CLab 10: Secure Networked Applications – Web Access

Joshua Ludolf
CSCI 4406 – Computer Networks

- To start this lab, I had to configure my fabric by running utilizing the blogs GitHub repo (git checkout, additionally had to modify cell 14):

```
import pandas as pd
pd.set_option('display.max_colwidth', None)

# Assuming fablib is an instance of FablibManager
ssh_str = 'ssh -i ' + slice.get_slice_private_key_file() + \
    ' -J ' + fablib.get_bastion_username() + '@' + fablib.get_bastion_host() + \
    ' -F /home/fabric/work/fabric_config/ssh_config '

slice_info = [{'Name': n.get_name(), 'SSH command': ssh_str + n.get_username() + '@' + str(n.get_management_ip())} for n in slice.get_nodes()]
pd.DataFrame(slice_info).set_index('Name')
```

```
Retry: 11, Time: 272 sec
```

Slice

ID	8d6c8390-a291-4545-b1ce-ccea9955ae19
Name	Joshua Ludolf Secure-Applications_jludo01
Lease Expiration (UTC)	2024-11-07 15:39:47 +0000
Lease Start (UTC)	2024-11-06 15:39:47 +0000
Project ID	a70de2f5-9e12-4b6b-b412-0ae1a2c553b0
State	StableOK

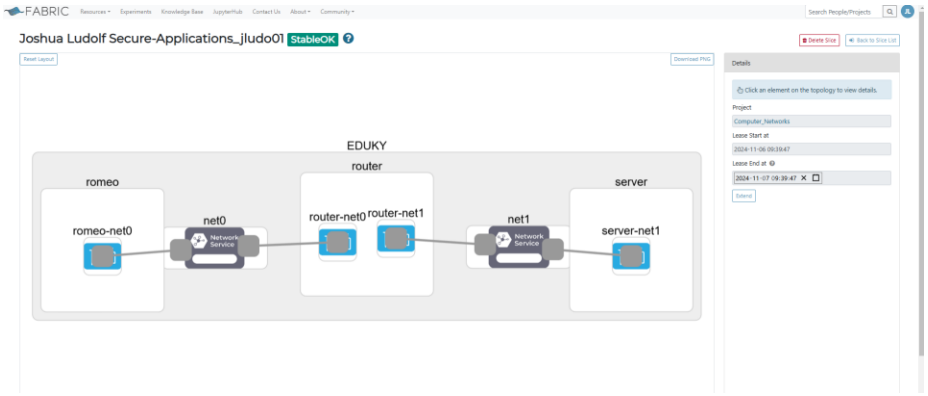
Networks

ID	Name	Layer	Type	Site	Subnet	Gateway	State	Error
669d50c7-3808-409f-a7ad-c3a89547f860	net0	L2	L2Bridge	EDUKY	None	None	Active	
3d8a0a55-64a0-42e5-8c43-b2bee86d5371	net1	L2	L2Bridge	EDUKY	None	None	Active	

Interfaces

Name	Short Name	Node	Network	Bandwidth	Mode	VLAN	MAC	Physical Device	Device	IP Address	Numa Node	Switch Port
romeo-net0-p1	p1	romeo	net0	100	config		1E:A5:A4:33:B4:B1	enp7s0	enp7s0	fe80::1ca5:a4ff:fe33:b4b1	1	HundredGigE0/0/0/34
router-net0-p1	p1	router	net0	100	config		1A:B3:86:14:30:B0	enp8s0	enp8s0	fe80::18b3:86ff:fe14:30b0	1	HundredGigE0/0/0/29
router-net1-p1	p1	router	net1	100	config		1A:78:5D:39:3D:D6	enp7s0	enp7s0	fe80::1878:5dff:fe39:3dd6	1	HundredGigE0/0/0/29
server-net1-p1	p1	server	net1	100	config		1A:79:0A:04:A3:DA	enp7s0	enp7s0	fe80::1879:aff:fe04:a3da	1	HundredGigE0/0/0/21

```
Time to print interfaces 288 seconds
'8d6c8390-a291-4545-b1ce-ccea9955ae19'
```



SSH command

Name	
romeo	ssh -i /home/fabric/work/fabric_config/slice_key -J jludo01_0000228382@bastion.fabric-testbed.net -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fee8:f504
router	ssh -i /home/fabric/work/fabric_config/slice_key -J jludo01_0000228382@bastion.fabric-testbed.net -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fe6c:6c20
server	ssh -i /home/fabric/work/fabric_config/slice_key -J jludo01_0000228382@bastion.fabric-testbed.net -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fe1a:2dc5

- From there, I followed the instructions from https://witestlab.poly.edu/blog/secure-networked-applications/ , starting from Web Access section:

- First, I needed to update “romeo” node and installed lynx (no issues at all 😎).

```
ubuntu@romeo:~$ sudo apt update
Get:1 http://nova.clouds.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:3 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [3303 kB]
Get:5 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Get:6 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [483 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [14.3 kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [3247 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [456 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [548 B]
Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [1014 kB]
Get:13 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
Get:14 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [214 kB]
Get:15 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [21.4 kB]
Get:16 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [24.8 kB]
Get:17 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5968 B]
Get:18 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [540 B]
Get:19 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:20 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:21 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:22 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:23 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [3692 kB]
Get:24 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [562 kB]
Get:25 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:26 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [3367 kB]
Get:27 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [471 kB]
Get:28 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [548 B]
Get:29 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1237 kB]
Get:30 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [297 kB]
Get:31 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [28.3 kB]
Get:32 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [27.0 kB]
Get:33 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [7936 B]
Get:34 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [612 B]
Get:35 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main amd64 Packages [45.7 kB]
Get:36 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main Translation-en [16.3 kB]
Get:37 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main amd64 c-n-f Metadata [1420 B]
Get:38 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/restricted amd64 c-n-f Metadata [116 B]
Get:39 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [25.0 kB]
Get:40 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe Translation-en [16.3 kB]
Get:41 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f Metadata [880 B]
Get:42 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/multiverse amd64 c-n-f Metadata [116 B]
Fetched 33.5 MB in 5s (6666 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
73 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@romeo:~$
```

```
ubuntu@romeo:~$ sudo apt -y install lynx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libidn11 lynx-common
The following NEW packages will be installed:
  libidn11 lynx lynx-common
0 upgraded, 3 newly installed, 0 to remove and 73 not upgraded.
Need to get 1586 kB of archives.
After this operation, 5731 kB of additional disk space will be used.
Get:1 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libidn11 amd64 1.33-2.2ubuntu2 [46.2 kB]
Get:2 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 lynx-common all 2.9.0dev.5-1 [914 kB]
Get:3 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 lynx amd64 2.9.0dev.5-1 [626 kB]
Fetched 1586 kB in 0s (4402 kB/s)
Selecting previously unselected package libidn11:amd64.
(Reading database ... 64102 files and directories currently installed.)
Preparing to unpack .../libidn11_1.33-2.2ubuntu2_amd64.deb ...
Unpacking libidn11:amd64 (1.33-2.2ubuntu2) ...
Selecting previously unselected package lynx-common.
Preparing to unpack .../lynx-common_2.9.0dev.5-1_all.deb ...
Unpacking lynx-common (2.9.0dev.5-1) ...
Selecting previously unselected package lynx.
Preparing to unpack .../lynx_2.9.0dev.5-1_amd64.deb ...
Unpacking lynx (2.9.0dev.5-1) ...
Setting up libidn11:amd64 (1.33-2.2ubuntu2) ...
Setting up lynx-common (2.9.0dev.5-1) ...
Setting up lynx (2.9.0dev.5-1) ...
update-alternatives: using /usr/bin/lynx to provide /usr/bin/www-browser (www-browser) in auto mode
Processing triggers for libc-bin (2.31-0ubuntu9.16) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
ubuntu@romeo:~$
```

- On the "server" node, I install the Apache web server after updating the “server” node (no issues at all 😍).

```
ubuntu@server:~$ sudo apt update
Get:1 http://nova.clouds.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [3303 kB]
Get:4 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:5 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Get:6 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [483 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [14.3 kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [3247 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [456 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [548 B]
Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [1014 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [214 kB]
Get:14 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
Get:15 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [21.4 kB]
Get:16 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [24.8 kB]
Get:17 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5968 B]
Get:18 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [540 B]
Get:19 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:20 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:21 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:22 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:23 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [3692 kB]
Get:24 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [562 kB]
Get:25 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:26 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [3367 kB]
Get:27 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [471 kB]
Get:28 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [548 B]
Get:29 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1237 kB]
Get:30 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [297 kB]
Get:31 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [28.3 kB]
Get:32 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [27.0 kB]
Get:33 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [7936 B]
Get:34 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [612 B]
Get:35 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main amd64 Packages [45.7 kB]
Get:36 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main Translation-en [16.3 kB]
Get:37 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main amd64 c-n-f Metadata [1420 B]
Get:38 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/restricted amd64 c-n-f Metadata [116 B]
Get:39 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [25.0 kB]
Get:40 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe Translation-en [16.3 kB]
Get:41 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f Metadata [880 B]
Get:42 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/multiverse amd64 c-n-f Metadata [116 B]
Fetched 33.5 MB in 5s (6801 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
73 packages can be upgraded. Run 'apt list --upgradable' to see them.

ubuntu@server:~$ sudo apt -y install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
0 upgraded, 11 newly installed, 0 to remove and 73 not upgraded.
Need to get 1875 kB of archives.
After this operation, 8121 kB of additional disk space will be used.
Get:1 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 libapr1 amd64 1.6.5-1ubuntu1.1 [91.5 kB]
Get:2 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 libaprutil1 amd64 1.6.1-4ubuntu2.2 [85.1 kB]
Get:3 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-4ubuntu2.2 [10.5 kB]
Get:4 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 libaprutil1-ldap amd64 1.6.1-4ubuntu2.2 [8752 B]
Get:5 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libjansson4 amd64 2.12-1build1 [28.9 kB]
Get:6 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.2-0 amd64 5.2.4-1.1build3 [106 kB]
Get:7 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-bin amd64 2.4.41-4ubuntu3.21 [1189 kB]
Get:8 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-data all 2.4.41-4ubuntu3.21 [159 kB]
Get:9 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-utils amd64 2.4.41-4ubuntu3.21 [84.7 kB]
Get:10 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2 amd64 2.4.41-4ubuntu3.21 [95.6 kB]
Get:11 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 ssl-cert all 1.0.39 [17.0 kB]
Fetched 1875 kB in 1s (1687 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1:amd64.
(Reading database ... 64102 files and directories currently installed.)
Preparing to unpack .../00-libapr1_1.6.5-1ubuntu1.1_amd64.deb ...
Unpacking libapr1:amd64 (1.6.5-1ubuntu1.1) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../01-libaprutil1_1.6.1-4ubuntu2.2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.6.1-4ubuntu2.2) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
Preparing to unpack .../02-libaprutil1-dbd-sqlite3_1.6.1-4ubuntu2.2_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.1-4ubuntu2.2) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
Preparing to unpack .../03-libaprutil1-ldap_1.6.1-4ubuntu2.2_amd64.deb ...
Unpacking libaprutil1-ldap:amd64 (1.6.1-4ubuntu2.2) ...
Selecting previously unselected package libjansson4:amd64.
Preparing to unpack .../04-libjansson4_2.12-1build1_amd64.deb ...
Unpacking libjansson4:amd64 (2.12-1build1) ...
Selecting previously unselected package liblua5.2-0:amd64.
```

- Then, I generated a self-signed certificate and key for it, which will be used to authenticate the server and to establish an encrypted connection to the server (no

issues at all 😍).

```
ubuntu@server:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/ssl-cert-snakeoil.key -out /etc/ssl/certs/ssl-cert-snakeoil.pem
Generating a RSA private key
..............+++++
.....................................................................+++++
writing new private key to '/etc/ssl/private/ssl-cert-snakeoil.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Texas
Locality Name (eg, city) []:San Antonio
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Texas A&M University of San Antonio
Organizational Unit Name (eg, section) []:Computer Networks
Common Name (e.g. server FQDN or YOUR name) []:server
Email Address []:Jludo01@jaguar.tamu.edu
ubuntu@server:~$
```

- From there, I edited the config file for the SSL-enabled version of the site, by adding the server name.

- Next, I enabled the SSL module for Apache and the new SSL-enabled site, and restart the service (no issues at all 😍).

```
ubuntu@server:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
ubuntu@server:~$
```

```
ubuntu@server:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
ubuntu@server:~$
```

```
ubuntu@server:~$ sudo systemctl restart apache2
ubuntu@server:~$
```

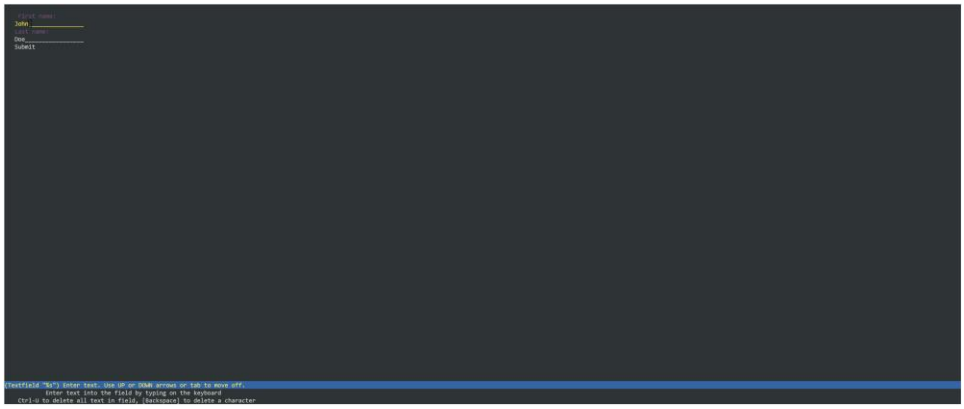
- Then, I created a form for data entry on my new site.

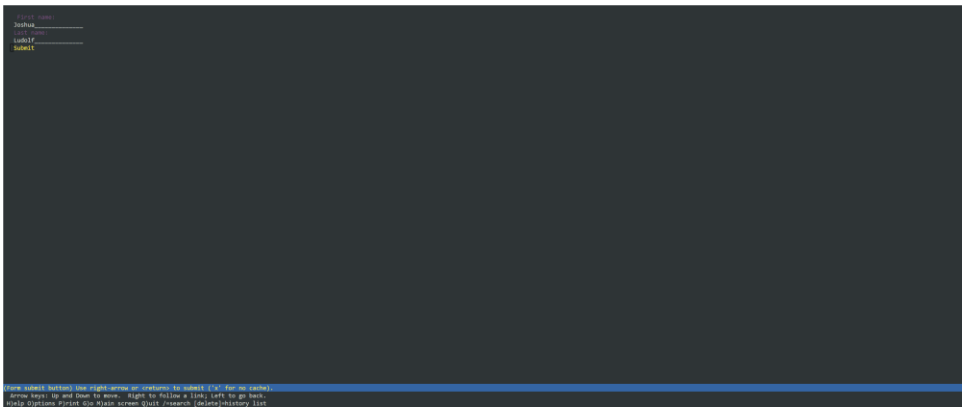
- From there I opened a new HTML file as shown.

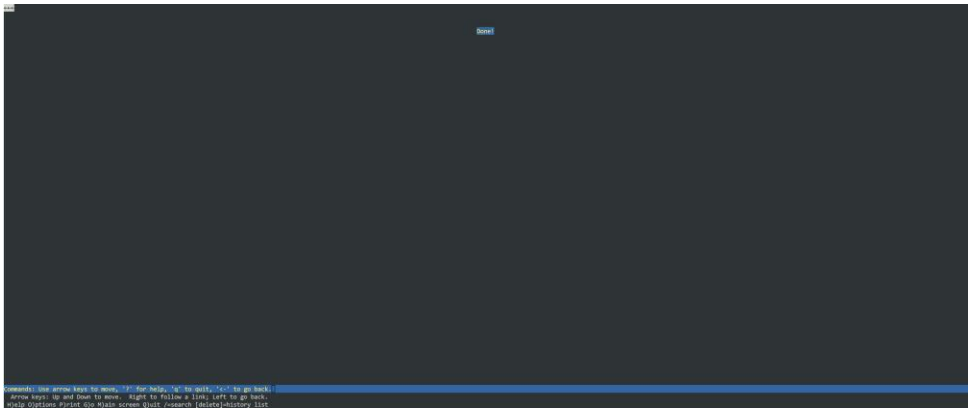
- Now that everything is prepared on the server. I'll be able to compare HTTP vs. HTTPS access to this web form. On the "romeo" host, run - sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev)[^]+") -w security-http-$(hostname -s).pcap:

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-http-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

- While this was running, I initiated an HTTP session from "romeo" to "server" - on "romeo" by running - lynx http://server/form.html



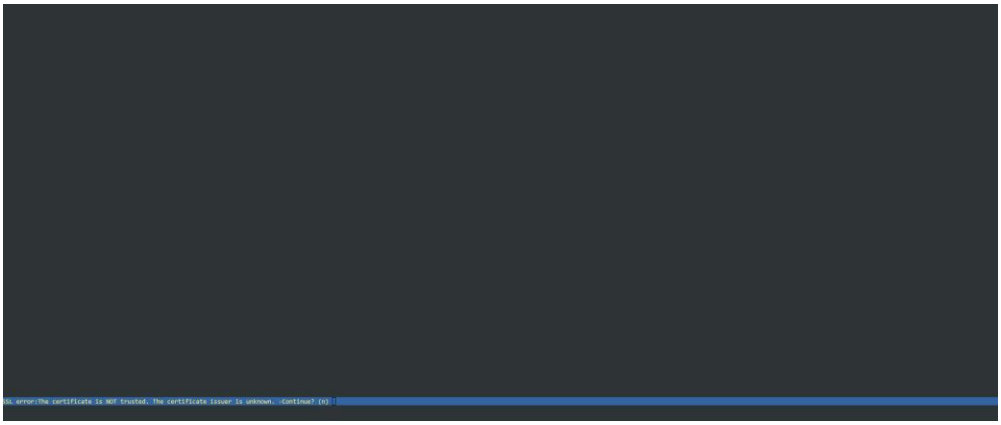


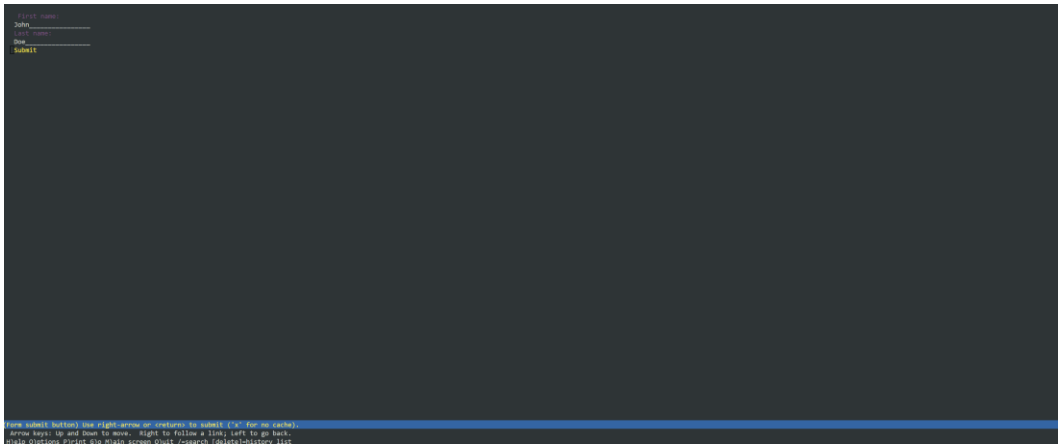


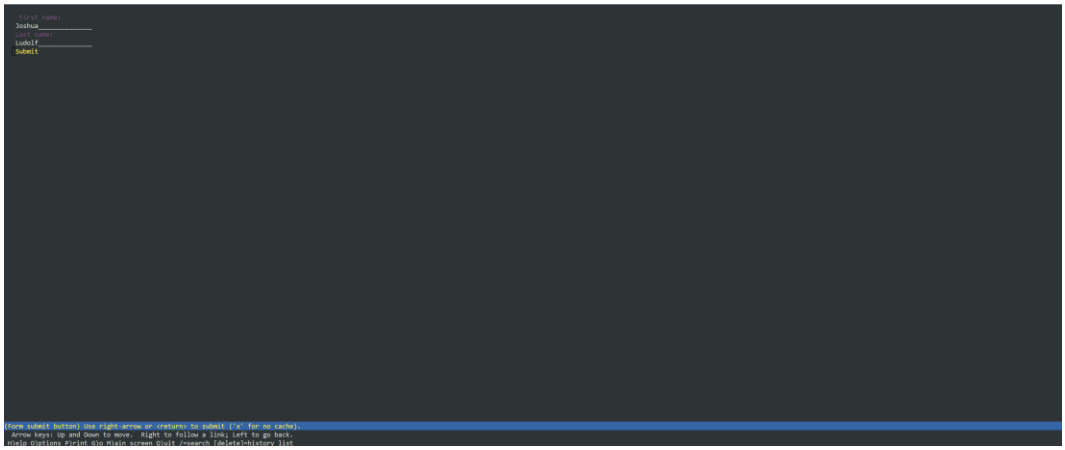
```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-http-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C28 packets captured
28 packets received by filter
0 packets dropped by kernel
ubuntu@romeo:~$
```

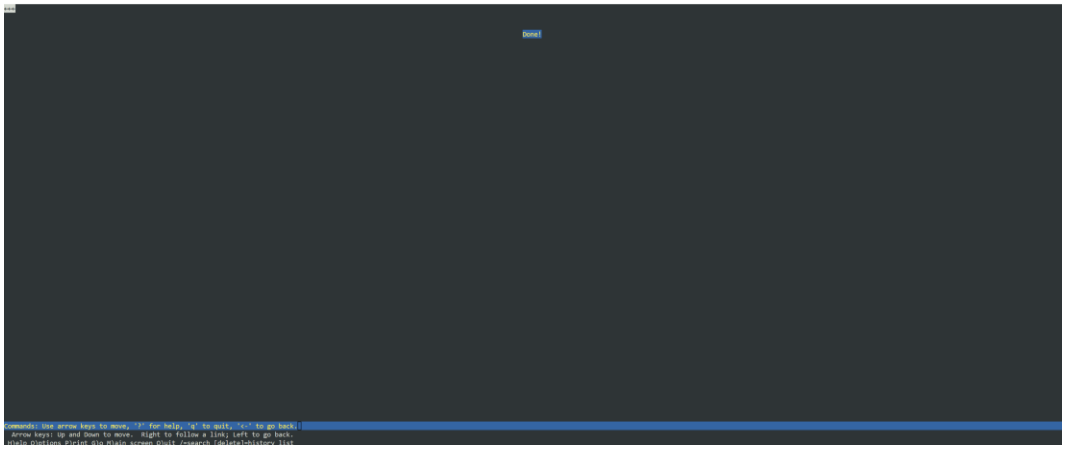
- Then ran the following command on “romeo” node - sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev)[^]+") -w security-https-$(hostname -s).pcap – to capture traffic on the network segment. This packet capture will show me what is visible to anyone eavesdropping on the network segment (same as last time but I got warned as the certificate was self-signed 😊):

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-https-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```





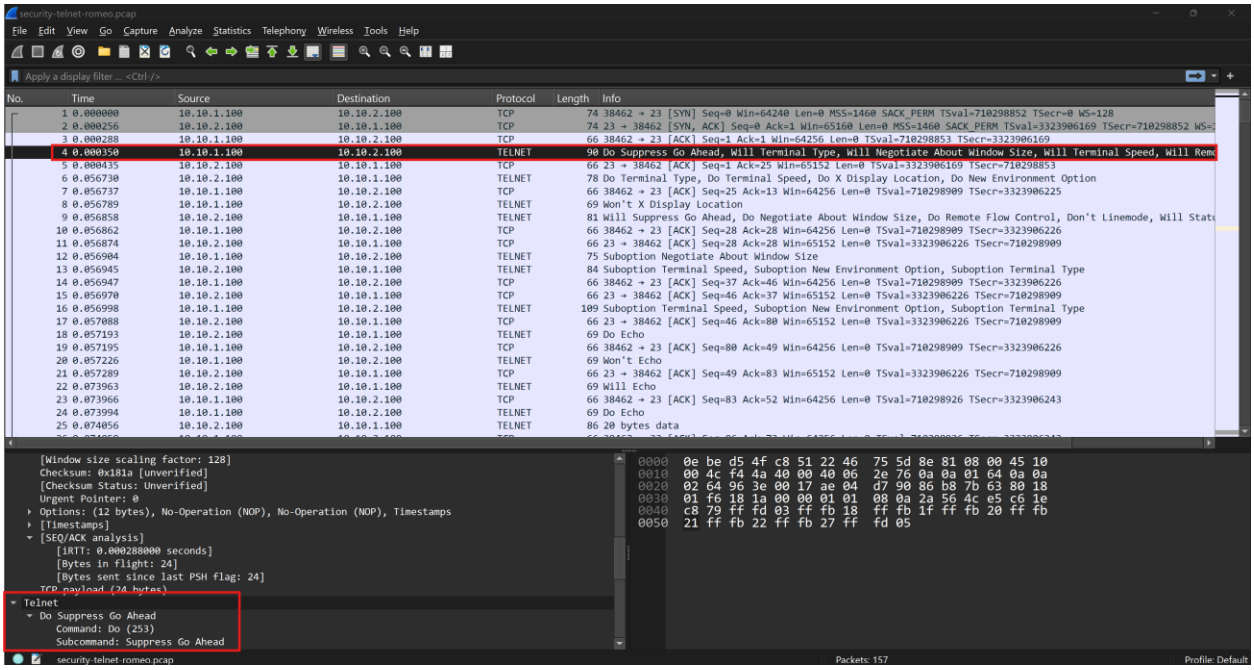


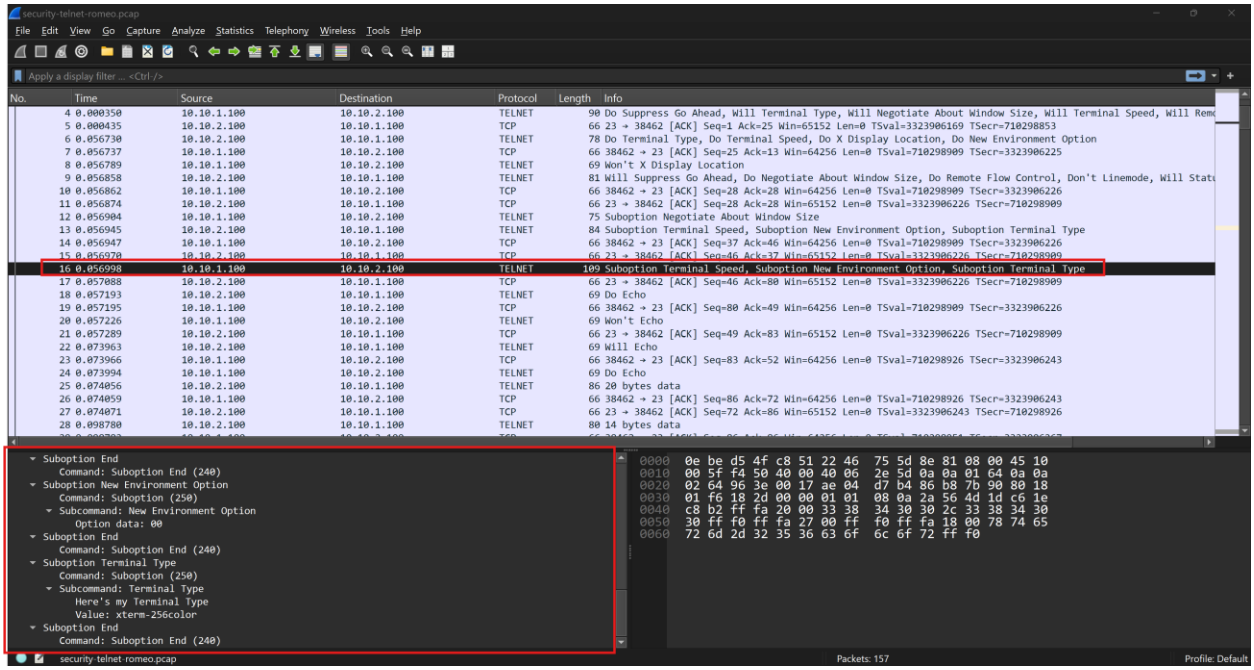



```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-https-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C52 packets captured
52 packets received by filter
0 packets dropped by kernel
ubuntu@romeo:~$
```

Lab 9

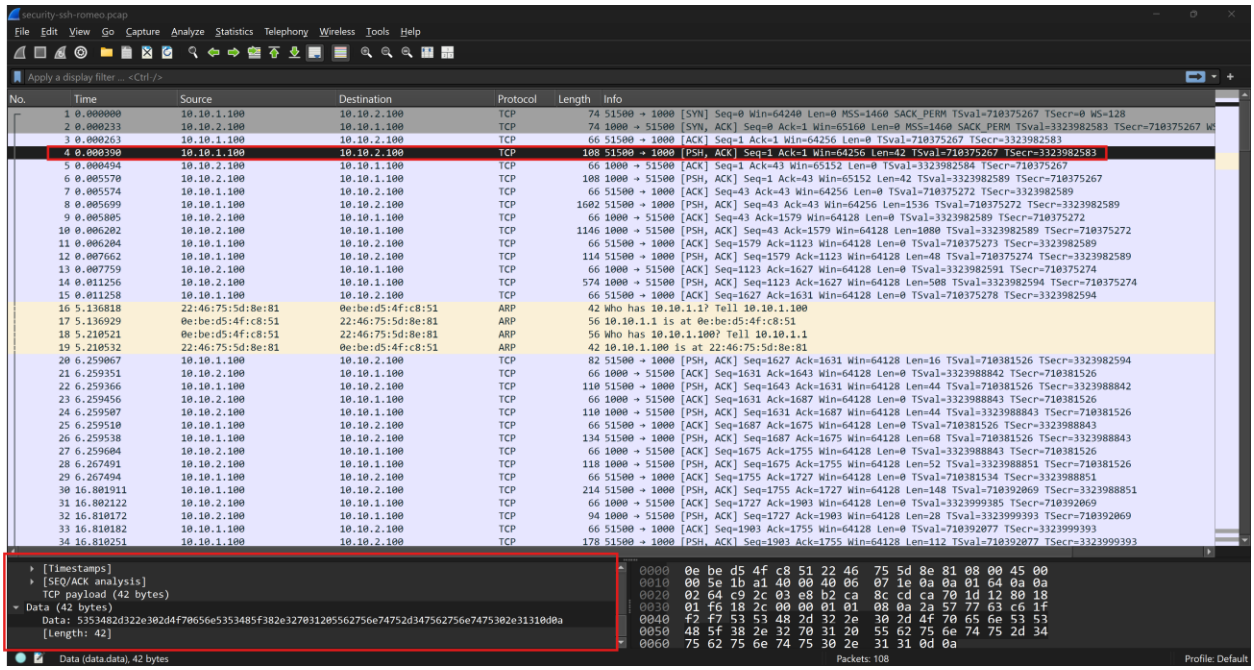
1. In the packet capture of the telnet experiment, can you read: the username and password? IP/TCP headers? Session data? Show evidence.





We can see the TCP & IP headers and we can see the commands, thus not very encrypted (we can see user information if we did bit more digging).

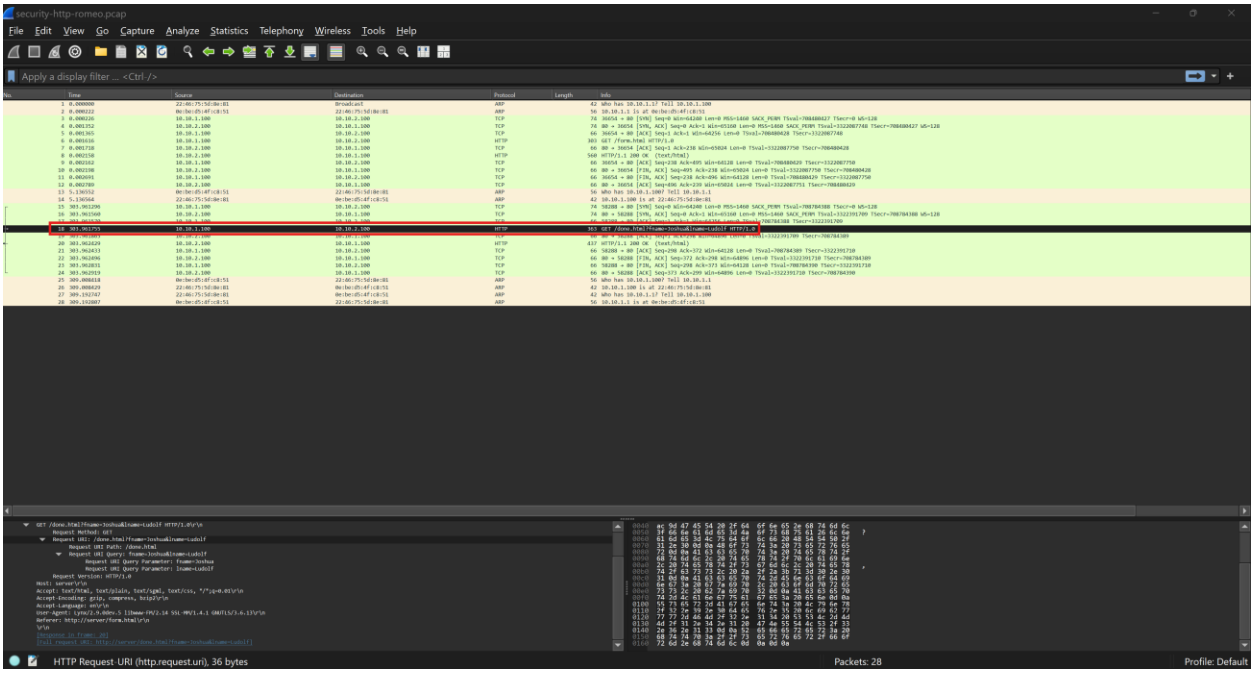
2. In the packet capture of the SSH experiment, can you read: the username and password? IP/TCP headers? Session data? Show evidence.



We can see the TCP and IP headers, but we can't get username and password as it's encrypted.

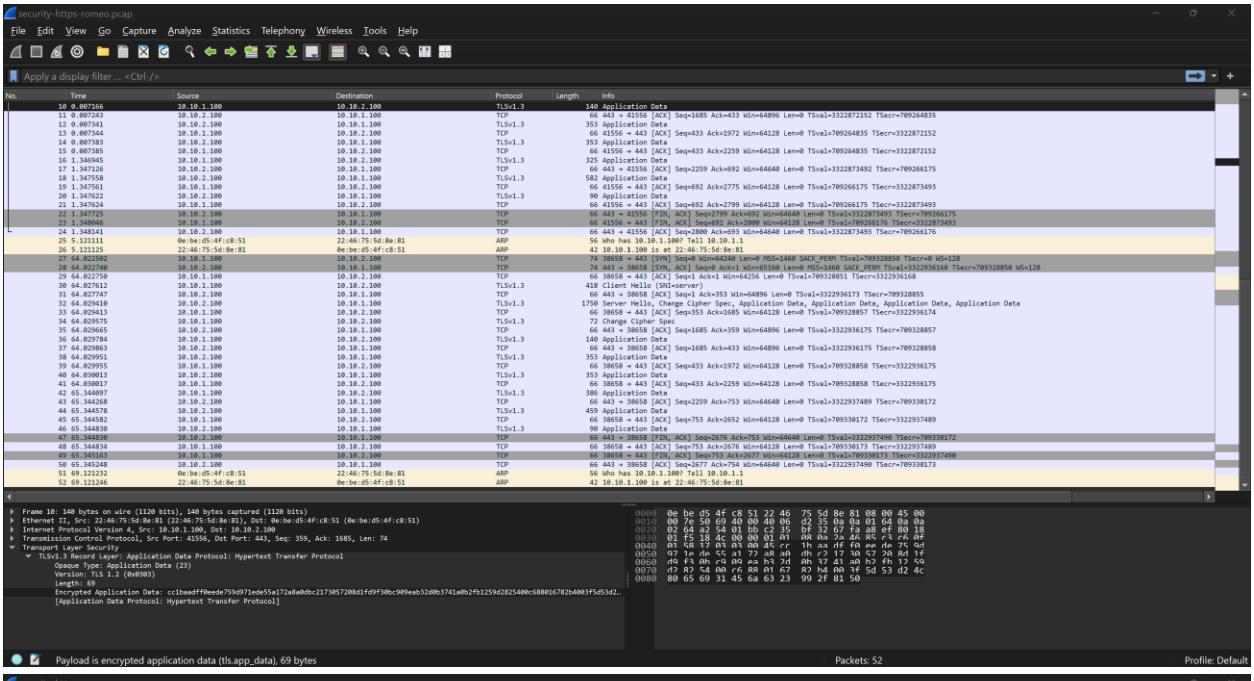
Lab 10

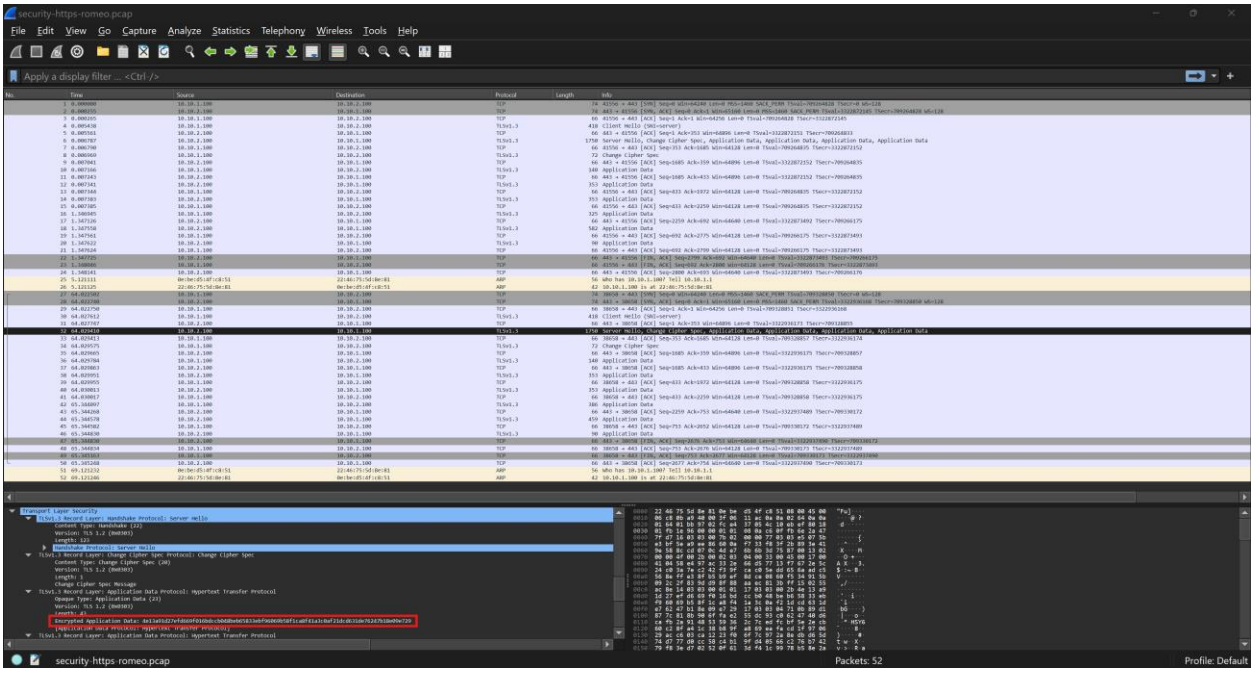
3. In the packet capture of the HTTP experiment, can you read: the IP and TCP headers? The contents of the HTTP GET (including the name of the page you visited, form.html)? The data you entered in the form? Show evidence.



I was able to read the contents from the form, additionally, was able to see the TCP and IP headers.

4. In the packet capture of the HTTPS experiment, can you read: the IP and TCP headers? The contents of the HTTP GET (including the name of the page you visited, form.html)? The data you entered in the form? Show evidence.





We can't see the packets, but we can see the headers of the TCP and IP of the packets.

- Summary of what I learned from this lab:

Through this lab exercise on comparing HTTP and HTTPS, I've gained a wealth of insights and practical experience. First, I set up a web server on a Linux machine, specifically the "server" node, by installing and configuring Apache. I also generated a self-signed SSL certificate to enable HTTPS, learning the importance of securing web traffic. By creating simple HTML forms for data entry, I could see firsthand how HTTP transmits data in plaintext, making it vulnerable to eavesdropping. Capturing network traffic with tcpdump, I analyzed the differences between HTTP and HTTPS using Wireshark, noting that HTTPS encrypts data, keeping it secure. I also navigated browser warnings about self-signed certificates, understanding the need for trusted certificates in real-world applications. This exercise reinforced my skills in command-line operations, configuration management, and network security, making me more adept at ensuring secure web communications. The hands-on experience with tools like Lynx and the practical setup of SSL/TLS added significant value to my learning, preparing me for real-world scenarios in network administration and cybersecurity.