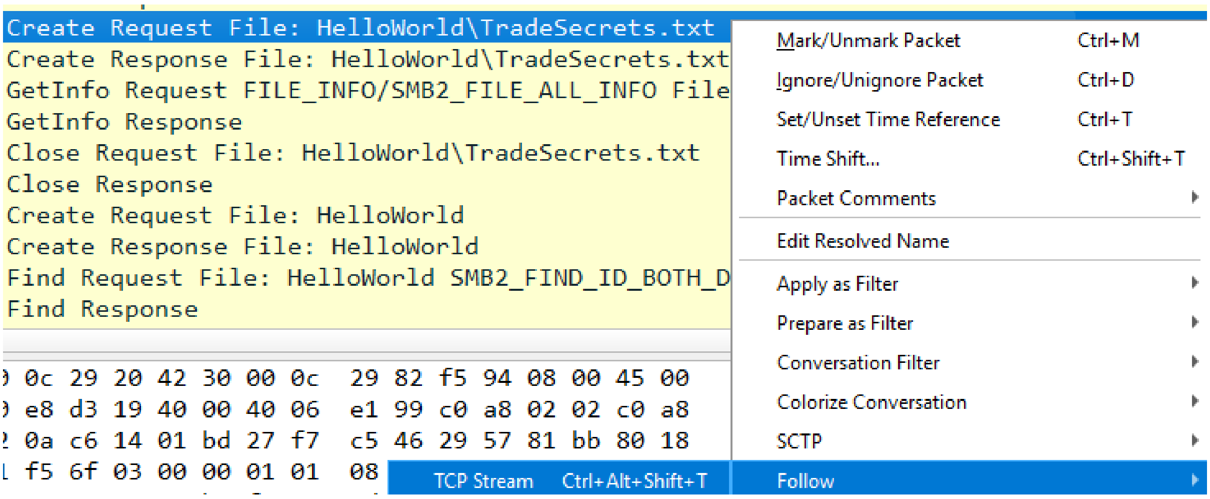


```
Tree Connect Request Tree: \\192.168.2.10\public
```

Answer: \\192.168.2.10\public

What is the flag in the file?

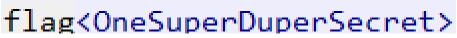
There are multiple ways to approach this. Firstly, we can view the TCP stream when the TradeSecrets.txt file is viewed:



```
Create Request File: HelloWorld\TradeSecrets.txt
Create Response File: HelloWorld\TradeSecrets.txt
GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File
GetInfo Response
Close Request File: HelloWorld\TradeSecrets.txt
Close Response
Create Request File: HelloWorld
Create Response File: HelloWorld
Find Request File: HelloWorld SMB2_FIND_ID_BOTH_D
Find Response

) 0c 29 20 42 30 00 0c  29 82 f5 94 08 00 45 00
) e8 d3 19 40 00 40 06  e1 99 c0 a8 02 02 c0 a8
! 0a c6 14 01 bd 27 f7  c5 46 29 57 81 bb 80 18
L f5 6f 03 00 00 01 01  08
```

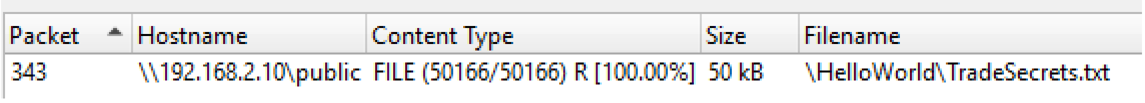
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
TCP Stream Ctrl+Alt+Shift+T

If you search for the string “flag”, we can find it within the TCP stream:



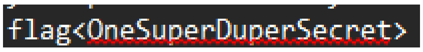
```
flag<OneSuperDuperSecret>
```

Alternatively, you can export the object by navigating to File > Export Objects > SMB:



Packet	Hostname	Content Type	Size	Filename
343	\\192.168.2.10\public	FILE (50166/50166) R [100.00%]	50 kB	\HelloWorld\TradeSecrets.txt

You can then view the txt file using a tool like notepad to find the flag:



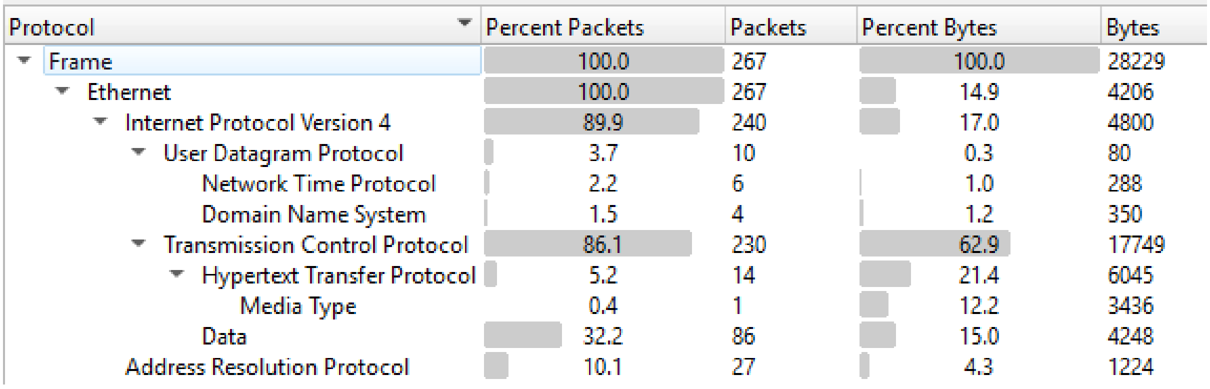
```
flag<OneSuperDuperSecret>
```

Answer: OneSuperDuperSecret

File: shell.pcapng

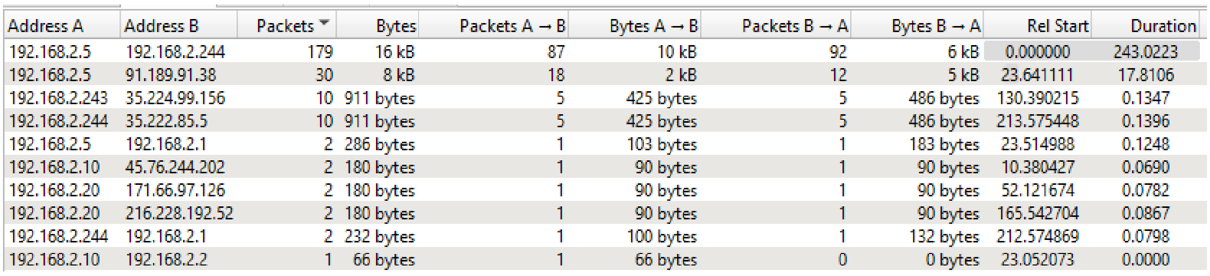
What port is the shell listening on?

To start, I’m going to navigate to Statistics > Protocol Hierarchy to get an idea of the sort of traffic within this PCAP:



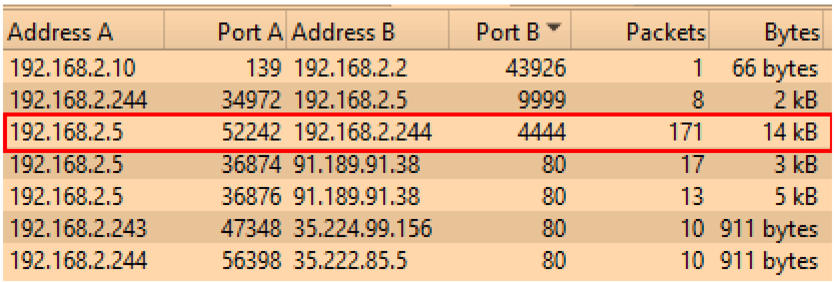
Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	267	100.0	28229
Ethernet	100.0	267	14.9	4206
Internet Protocol Version 4	89.9	240	17.0	4800
User Datagram Protocol	3.7	10	0.3	80
Network Time Protocol	2.2	6	1.0	288
Domain Name System	1.5	4	1.2	350
Transmission Control Protocol	86.1	230	62.9	17749
Hypertext Transfer Protocol	5.2	14	21.4	6045
Media Type	0.4	1	12.2	3436
Data	32.2	86	15.0	4248
Address Resolution Protocol	10.1	27	4.3	1224

I am also going to navigate to Statistics > Conversations > IPv4 to get an idea of the hosts within this PCAP:



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.2.5	192.168.2.244	179	16 kB	87	10 kB	92	6 kB	0.000000	243.0223
192.168.2.5	91.189.91.38	30	8 kB	18	2 kB	12	5 kB	23.641111	17.8106
192.168.2.243	35.224.99.156	10	911 bytes	5	425 bytes	5	486 bytes	130.390215	0.1347
192.168.2.244	35.222.85.5	10	911 bytes	5	425 bytes	5	486 bytes	213.575448	0.1396
192.168.2.5	192.168.2.1	2	286 bytes	1	103 bytes	1	183 bytes	23.514988	0.1248
192.168.2.10	45.76.244.202	2	180 bytes	1	90 bytes	1	90 bytes	10.380427	0.0690
192.168.2.20	171.66.97.126	2	180 bytes	1	90 bytes	1	90 bytes	52.121674	0.0782
192.168.2.20	216.228.192.52	2	180 bytes	1	90 bytes	1	90 bytes	165.542704	0.0867
192.168.2.244	192.168.2.1	2	232 bytes	1	100 bytes	1	132 bytes	212.574869	0.0798
192.168.2.10	192.168.2.2	1	66 bytes	1	66 bytes	0	0 bytes	23.052073	0.0000

This first conversation stands out due to its long duration relative to other conversations and the total number of packets sent. If you navigate to the TCP tab, we can also see that the destination port for this conversation is 4444, which is a very common listening port:

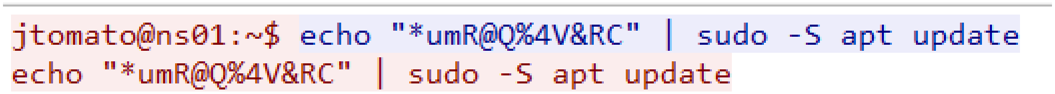


Address A	Port A	Address B	Port B	Packets	Bytes
192.168.2.10	139	192.168.2.2	43926	1	66 bytes
192.168.2.244	34972	192.168.2.5	9999	8	2 kB
192.168.2.5	52242	192.168.2.244	4444	171	14 kB
192.168.2.5	36874	91.189.91.38	80	17	3 kB
192.168.2.5	36876	91.189.91.38	80	13	5 kB
192.168.2.243	47348	35.224.99.156	80	10	911 bytes
192.168.2.244	56398	35.222.85.5	80	10	911 bytes

Using the following display filter, we can inspect the traffic for this suspicious conversation:

- ip.addr==192.168.2.5 && ip.addr==192.168.2.244

If you follow the TCP stream, we can immediately see commands being executed by:



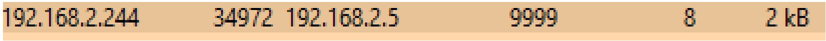
```
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S apt update
echo "*umR@Q%4V&RC" | sudo -S apt update
```

In this instance, 192.168.2.5 is the client/threat actor that is attempting to connect to 192.168.2.244 on port 4444.

Answer: 4444

What is the port for the second shell?

Another destination port that really stands out is 9999:

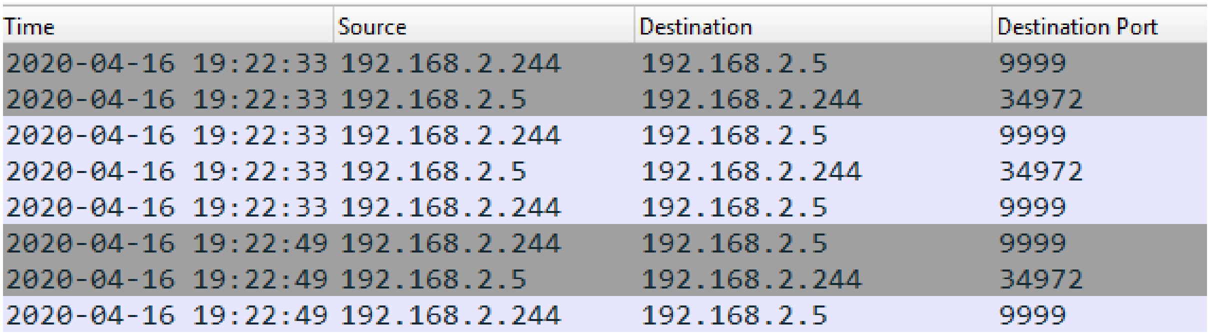


192.168.2.244	34972	192.168.2.5	9999	8	2 kB

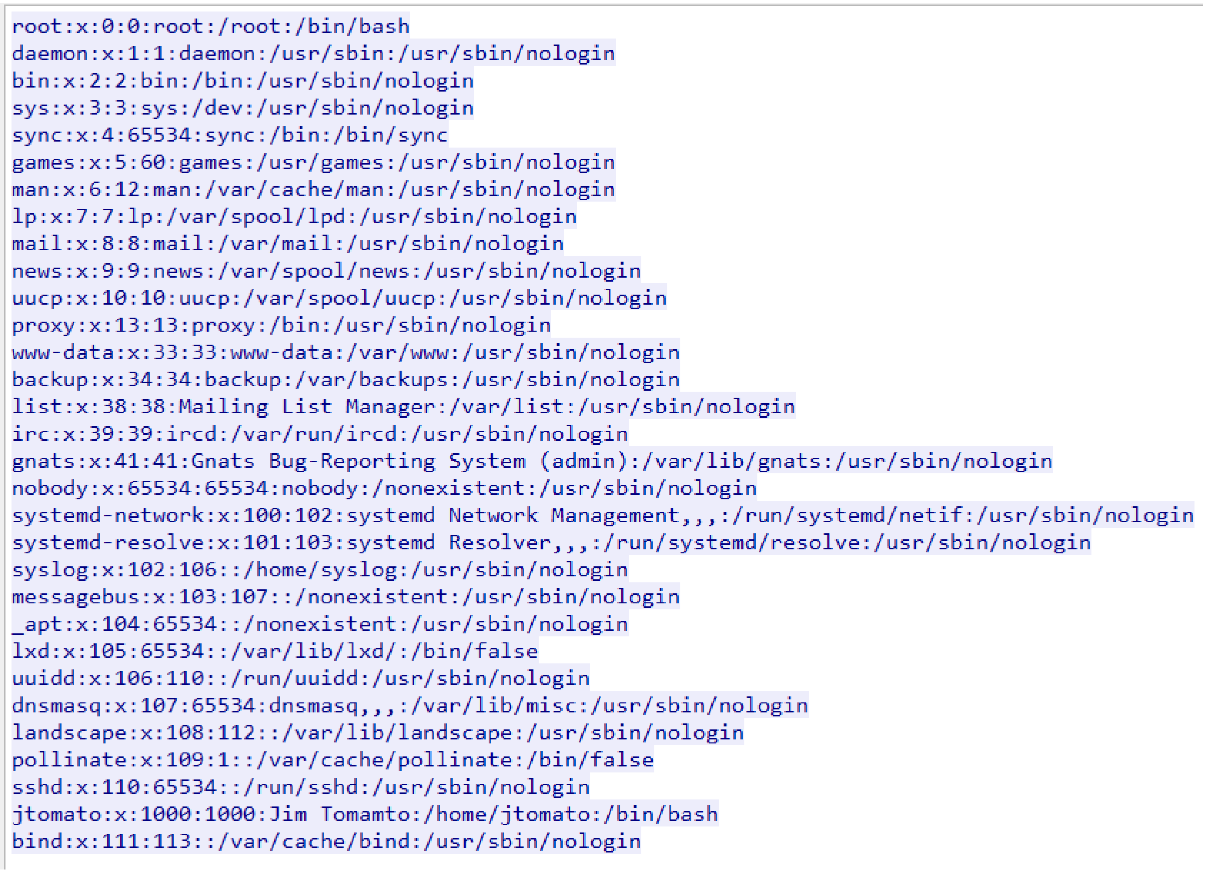
Using the following filter:

- ip.addr==192.168.2.244 && tcp.port==34972 && ip.addr==192.168.2.5 && tcp.port==9999

We can inspect this traffic further. If you view the TCP stream of this traffic, we can see that 192.168.2.244 is connection to 192.168.2.5 over port 9999:



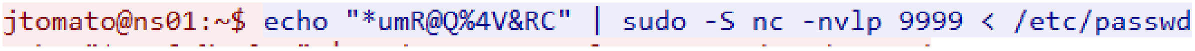
Time	Source	Destination	Destination Port
2020-04-16 19:22:33	192.168.2.244	192.168.2.5	9999
2020-04-16 19:22:33	192.168.2.5	192.168.2.244	34972
2020-04-16 19:22:33	192.168.2.244	192.168.2.5	9999
2020-04-16 19:22:33	192.168.2.5	192.168.2.244	34972
2020-04-16 19:22:33	192.168.2.244	192.168.2.5	9999
2020-04-16 19:22:49	192.168.2.244	192.168.2.5	9999
2020-04-16 19:22:49	192.168.2.5	192.168.2.244	34972
2020-04-16 19:22:49	192.168.2.244	192.168.2.5	9999



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
jtomato:x:1000:1000:Jim Tomamto:/home/jtomato:/bin/bash
bind:x:111:113::/var/cache/bind:/usr/sbin/nologin
```

The TCP stream contains the /etc/passwd file.

Alternatively, we can see a netcat listener being created over the first shell on port 4444:



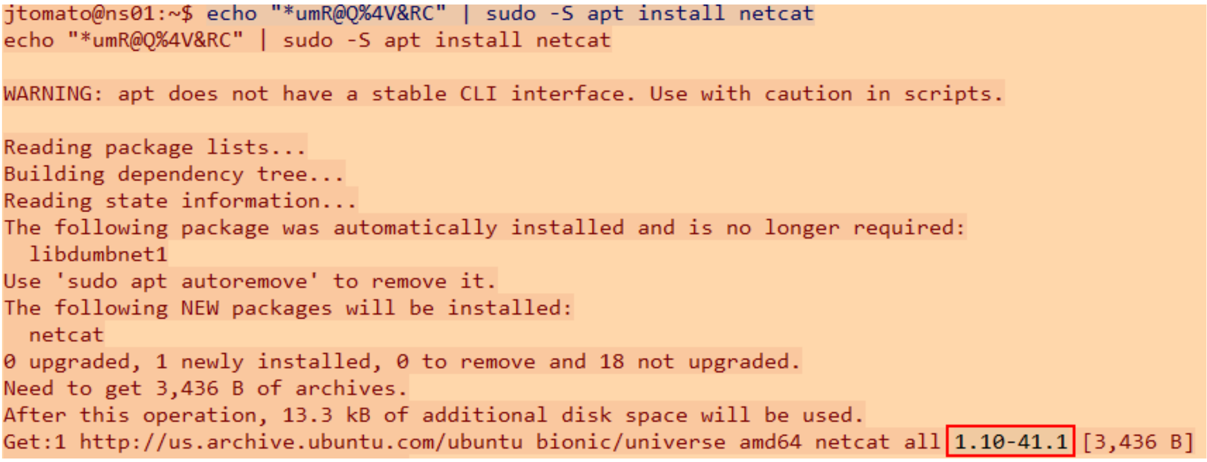
```
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd
```

This command starts a netcat listener on port 9999 that will send /etc/passwd to anyone who connects.

Answer: 9999

What version of netcat is installed?

We can see the version of netcat installed by inspecting the TCP stream of the shell traffic over port 4444:

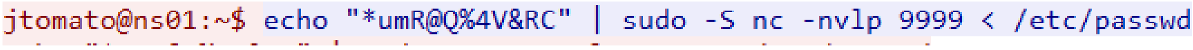


```
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S apt install netcat
echo "*umR@Q%4V&RC" | sudo -S apt install netcat

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists...
Building dependency tree...
Reading state information...
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  netcat
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
Need to get 3,436 B of archives.
After this operation, 13.3 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat all 1.10-41.1 [3,436 B]
```

Answer: 1.10-41.1

What file is added to the second shell

We found this earlier:



```
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd
```

Answer: /etc/passwd

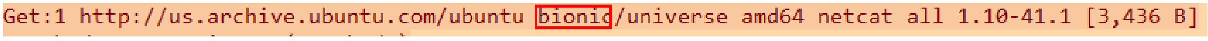
What password is used to elevate the shell?

See above.

Answer: *umR@Q%4V&RC

What is the codename of the target system's OS version?

When the threat actor installs netcat, we can see the codename of the target system:

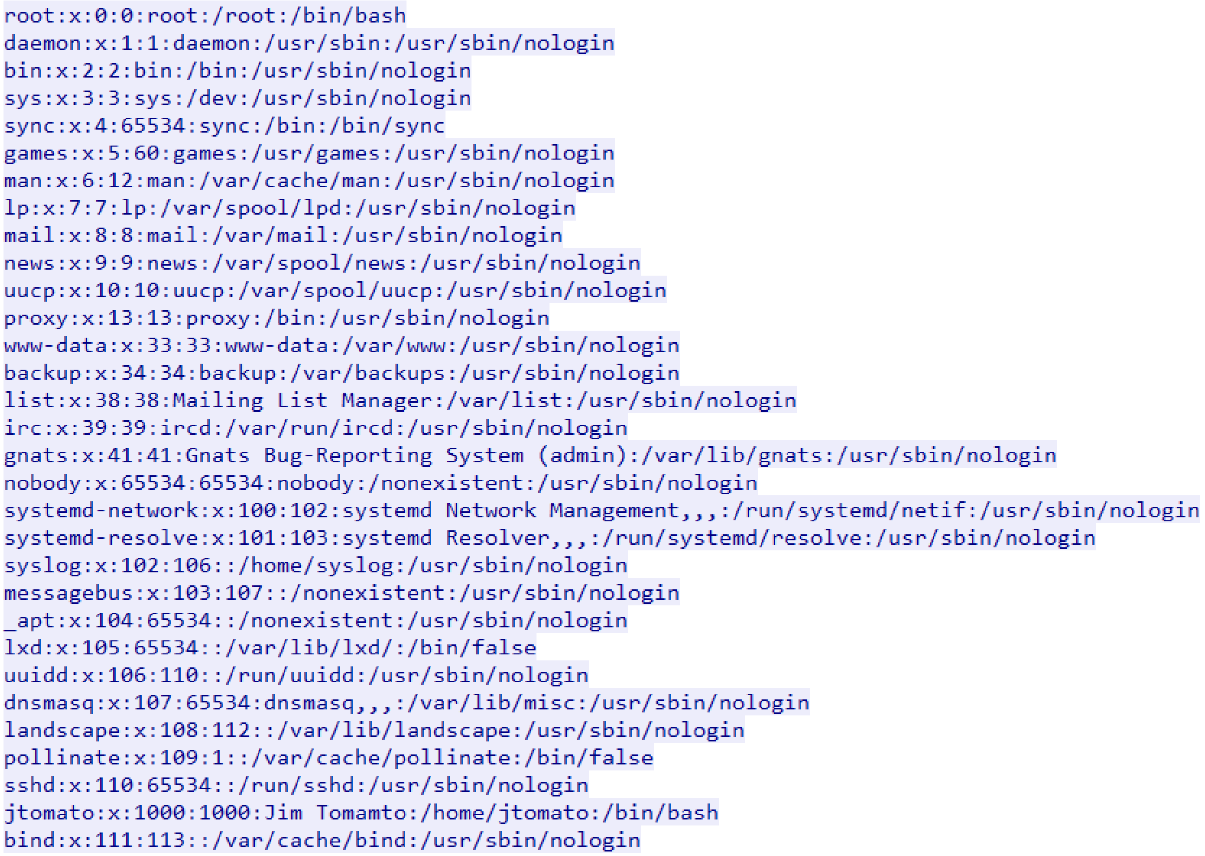


```
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat all 1.10-41.1 [3,436 B]
```

Answer: bionic

How many users are on the target system?

To find how many users are on the target system, you can count the number of lines within the /etc/passwd file, as each line represents a user on the system:



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
jtomato:x:1000:1000:Jim Tomamto:/home/jtomato:/bin/bash
bind:x:111:113::/var/cache/bind:/usr/sbin/nologin
```

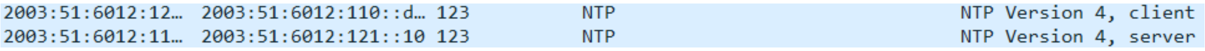
Answer: 31

File: network.pcapng

What is the IPv6 NTP server IP?

To find the IPv6 address of the NTP server, we can use the following display filter, which shows all ntp traffic within the PCAP:

- ntp

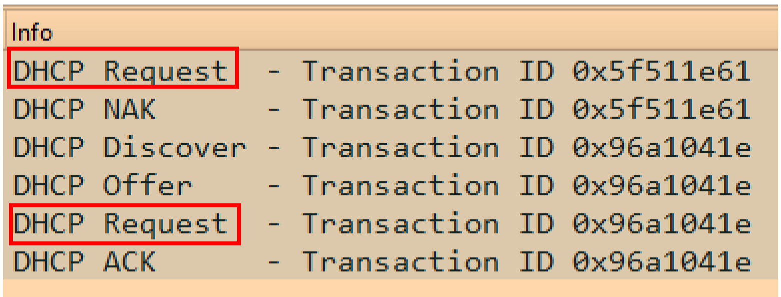


```
2003:51:6012:12…  2003:51:6012:110::d… 123        NTP                          NTP Version 4, client
2003:51:6012:11…  2003:51:6012:121::10 123        NTP                          NTP Version 4, server
```

Answer: 2003:51:6012:110::dcf7:123

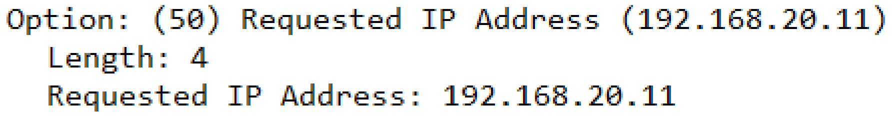
What is the first IP address that is requested by the DHCP client?

Like done previously, we can use the dhcp display filter to look for all DHCP traffic. In this pcap, there are only two DHCP Requests:



```
Info
DHCP Request  - Transaction ID 0x5f511e61
DHCP NAK      - Transaction ID 0x5f511e61
DHCP Discover - Transaction ID 0x96a1041e
DHCP Offer    - Transaction ID 0x96a1041e
DHCP Request  - Transaction ID 0x96a1041e
DHCP ACK      - Transaction ID 0x96a1041e
```

If you view the first request, you can find the requested IP address in the packet details pane:

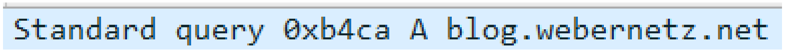


```
Option: (50) Requested IP Address (192.168.20.11)
  Length: 4
  Requested IP Address: 192.168.20.11
```

Answer: 192.168.20.11

What is the first authoritative name server returned for the domain that is being queried?

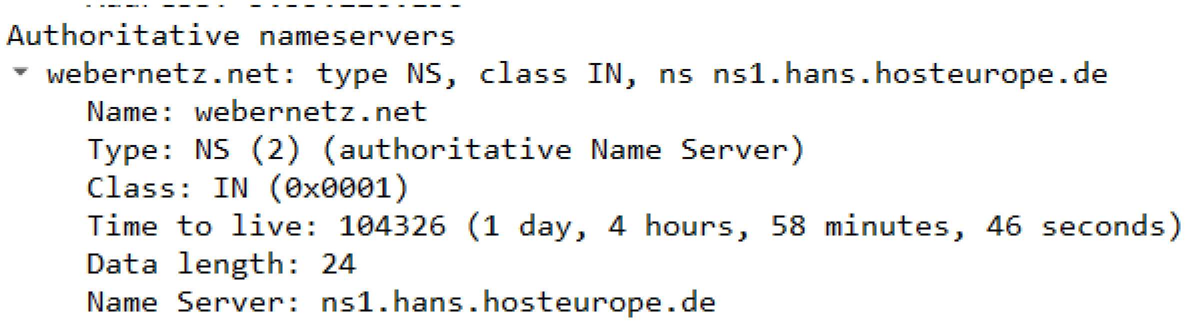
The first domain that is being queries is blog.webernetz.net:



```
Standard query 0xb4ca A blog.webernetz.net
```

To find the first authoritative name server returned for this domain, we can use the following query:

- dns.qry.name == "blog.webernetz.net" and dns.response_to



```
Authoritative nameservers
▾ webernetz.net: type NS, class IN, ns ns1.hans.hosteurope.de
    Name: webernetz.net
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 104326 (1 day, 4 hours, 58 minutes, 46 seconds)
    Data length: 24
    Name Server: ns1.hans.hosteurope.de
```

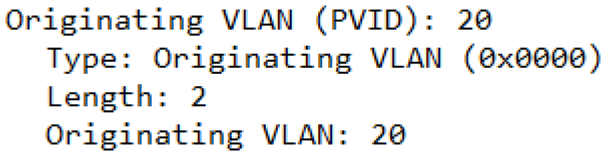
Answer: ns1.hans.hosteurope.de

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

To find the number of the first VLAN to have a topology change, we can use the following display filter:

- stp.flags.tc == 1

If you view the first packet (packet number 42), you can find the VLAN number:



```
Originating VLAN (PVID): 20
  Type: Originating VLAN (0x0000)
  Length: 2
  Originating VLAN: 20
```

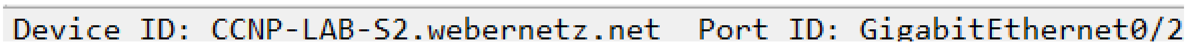
Answer: 20

What is the port for CDP for CCNP-LAB-S2?

Start by using the CDP display filter:

- cdp

We can see the port for CCNP-LAB-S2 is GigabitEthernet0/2:



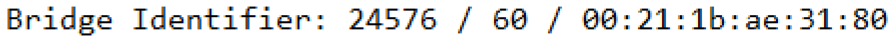
```
Device ID: CCNP-LAB-S2.webernetz.net  Port ID: GigabitEthernet0/2
```

Answer: GigabitEthernet0/2

What is the MAC address for the root bridge for VLAN 60?

- vlan.id == 60

If you explore one of the packets, you can find the MAC address of the root bridge:



```
Bridge Identifier: 24576 / 60 / 00:21:1b:ae:31:80
```

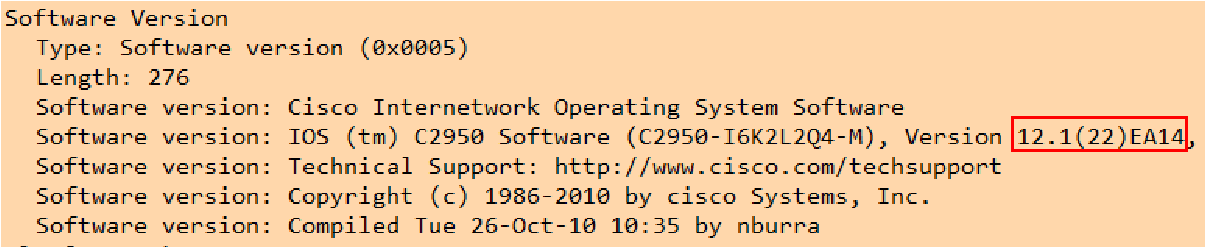
Answer: 00:21:1b:ae:31:80

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

Using the CDP display filter:

- cdp

You can find the IOS version by clicking on packets for CCNP-LAB-S2 and viewing the packet details pane:

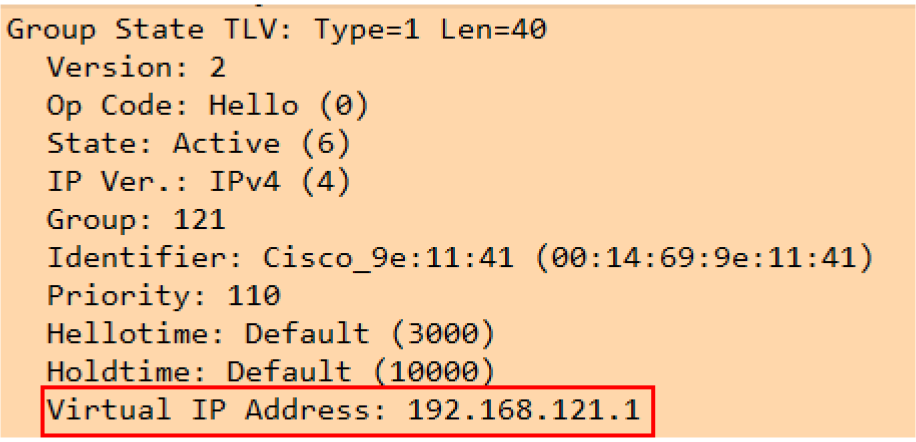


```
Software Version
  Type: Software version (0x0005)
  Length: 276
  Software version: Cisco Internetwork Operating System Software
  Software version: IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14,
  Software version: Technical Support: http://www.cisco.com/techsupport
  Software version: Copyright (c) 1986-2010 by cisco Systems, Inc.
  Software version: Compiled Tue 26-Oct-10 10:35 by nburra
```

Answer: 12.1(22)EA14

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

- hsrp2.group == 121

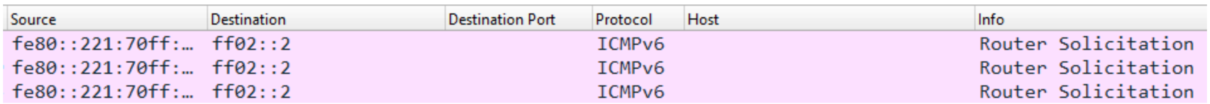


```
Group State TLV: Type=1 Len=40
   Version: 2
   Op Code: Hello (0)
   State: Active (6)
   IP Ver.: IPv4 (4)
   Group: 121
   Identifier: Cisco_9e:11:41 (00:14:69:9e:11:41)
   Priority: 110
   Hellotime: Default (3000)
   Holdtime: Default (10000)
   Virtual IP Address: 192.168.121.1
```

Answer: 192.168.121.1

How many router solicitations were sent?

- icmpv6.type==133

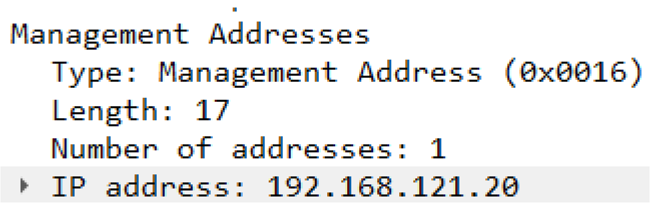


Source	Destination	Destination Port	Protocol	Host	Info
fe80::221:70ff:…	ff02::2		ICMPv6		Router Solicitation
fe80::221:70ff:…	ff02::2		ICMPv6		Router Solicitation
fe80::221:70ff:…	ff02::2		ICMPv6		Router Solicitation

Answer: 3

What is the management address of CCNP-LAB-S2?

- cdp



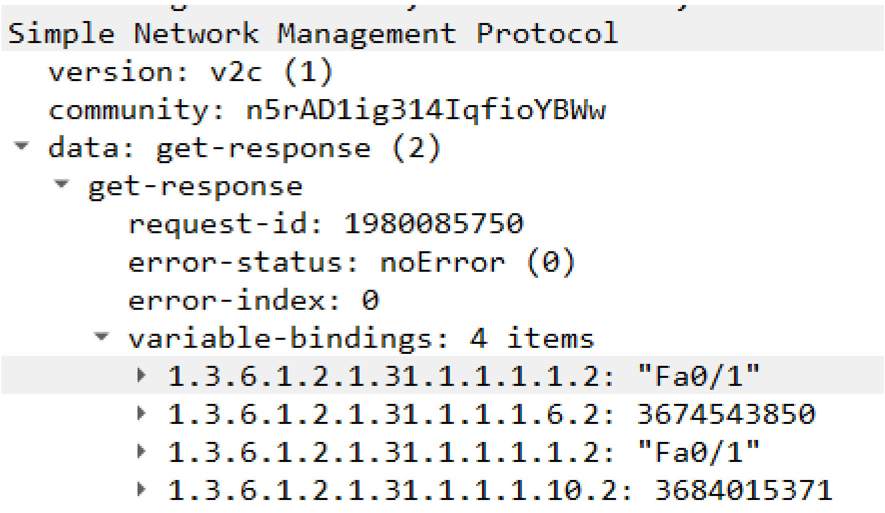
```
Management Addresses
   Type: Management Address (0x0016)
   Length: 17
   Number of addresses: 1
 ▸ IP address: 192.168.121.20
```

Answer: 192.168.121.20

What is the interface being reported on in the first SNMP query?

- snmp

If you view the response for the first SNMP query, you can find the interface being reported on:



```
Simple Network Management Protocol
   version: v2c (1)
   community: n5rAD1ig314IqfioYBWw
 ▾ data: get-response (2)
   ▾ get-response
       request-id: 1980085750
       error-status: noError (0)
       error-index: 0
     ▾ variable-bindings: 4 items
       ▸ 1.3.6.1.2.1.31.1.1.1.1.2: "Fa0/1"
       ▸ 1.3.6.1.2.1.31.1.1.1.6.2: 3674543850
       ▸ 1.3.6.1.2.1.31.1.1.1.1.2: "Fa0/1"
       ▸ 1.3.6.1.2.1.31.1.1.1.10.2: 3684015371
```

Answer: Fa0/1

When was the NVRAM config last updated?

Answer: 2017-03-03 21:02

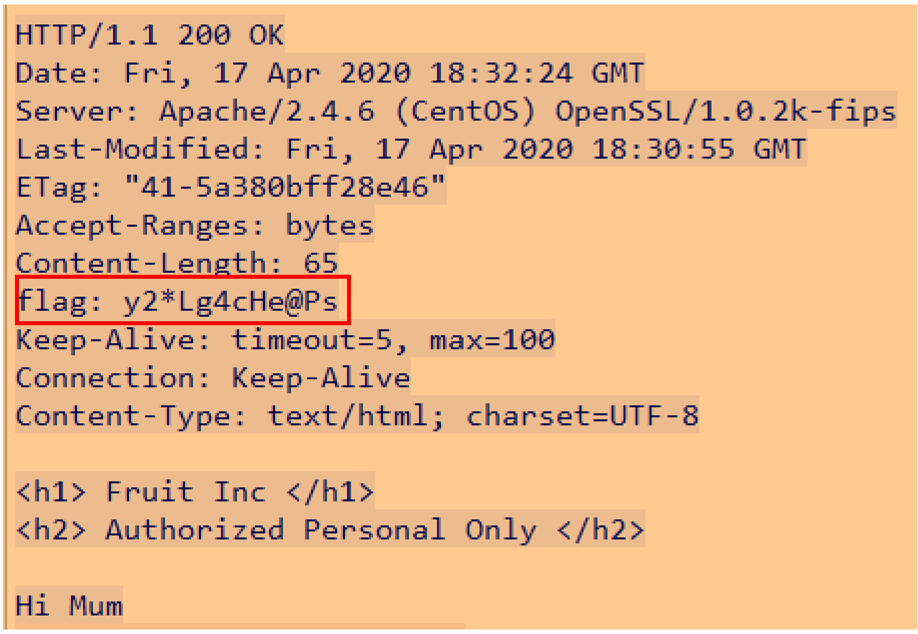
What is the IPv6 of the RADIUS server?

Answer: 2001:DB8::1812

File: https:pcapng

What has been added to web interaction with web01.fruitinc.xyz?

After decrypting the TLS traffic with the secret-secret.txt file, if you look at HTTP requests made to web01.fruitinc.xyz and follow the HTTP stream, you can find the answer in the flag field:

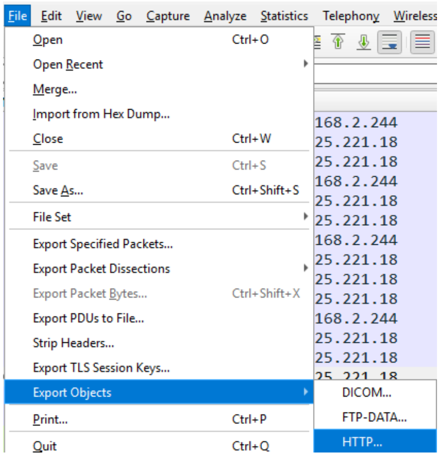


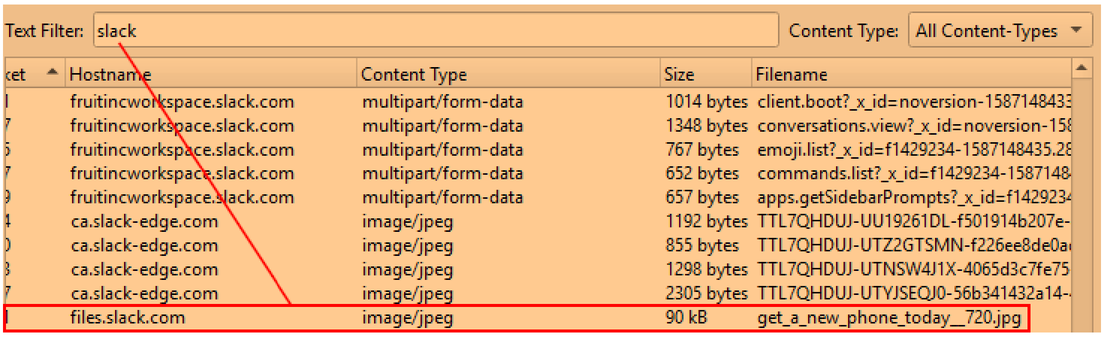
```
HTTP/1.1 200 OK
Date: Fri, 17 Apr 2020 18:32:24 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
Last-Modified: Fri, 17 Apr 2020 18:30:55 GMT
ETag: "41-5a380bff28e46"
Accept-Ranges: bytes
Content-Length: 65
flag: y2*Lg4cHe@Ps
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<h1> Fruit Inc </h1>
<h2> Authorized Personal Only </h2>

Hi Mum
```

Answer: y2*Lg4cHe@Ps

What is the name of the photo that is viewed in slack?

The easiest method of identifying the photo that is viewed in slack is by navigating to File > Export Objects > HTTP and filtering for slack:

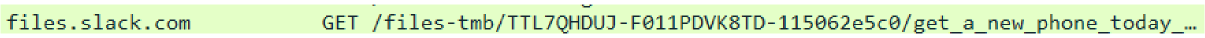




Text Filter: slack Content Type: All Content-Types

ket	Hostname	Content Type	Size	Filename
l	fruitincworkspace.slack.com	multipart/form-data	1014 bytes	client.boot?_x_id=noversion-158714843
7	fruitincworkspace.slack.com	multipart/form-data	1348 bytes	conversations.view?_x_id=noversion-15
5	fruitincworkspace.slack.com	multipart/form-data	767 bytes	emoji.list?_x_id=f1429234-1587148435.2
7	fruitincworkspace.slack.com	multipart/form-data	652 bytes	commands.list?_x_id=f1429234-1587148
9	fruitincworkspace.slack.com	multipart/form-data	657 bytes	apps.getSidebarPrompts?_x_id=f142923
4	ca.slack-edge.com	image/jpeg	1192 bytes	TTL7QHDUJ-UU19261DL-f501914b207e-
0	ca.slack-edge.com	image/jpeg	855 bytes	TTL7QHDUJ-UTZ2GTSMN-f226ee8de0a
3	ca.slack-edge.com	image/jpeg	1298 bytes	TTL7QHDUJ-UTNSW4J1X-4065d3c7fe75
7	ca.slack-edge.com	image/jpeg	2305 bytes	TTL7QHDUJ-UTYJSEQJ0-56b341432a14-
l	files.slack.com	image/jpeg	90 kB	get_a_new_phone_today__720.jpg

Alternatively, if you filter for http traffic and look through the requests, we can see a GET request being made to files.slack.com:



```
files.slack.com          GET /files-tmb/TTL7QHDUJ-F011PDVK8TD-115062e5c0/get_a_new_phone_today_…
```

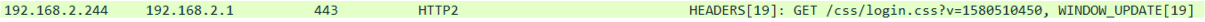
Answer: get_a_new_phone_today__720.jpg

What is the username and password to login to 192.168.2.1?

Using the following filter, we can see all HTTP2 traffic where 192.168.2.1 is the destination address:

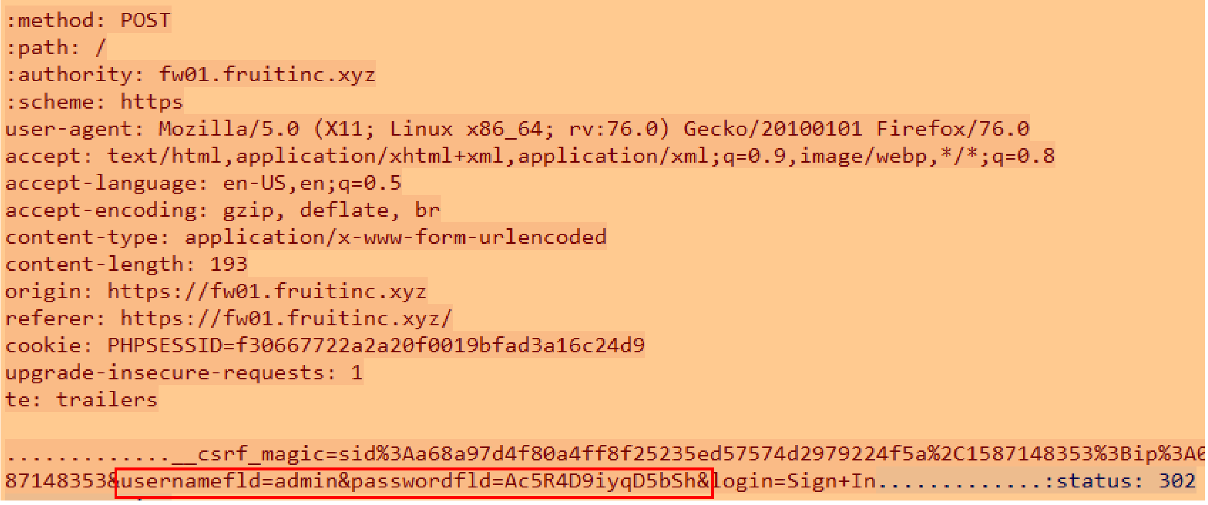
- ip.dst == 192.168.2.1 && http2

If you look through the output, we can see a GET request to css/login.css:



```
192.168.2.244    192.168.2.1         443         HTTP2                         HEADERS[19]: GET /css/login.css?v=1580510450, WINDOW_UPDATE[19]
```

If you follow the HTTP2 stream, you can find the credentials:

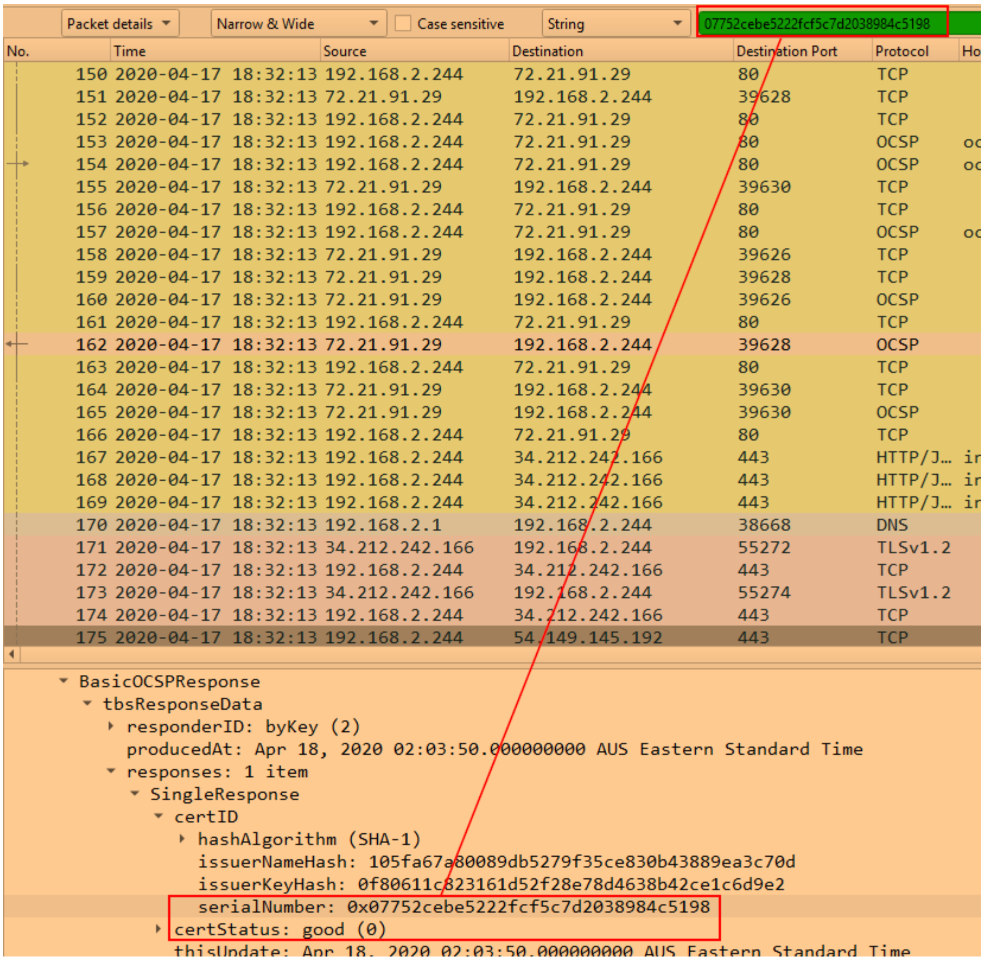


```
:method: POST
:path: /
:authority: fw01.fruitinc.xyz
:scheme: https
user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
content-type: application/x-www-form-urlencoded
content-length: 193
origin: https://fw01.fruitinc.xyz
referer: https://fw01.fruitinc.xyz/
cookie: PHPSESSID=f30667722a2a20f0019bfad3a16c24d9
upgrade-insecure-requests: 1
te: trailers

.............__csrf_magic=sid%3Aa68a97d4f80a4ff8f25235ed57574d2979224f5a%2C1587148353%3Bip%3A6
87148353&usernamefld=admin&passwordfld=Ac5R4D9iyqD5bSh&login=Sign+In.............:status: 302
```

Answer: admin:Ac5R4D9iyqD5bSh

What is the certStatus for the certificate with a serial number of 07752cebe5222fcf5c7d2038984c5198?

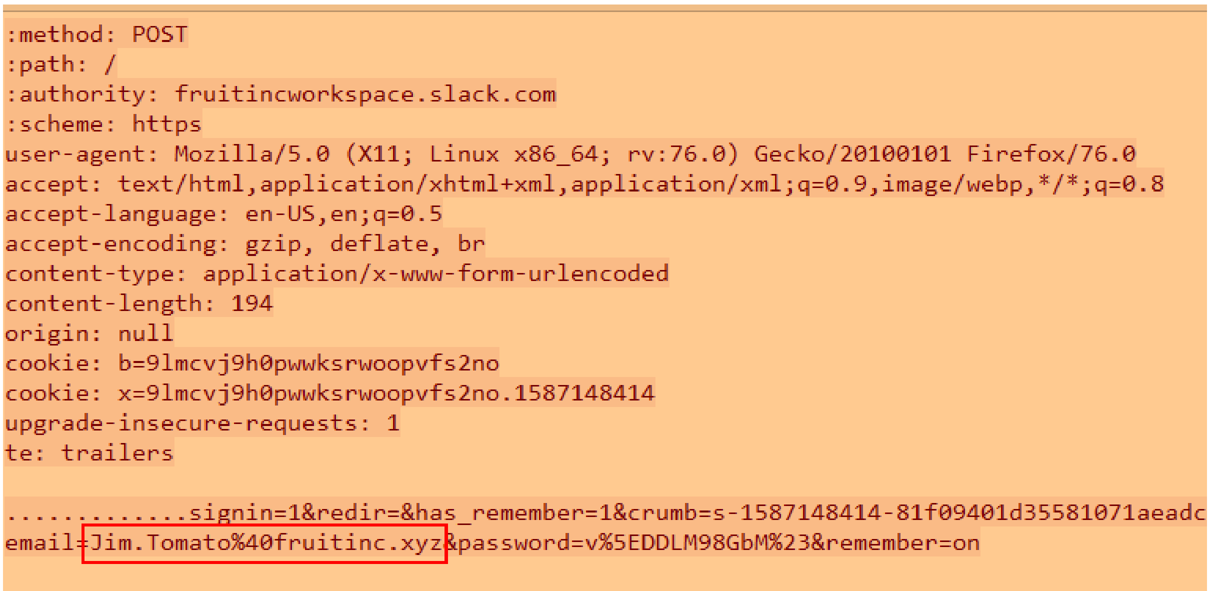
The easiest way to find the certStatus is to press Ctrl + F and search for the serial number:



```
No.     Time                Source          Destination     Destination Port  Protocol  Ho
  150 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               TCP
  151 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39628            TCP
  152 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               TCP
  153 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               OCSP      oc
  154 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               OCSP      oc
  155 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39630            TCP
  156 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               TCP
  157 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               OCSP      oc
  158 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39626            TCP
  159 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39628            TCP
  160 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39626            OCSP
  161 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               TCP
  162 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39628            OCSP
  163 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               TCP
  164 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39630            TCP
  165 2020-04-17 18:32:13 72.21.91.29     192.168.2.244    39630            OCSP
  166 2020-04-17 18:32:13 192.168.2.244   72.21.91.29      80               TCP
  167 2020-04-17 18:32:13 192.168.2.244   34.212.242.166   443              HTTP/J…   ir
  168 2020-04-17 18:32:13 192.168.2.244   34.212.242.166   443              HTTP/J…   ir
  169 2020-04-17 18:32:13 192.168.2.244   34.212.242.166   443              HTTP/J…   ir
  170 2020-04-17 18:32:13 192.168.2.1     192.168.2.244    38668            DNS
  171 2020-04-17 18:32:13 34.212.242.166  192.168.2.244    55272            TLSv1.2
  172 2020-04-17 18:32:13 192.168.2.244   34.212.242.166   443              TCP
  173 2020-04-17 18:32:13 34.212.242.166  192.168.2.244    55274            TLSv1.2
  174 2020-04-17 18:32:13 192.168.2.244   34.212.242.166   443              TCP
  175 2020-04-17 18:32:13 192.168.2.244   54.149.145.192   443              TCP

  BasicOCSPResponse
    tbsResponseData
      responderID: byKey (2)
      producedAt: Apr 18, 2020 02:03:50.000000000 AUS Eastern Standard Time
      responses: 1 item
        SingleResponse
          certID
            hashAlgorithm (SHA-1)
            issuerNameHash: 105fa67a80089db5279f35ce830b43889ea3c70d
            issuerKeyHash: 0f80611c823161d52f28e78d4638b42ce1c6d9e2
            serialNumber: 0x07752cebe5222fcf5c7d2038984c5198
          certStatus: good (0)
          thisUpdate: Apr 18, 2020 02:03:50.000000000 AUS Eastern Standard Time
```

Answer: good

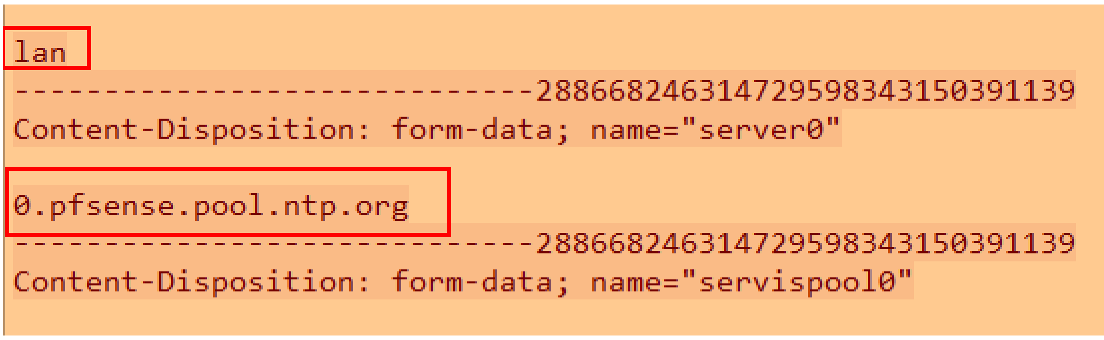
What is the email of someone who needs to change their password?



```
:method: POST
:path: /
:authority: fruitincworkspace.slack.com
:scheme: https
user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
content-type: application/x-www-form-urlencoded
content-length: 194
origin: null
cookie: b=9lmcvj9h0pwwksrwoopvfs2no
cookie: x=9lmcvj9h0pwwksrwoopvfs2no.1587148414
upgrade-insecure-requests: 1
te: trailers

...............signin=1&redir=&has_remember=1&crumb=s-1587148414-81f09401d35581071aeadc
email=Jim.Tomato%40fruitinc.xyz&password=v%5EDDLM98GbM%23&remember=on
```

Answer: Jim.Tomato@fruitinc.xyz

A service is assigned to an interface. What is the interface, and what is the service?



```
lan
-----------------------------288668246314729598343150391139
Content-Disposition: form-data; name="server0"

0.pfsense.pool.ntp.org
-----------------------------288668246314729598343150391139
Content-Disposition: form-data; name="servispool0"
```

Answer: lan:ntp