Labs - Intro to Network Traffic Analysis

Introduction

Network Primer - Layers 1-4

Question

- How many layers does the OSI model have?
  -> The OSI model has 7 layers, comprised of Application, Presentation, Session, transport, network, data-link and physical layer
- How many layers are there in the TCP/IP model?
  -> The TCP/IP model has 4 layers, comprised of Application, transport, Internet and link layer.
- True or False: Routers operate at layer 2 of the OSI model?
  False, Routers operate at layer 3, the network layer of the OSI model.
- What addressing mechanism is used at the Link Layer of the TCP/IP model?
  -> The link layer is comprised of layer 1 and 2 of the OSI model, so it uses MAC-Addressing.
- At what layer of the OSI model is a PDU encapsulated into a packet? (the number).
  -> We know that the PDU is encapsulated into a packet at the Network layer, which corresponds to layer 3 of the OSI model.
- What addressing mechanism utilizes a 32-bit address?
  -> IPv4 utilises a 32-bit address.
- What Transport layer protocol is connection oriented?
  -> We know that TCP protocol is connection oriented, with an TCP handshake for both initialisation and shutting down of a session.
- What Transport Layer protocol is considered unreliable?
  -> UDP is generally considered unreliable as it is a connection less protocol and does not care about if the destination is active.
- TCP's three-way handshake consists of 3 packets: 1.Syn, 2.Syn & ACK, 3. _? What is the final packet of the handshake?
  -> We know that the last part of the packet is ACK, where the client responds to the server it is ready for connection.

Networking Primer - Layers 5-7

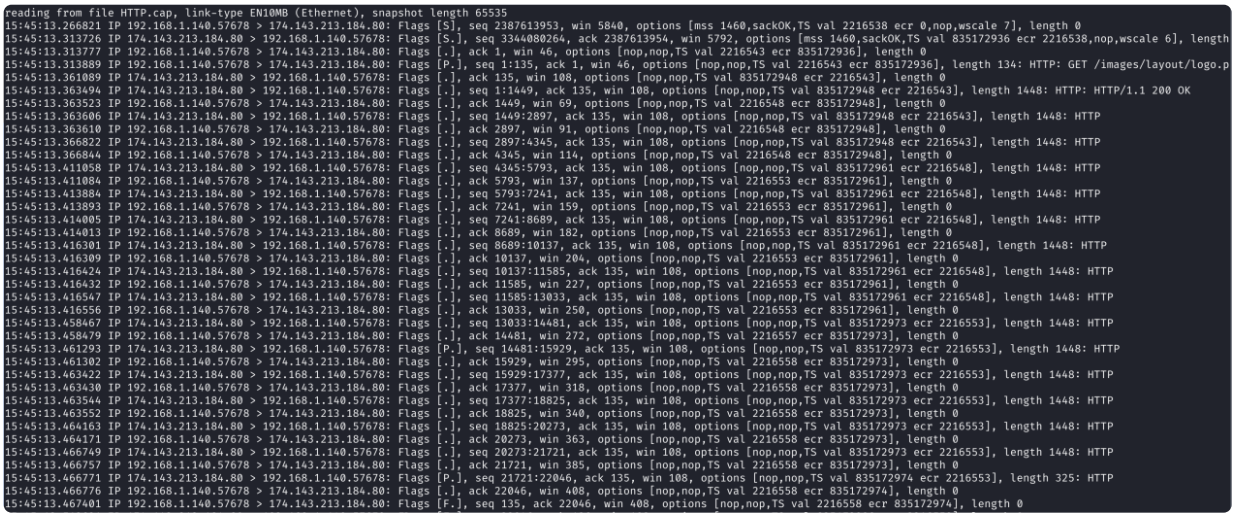
Questions

- What is the default operational mode method used by FTP?
  -> We know that by default, it uses the active mode, where it listens for control command PORT from the client on what port to use for.
- FTP utilizes what two ports for command and data transfer? (separate the two numbers with a space)
  -> FTP uses TCP on port 20 for data transfer and 21 for command issued during the FTP session.
- Does SMB utilize TCP or UDP as its transport layer protocol?
  -> SMB utilises the TCP protocol as the transport layer protocol.
- SMB has moved to using what TCP port?
  -> SMB in the past utilised UDP ports 137 and 138, since modern changes, it has moved to TCp transport over port 445.
- Hypertext Transfer Protocol uses what well known TCP port number?
  -> HTTP protocol mostly uses TCP port 80 and 8000, but 80 is more common than 8000.
- What HTTP method is used to request information and content from the webserver?
  -> The GET method is used to request information and content from the webserver.
- What web based protocol uses TLS as a security measure?
  -> HTTPS uses TLS as a security measure, where certificate services and cryptographic measures (e.g. public-private key cryptography) are utilised.
- True or False: when utilizing HTTPS, all data sent across the session will appear as TLS Application data?
  -> Yes, from the example of HTTPS traffic, all data sent across the session will appear as TLS Application data.

Tcpdump Fundamentals

Question

- Utilizing the output shown in question-1.png, who is the server in this communication? (IP Address)



-> We look at the snap shot, we can see that the IP adddress 174.143.213.184 is an web server that is responding through port 80 http.

- Were absolute or relative sequence numbers used during the capture? (see question-1.zip to answer)
  -> We looked at the sequence numbers and they were relatively small. Hence it is the absolute sequence numbers used during the capture.
- If I wish to start a capture without hostname resolution, verbose output, showing contents in ASCII and hex, and grab the first 100 packets; what are the switches used? please answer in the order the switches are asked for in the question.
  -> We should chain the switches tgoether, we know that without hostname resolution would be n, verbose would be v, contents in ASCII and Hex would be X and first 100 packets would be s 100.
  -> Hence, the chain would be `-nvXc 100`
- Given the capture file at /tmp/capture.pcap, what tcpdump command will enable you to read from the capture and show the output contents in Hex and ASCII? (Please use best practices when using switches)
  -> We would use the read switch with output contents in HEX and ASCII, which would be

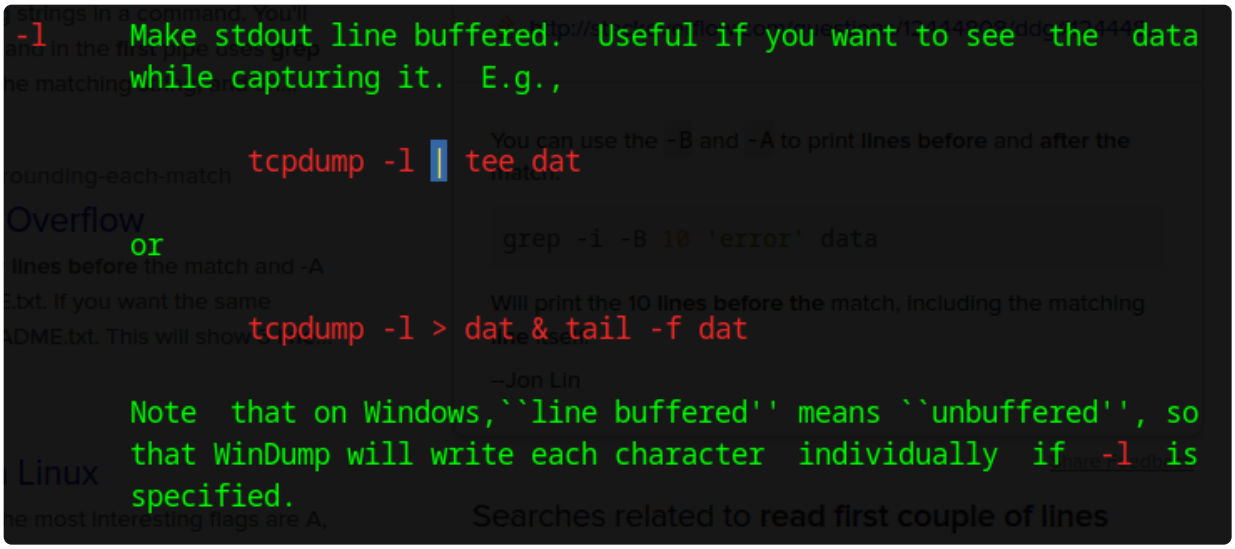
```
sudo tcpdump -Xr /tmp/capture.pcap
```

- What TCPDump switch will increase the verbosity of our output? (Include the - with the proper switch)
  -> It would be the -v switch, with additional v's increasing the verbosity.
- What built in terminal help reference can tell us more about TCPDump?
  -> We can look at the man page for more help.
- What TCPDump switch will let me write my output to a file?
  -> That would be the -w switch.

Fundamentals Lab

Question

- What TCPDump switch will allow us to pipe the contents of a pcap file out to another function such as 'grep'?
  -> We search for the | or pipe message in the man page, where we see that it is the -l switch.



- True or False: The filter "port" looks at source and destination traffic.

To print all ftp traffic through internet gateway *snup*: (note that the expression is quoted to prevent the shell from (mis-)interpreting the parentheses):

```
tcpdump 'gateway snup and (port ftp or ftp-data)'
```

To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net).

```
tcpdump ip and not net localnet
```

To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host.

```
tcpdump 'tcp[tcpflags] & (tcp-syn|tcp-fin) != 0 and not src and dst net localnet'
```

To print the TCP packets with flags RST and ACK both set. (i.e. select only the RST and ACK flags in the flags field, and if the result is "RST and ACK both set", match)

```
tcpdump 'tcp[tcpflags] & (tcp-rst|tcp-ack) == (tcp-rst|tcp-ack)'
```

To print all IPv4 HTTP packets to and from port 80, i.e. print only packets that contain data, not, for example, SYN and FIN packets and ACK-only packets. (IPv6 is left as an exercise for the reader.)

```
tcpdump 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)'
```

  -> Yes, we look at the man page of tcpdump and it filters for source and destination traffic.
- If we wished to filter out ICMP traffic from our capture, what filter could we use? (word only, not symbol please.)
  -> We know that to capture ICMP traffic, we have the following

How to Capture ICMPv6 packets With Tcpdump

In IPv6, an IPv6 packet is 40 bytes long, and the first 8 bits of the ICMPv6 header specify its type. We can use this tcpdump command to filter all ICMPv6 packets.

```
# tcpdump -i eth0 icmp6
```

-> Hence, we can deduce that to not capture ICMP traffic, we could do `not icmp`.

- What command will show you where / if TCPDump is installed?
  -> We know that `which tcpdump` tells you whether TCPDump is installed.
- How do you start a capture with TCPDump to capture on eth0?
  -> We capture with `sudp tcpdump -i eth0`
- What switch will provide more verbosity in your output?
  -> We know that the -v verbose switch will, increasing by verbosity the more we add.
- What switch will write your capture output to a .pcap file?
  -> The -w switch will ensure we write our captured output to a .pcap file.
- What switch will read a capture from a .pcap file?
  -> Similarly, -r would alllow us to read capture form a .pcap file
- What switch will show the contents of a capture in Hex and ASCII?
  -> The -X switch would show contents of a cpature in Hex and ASCII.

Tcpdump Packet Filtering

Question

- What filter will allow me to see traffic coming from or destined to the host with an ip of 10.10.20.1?
  -> We can do so with `host 10.10.20.1`
- What filter will allow me to capture based on either of two options?
  -> We can do so with the or option.
- True or False: TCPDump will resolve IPs to hostnames by default.
  -> Yes, through our lab experiences, it does so by default.

Interrogating Network Traffic With Capture and Display Filters

Question

- What are the client and server port numbers used in first full TCP three-way handshake? (low number first then high number)
  -> We look for first 20 packet (without resolving hostname or well-known ports_ to determine the first full TCP three-way handshake

```
sudo tcpdump -nnr TCPDump-lab-2.pcap -c 20
```

```
01:34:01.246293 IP 172.16.146.2.43806 > 95.216.26.30.80: Flags [S], seq 3078186339, win 64240, options [mss
1460,sackOK,TS val 3101551040 ecr 0,nop,wscale 7], length 0
01:34:01.254402 IP 172.16.146.2.52520 > 207.244.88.140.443: Flags [S], seq 75289295, win 64240, options [mss
 1460,sackOK,TS val 4062857 ecr 0,nop,wscale 7], length 0
01:34:01.296423 IP 207.244.88.140.443 > 172.16.146.2.52520: Flags [S.], seq 2053874896, ack 75289296, win 65
160, options [mss 1460,sackOK,TS val 3444223749 ecr 4062857,nop,wscale 7], length 0
01:34:01.296454 IP 172.16.146.2.52520 > 207.244.88.140.443: Flags [R], seq 75289296, win 0, length 0
01:34:01.389479 IP 95.216.26.30.80 > 172.16.146.2.43804: Flags [S.], seq 2667566931, ack 749874085, win 6516
0, options [mss 1460,sackOK,TS val 1169094229 ecr 3101551032,nop,wscale 7], length 0
01:34:01.389497 IP 172.16.146.2.43804 > 95.216.26.30.80: Flags [R], seq 749874085, win 0, length 0
01:34:01.401231 IP 95.216.26.30.80 > 172.16.146.2.43806: Flags [S.], seq 4210180338, ack 3078186340, win 651
60, options [mss 1460,sackOK,TS val 1169094240 ecr 3101551040,nop,wscale 7], length 0
01:34:01.401270 IP 172.16.146.2.43806 > 95.216.26.30.80: Flags [.], ack 1, win 502, options [nop,nop,TS val
3101551195 ecr 1169094240], length 0
01:34:02.216846 IP 172.16.146.2.56506 > 172.16.146.1.53: 42121+ A? fonts.googleapis.com. (38)
01:34:02.216954 IP 172.16.146.2.56506 > 172.16.146.1.53: 37006+ AAAA? fonts.googleapis.com. (38)
```

-> So the first conversation is on the client 172.16.146.2 on port 43806 towards server 95.216.30.80

- Based on the traffic seen in the pcap file, who is the DNS server in this network segment? (ip address)
  -> We filter the source port 53 on the pcap file on the first 10 captures

```
sudo tcpdump -nnr TCPDump-lab-2.pcap src port 53 -c 10
```

```
└─╼ [★]$ sudo tcpdump -nnr TCPDump-lab-2.pcap src port 53 -c 10
reading from file TCPDump-lab-2.pcap, link-type EN10MB (Ethernet), snapshot length 262144
01:34:01.237443 IP 172.16.146.1.53 > 172.16.146.2.57752: 41819 2/0/0 A 95.216.26.30, A 207.244.88.140 (60)
01:34:01.237444 IP 172.16.146.1.53 > 172.16.146.2.57752: 46943 0/1/0 (112)
01:34:02.217577 IP 172.16.146.1.53 > 172.16.146.2.56506: 42121 1/0/0 A 172.217.164.74 (54)
01:34:02.217577 IP 172.16.146.1.53 > 172.16.146.2.56506: 37006 1/0/0 AAAA 2607:f8b0:4002:c06::5f (66)
01:34:02.241342 IP 172.16.146.1.53 > 172.16.146.2.50587: 18737 6/0/0 A 64.233.177.100, A 64.233.177.101, A
4.233.177.138, A 64.233.177.139, A 64.233.177.102, A 64.233.177.113 (128)
01:34:02.241342 IP 172.16.146.1.53 > 172.16.146.2.50587: 48695 4/0/0 AAAA 2607:f8b0:4002:c08::8b, AAAA 2607
f8b0:4002:c08::66, AAAA 2607:f8b0:4002:c08::8a, AAAA 2607:f8b0:4002:c08::65 (144)
01:34:02.249114 IP 172.16.146.1.53 > 172.16.146.2.37580: 2236 3/0/0 CNAME apache.org., A 95.216.26.30, A 20
.244.88.140 (91)
01:34:02.249114 IP 172.16.146.1.53 > 172.16.146.2.37580: 62143 1/1/0 CNAME apache.org. (140)
01:34:02.386835 IP 172.16.146.1.53 > 172.16.146.2.50588: 64771 1/0/0 A 108.177.122.95 (61)
01:34:02.416084 IP 172.16.146.1.53 > 172.16.146.2.34235: 55566 2/0/0 CNAME gstaticadssl.l.google.com., AAAA
2607:f8b0:4002:c09::5e (99)
```

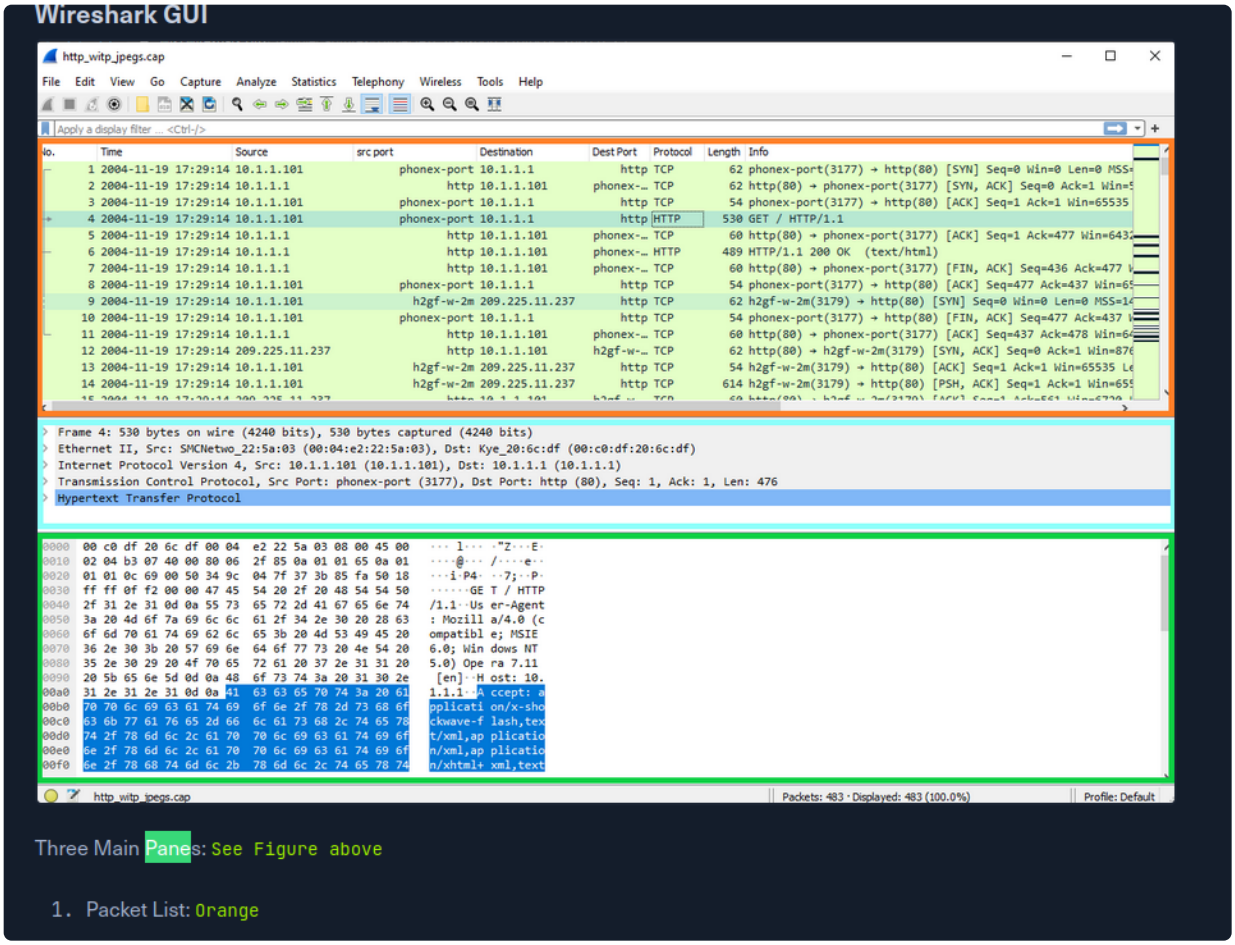
-> This becomes evident that 172.16.146.1 is the dns server.

Wireshark

Analysis with Wireshark

Question

- True or False: Wireshark can run on both Windows and Linux.
  -> Yes, wireshark can run on both Windows and Linux, provided specifications for hardware is met.
- Which Pane allows a user to see a summary of each packet grabbed during the capture?
  -> If we observe the panes, we see that



1. Packet List: Orange
    - In this window, we see a summary line of each packet that includes the fields listed below by default. We can add or remove columns to change what information is presented.
        - Number- Order the packet arrived in Wireshark
        - Time- Unix time format
        - Source- Source IP
        - Destination- Destination IP
        - Protocol- The protocol used (TCP, UDP, DNS, ETC.)
        - Information- Information about the packet. This field can vary based on the type of protocol used within. It will show, for example, what type of query It is for a DNS packet.
2. Packet Details: Blue
    - The Packet Details window allows us to drill down into the packet to inspect the protocols with greater detail. It will break it down into chunks that we would expect following the typical OSI Model reference. The packet is dissected into different encapsulation layers for inspection.
    - Keep in mind, Wireshark will show this encapsulation in reverse order with lower layer encapsulation at the top of the window and higher levels at the bottom.
3. Packet Bytes: Green
    - The Packet Bytes window allows us to look at the packet contents in ASCII or hex output. As we select a field from the windows above, it will be highlighted in the Packet Bytes window and show us where that bit or byte falls within the overall packet.

-> Hence, it the orange pane (packet list that we can see summary of each packet grbbed during the capture)

- Which pane provides you insight into the traffic you captured and displays it in both ASCII and Hex?
  -> Again, if we look at the panes above, we see that it is the pane in green that displays the traffic we captured in both ASCII and Hex, which is called the packet Bytes pane.
- What switch is used with TShark to list possible interfaces to capture on?
  -> If we look at the option provided with TShark, we see that it is -D, as shown below

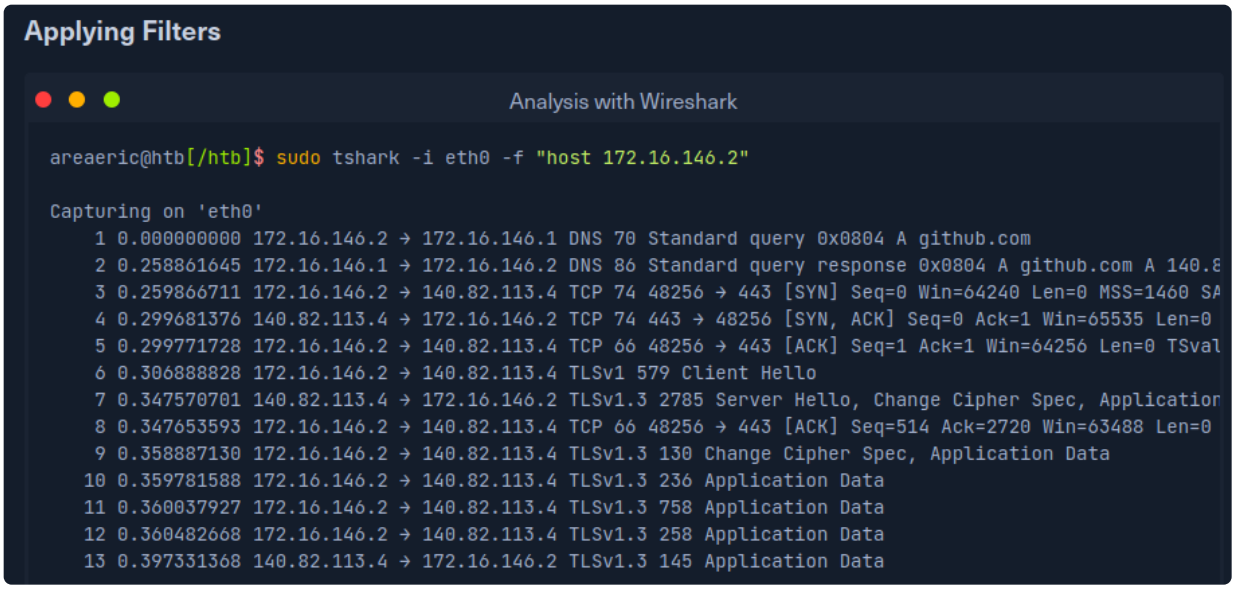
Basic TShark Switches

Switch Command	Result
D	Will display any interfaces available to capture from and then exit out.

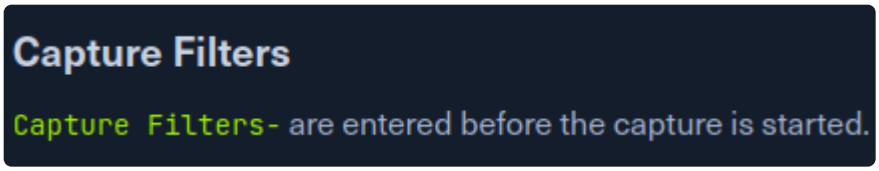
- What switch allows us to apply filters in TShark?
  -> Again, if we look at the option provided with t shark, we see it is -f switch

f	packet filter in libpcap syntax. Used during capture.

-> Furthermore, we have an example that utilises it on the host (client or server)



- Is a capture filter applied before the capture starts or after? (answer before or after)
  -> A capture filter is appllied before, as we can see in the section

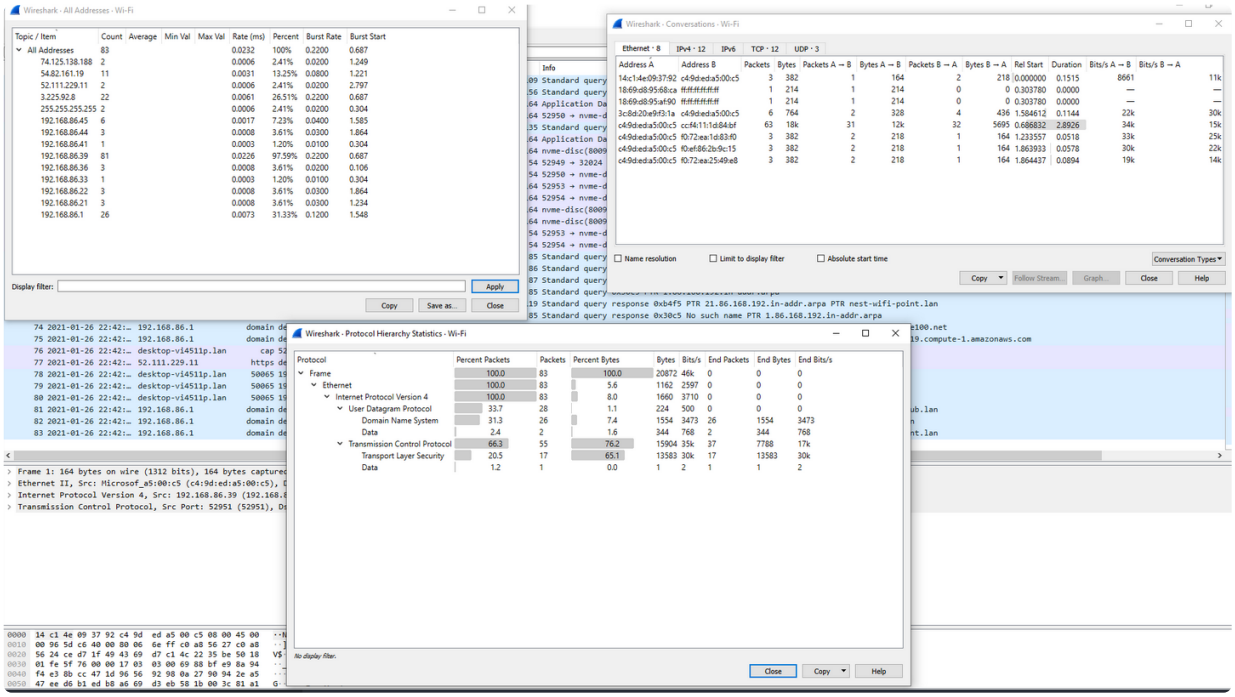
  while a display filter is applied while the capture is running and after it has stopped.

Wireshark Advanced Usage

Question

- Which plugin tab can provide us with a way to view conversation metadata and even protocol breakdowns for the entire PCAP file?
  -> Observe that in the statistics tab, we can view conversation metadata through statistics -> Conversations and protocol breakdowns through statistics -> IPv4 statisics

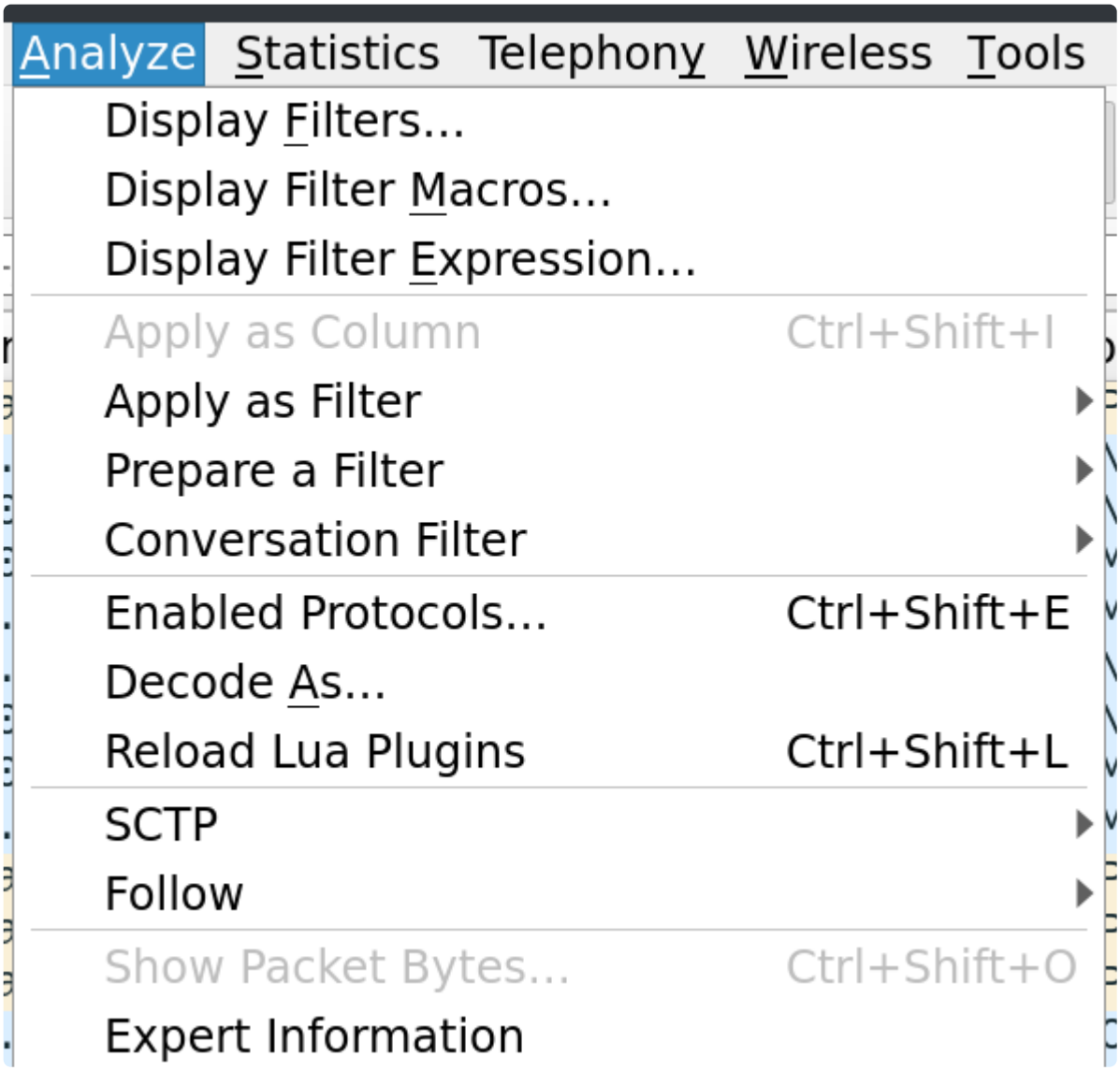
-> IP protocol types, with an sample screen shot below



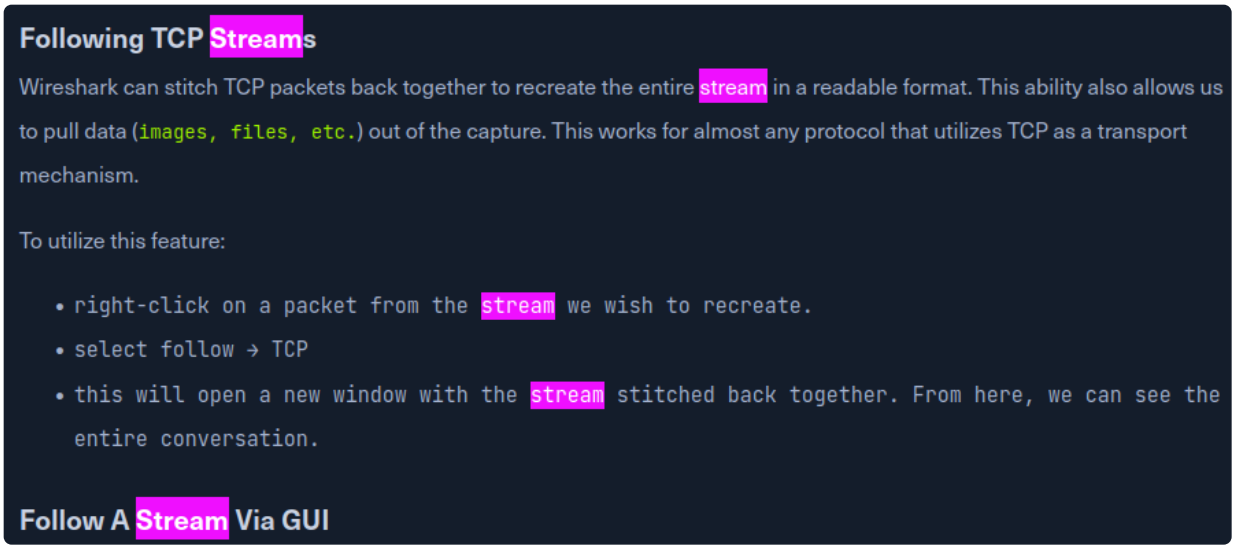
- What plugin tab will allow me to accomplish tasks such as applying filters, following streams, and viewing expert info?

  -> When looking at the Analyse tab, we see we can apply filers, follow streams and

view expert info as follows:



- What stream oriented Transport protocol enables us to follow and rebuild conversations and the included data?
  -> We know that wireshark can stitch TCP packets back together to recreate the entire stream readable format as follows

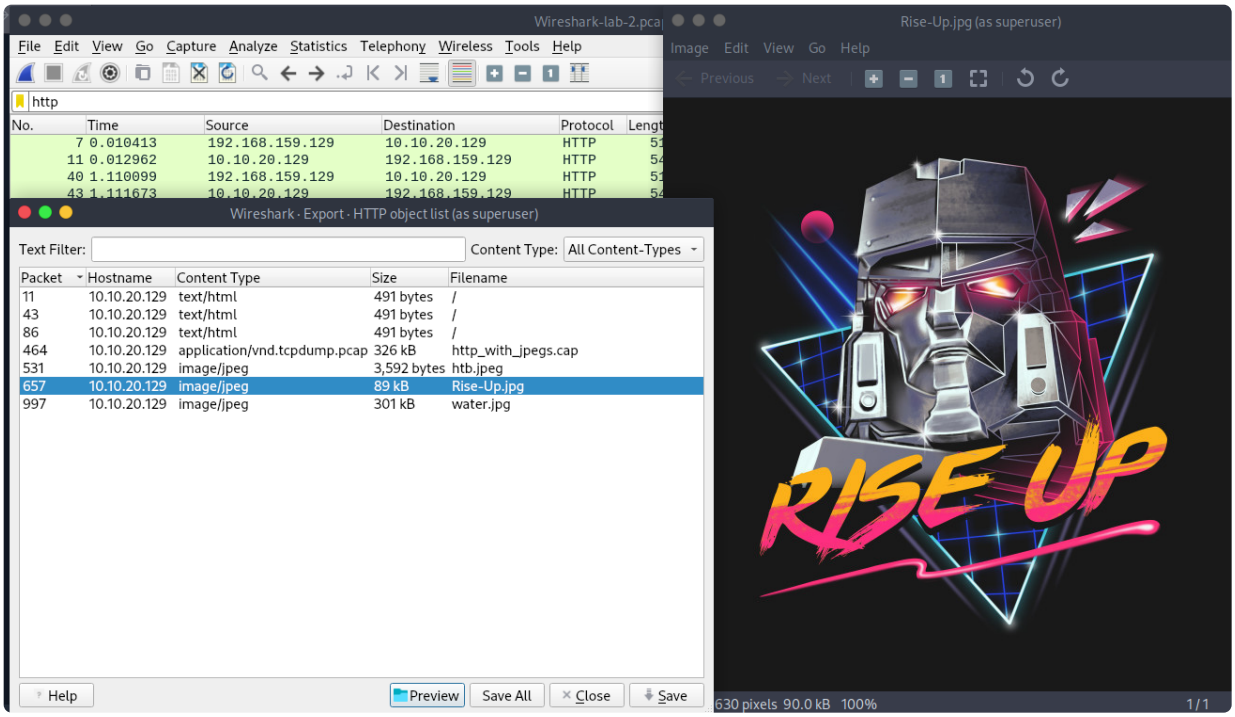


- True or False: Wireshark can extract files from HTTP traffic.
  -> True, wireshark can extract files form http traffic through the file -> export objects -> http and save the content required.
- True or False: The ftp-data filter will show us any data sent over TCP port 21.
  -> No, ftp-data will show us any data sent over TCP port 20, port 21 is for seeing the commands across the ftp-control channel.

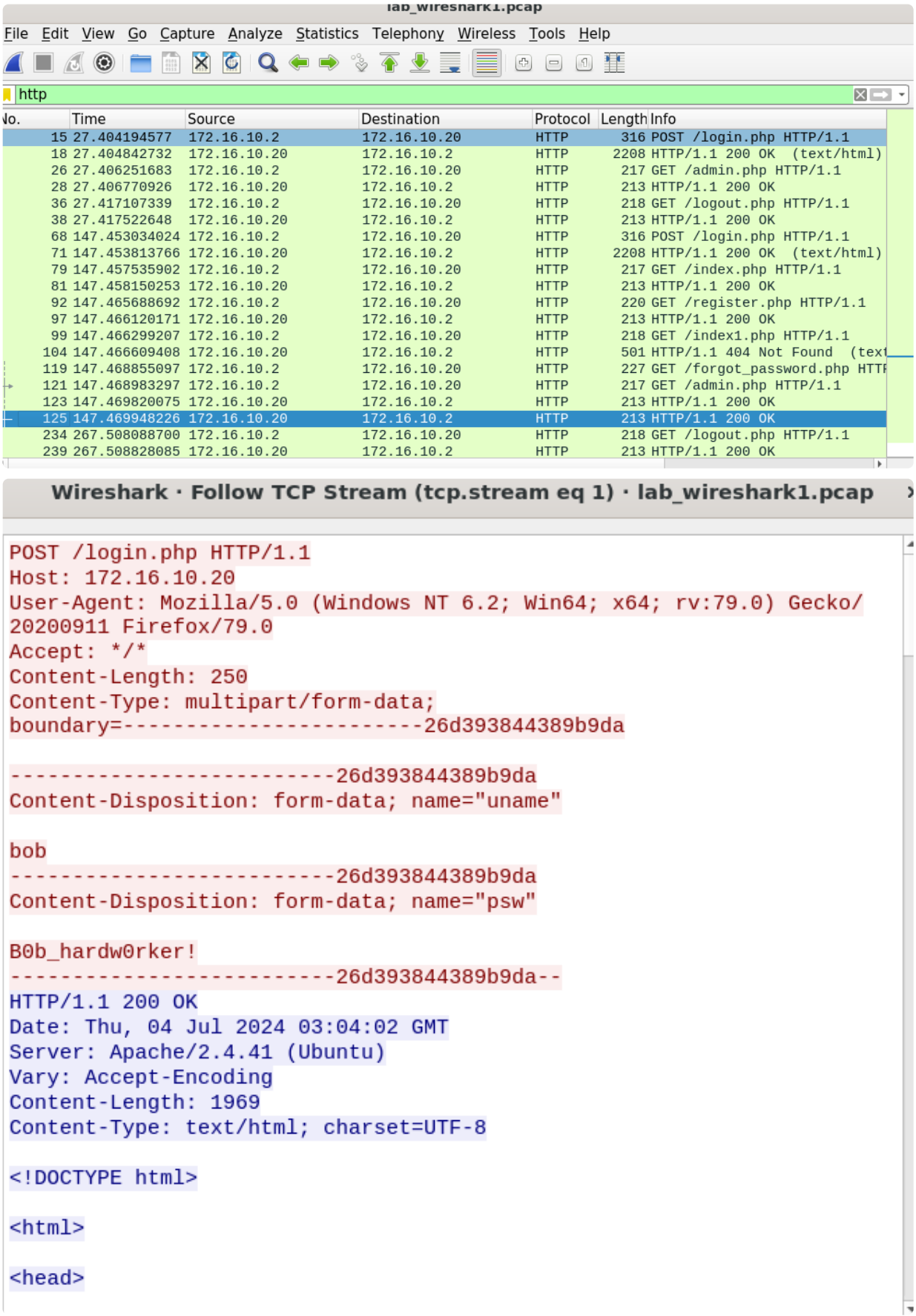
Packet Inception, Dissecting Network Traffic With Wireshark

Question

- What was the filename of the image that contained a certain Transformer Leader? (name.filetype)
  -> We see that when we capture the traffic, filter out for http traffic and export the object on the corresponding pcap file, we obtain that:



  -> Hence, Rise-up.jpg is the answer required
- Which employee is suspected of performing potentially malicious actions in the live environment?
  -> When we capture traffic life traffic on the target, filtered out for http traffic and followed the stream, we see that

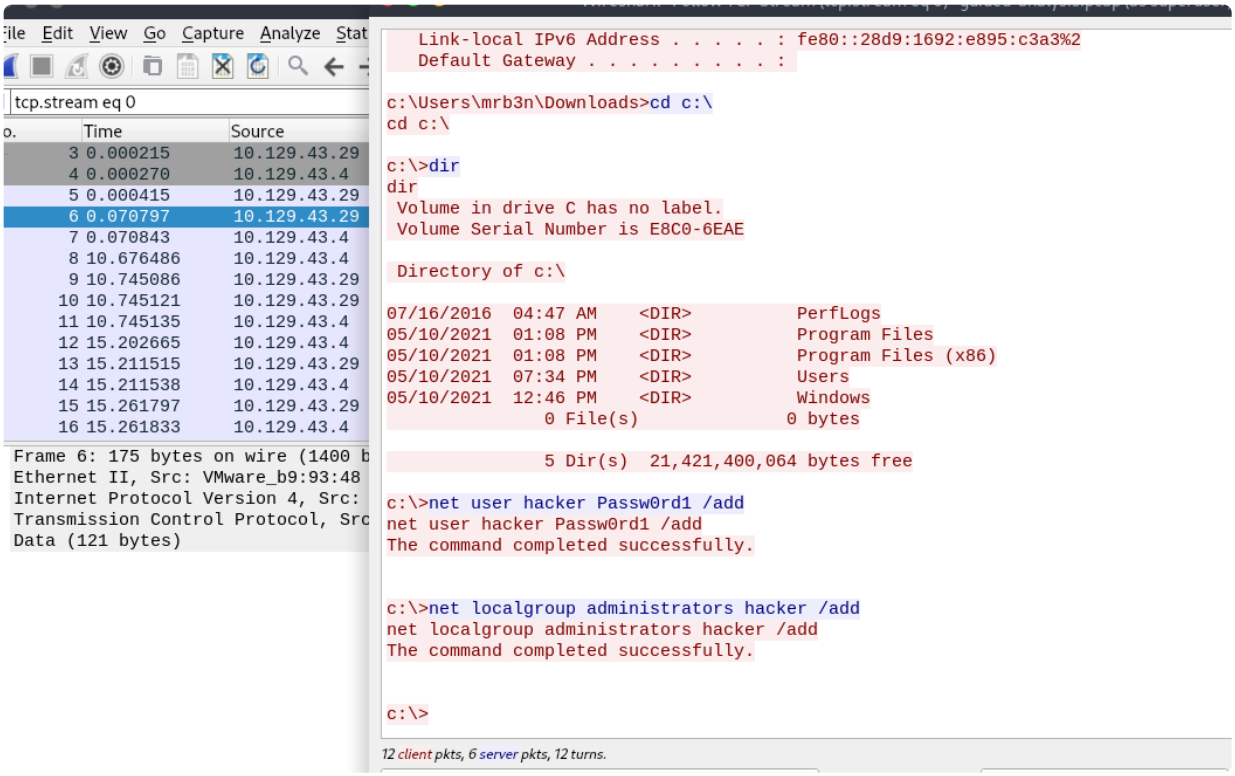


-> It is the user bob suspected of doing malicious stuff.

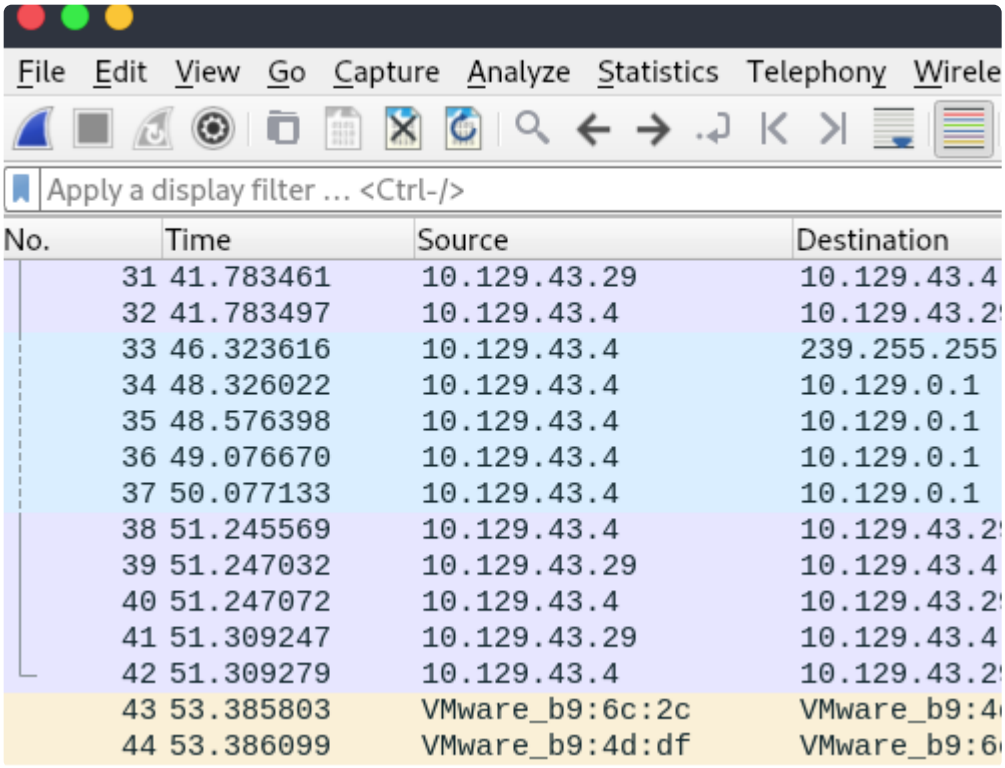
Guided Lab: Traffic Analysis Workflow

Question

- What was the name of the new user created on mrb3n's host?
  -> Following the TCP stream, we see it is the user Bob being created as administrator.

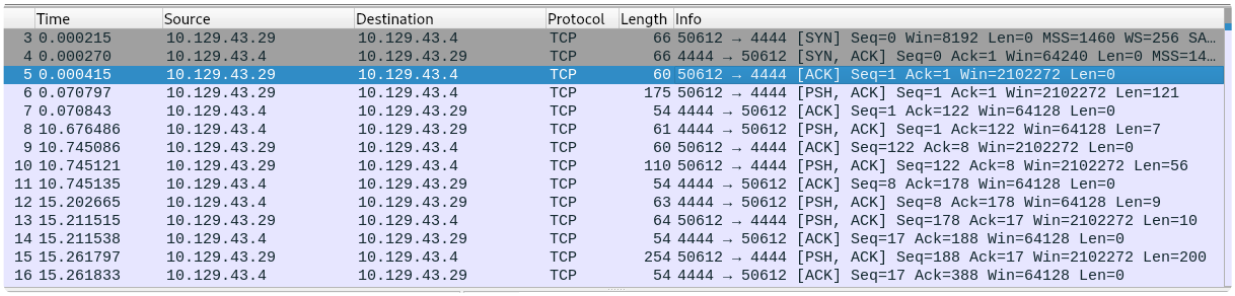


- How many total packets were there in the Guided-analysis PCAP?
  -> Scrolling to the very bottom, we see there are 44 packets in the PCAP file.



- What was the suspicious port that was being used?
  -> We see that the suspicious port being used is port 4444 from the host 10.129.43.4

(also the compromised host that attacker tried to connect to)



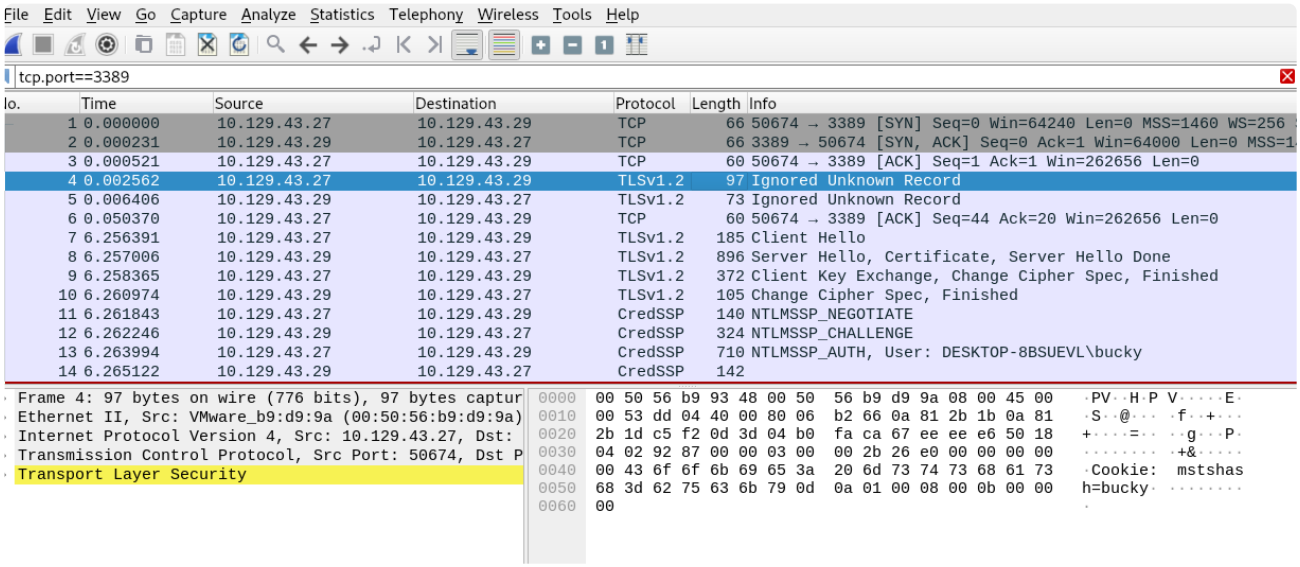
	Time	Source	Destination	Protocol	Length	Info
3	0.000215	10.129.43.29	10.129.43.4	TCP	66	50612 → 4444 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA…
4	0.000270	10.129.43.4	10.129.43.29	TCP	66	4444 → 50612 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=14…
5	0.000415	10.129.43.29	10.129.43.4	TCP	60	50612 → 4444 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
6	0.070797	10.129.43.29	10.129.43.4	TCP	175	50612 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=121
7	0.070843	10.129.43.4	10.129.43.29	TCP	54	4444 → 50612 [ACK] Seq=1 Ack=122 Win=64128 Len=0
8	10.676486	10.129.43.4	10.129.43.29	TCP	61	4444 → 50612 [PSH, ACK] Seq=1 Ack=122 Win=64128 Len=7
9	10.745086	10.129.43.29	10.129.43.4	TCP	60	50612 → 4444 [ACK] Seq=122 Ack=8 Win=2102272 Len=0
10	10.745121	10.129.43.29	10.129.43.4	TCP	110	50612 → 4444 [PSH, ACK] Seq=122 Ack=8 Win=2102272 Len=56
11	10.745135	10.129.43.4	10.129.43.29	TCP	54	4444 → 50612 [ACK] Seq=8 Ack=178 Win=64128 Len=0
12	15.202665	10.129.43.4	10.129.43.29	TCP	63	4444 → 50612 [PSH, ACK] Seq=8 Ack=178 Win=64128 Len=9
13	15.211515	10.129.43.29	10.129.43.4	TCP	64	50612 → 4444 [PSH, ACK] Seq=178 Ack=17 Win=2102272 Len=10
14	15.211538	10.129.43.4	10.129.43.29	TCP	54	4444 → 50612 [ACK] Seq=17 Ack=188 Win=64128 Len=0
15	15.261797	10.129.43.29	10.129.43.4	TCP	254	50612 → 4444 [PSH, ACK] Seq=188 Ack=17 Win=2102272 Len=200
16	15.261833	10.129.43.4	10.129.43.29	TCP	54	4444 → 50612 [ACK] Seq=17 Ack=388 Win=64128 Len=0

Decrypting RDP connections

Question

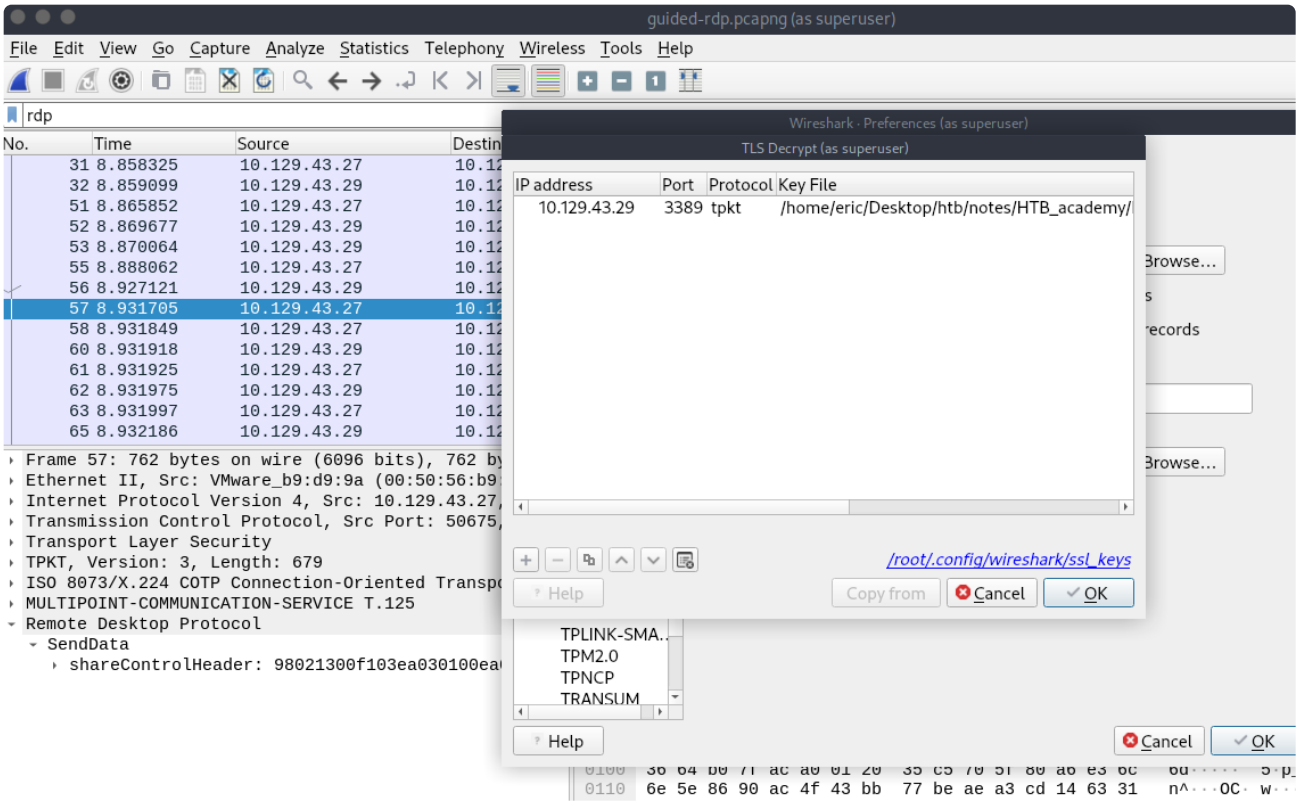
- What user account was used to initiate the RDP connection?

-> When we examine one of the records (ignored unknown record) when filtering for TCP port 3389, we see that



-> Hence, the user is bucky.

or, we would use the key given as follows



-> And filter out for rdp protocols on display filter, where we see on clientinfo, we see the username is bucky with password Welcome1.