

در تمامی تصاویر از ترمینال، ساعت و تاریخ در پایین ترمینال (قسمت سیز رنگ) مشخص است.

راه‌اندازی سرور HTTP با احراز هویت کاربری

1. نصب وب‌سرور Apache

برای این کار، مراحل زیر را طی می‌کنیم:

```
sudo apt update  
sudo apt install apache2
```

با این کار، نرم‌افزار apache بر روی سرور نصب می‌شود.

```
sudo ufw app list  
sudo ufw allow 'Apache'  
sudo ufw status  
sudo systemctl status apache2
```

با انجام این دستورات، تنظیمات firewall را تغییر داده و اجازه دسترسی به apache (برای پورت 80) را می‌دهد و سپس، وضعیت سرویس apache را مشاهده می‌کند.

The screenshot shows a terminal window titled 'tmux' with several command-line entries. The user runs 'sudo apt update', 'sudo apt install apache2', 'sudo ufw app list', 'sudo ufw allow 'Apache'', 'sudo ufw status', and 'sudo systemctl status apache2'. The output shows the Apache service is active and running. The log at the bottom indicates the server is starting and facing a domain name resolution issue.

```
Fetched 97.8 kB in 1s (95.8 kB/s)  
Selecting previously unselected package apache2.  
(Reading database ... 272738 files and directories currently installed.)  
Preparing to unpack .../apache2_2.4.52-1ubuntu4.7_amd64.deb ...  
Unpacking apache2 (2.4.52-1ubuntu4.7) ...  
Setting up apache2 (2.4.52-1ubuntu4.7) ...  
apache-htcacheclean.service is a disabled or a static unit not running, not starting it.  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...  
Rules updated for profile 'Apache'  
  
> sudo ufw app list  
Available applications:  
 Apache  
 Apache Full  
 Apache Secure  
 CUPS  
 OpenSSH  
> sudo ufw allow 'Apache'  
Skipping adding existing rule  
Skipping adding existing rule (v6)  
> sudo ufw status  
Status: inactive  
> sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)  
     Active: active (running) since Fri 2023-11-24 19:58:14 +0330; 32s ago  
       Docs: https://httpd.apache.org/docs/2.4/  
 Main PID: 11100 (apache2)  
    Tasks: 55 (limit: 18382)  
   Memory: 5.0M  
    CPU: 51ms  
   CGroup: /system.slice/apache2.service  
         ├─11100 /usr/sbin/apache2 -k start  
         ├─11101 /usr/sbin/apache2 -k start  
         └─11102 /usr/sbin/apache2 -k start  
  
Nov 24 19:58:14 Patrick systemd[1]: Starting The Apache HTTP Server...  
Nov 24 19:58:14 Patrick apachectl[11099]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' di  
Nov 24 19:58:14 Patrick systemd[1]: Started The Apache HTTP Server.  
Lines 1-16/16 (END)  
[root@patrick ~]
```

حال یک virtual host به نام patrick را به کانفیگ apache اضافه می‌کنیم.

```
sudo mkdir /var/www/patrick  
sudo chown -R $USER:$USER /var/www/patrick  
sudo chmod -R 755 /var/www/patrick  
sudo nvim /var/www/patrick/index.html
```

و داده زیر را در آن قرار می‌دهیم:

```
<html>
  <head>
    <title>Welcome to Patrick!</title>
  </head>
  <body>
    <h1>Success! The Patrick virtual host is working!</h1>
  </body>
</html>
```

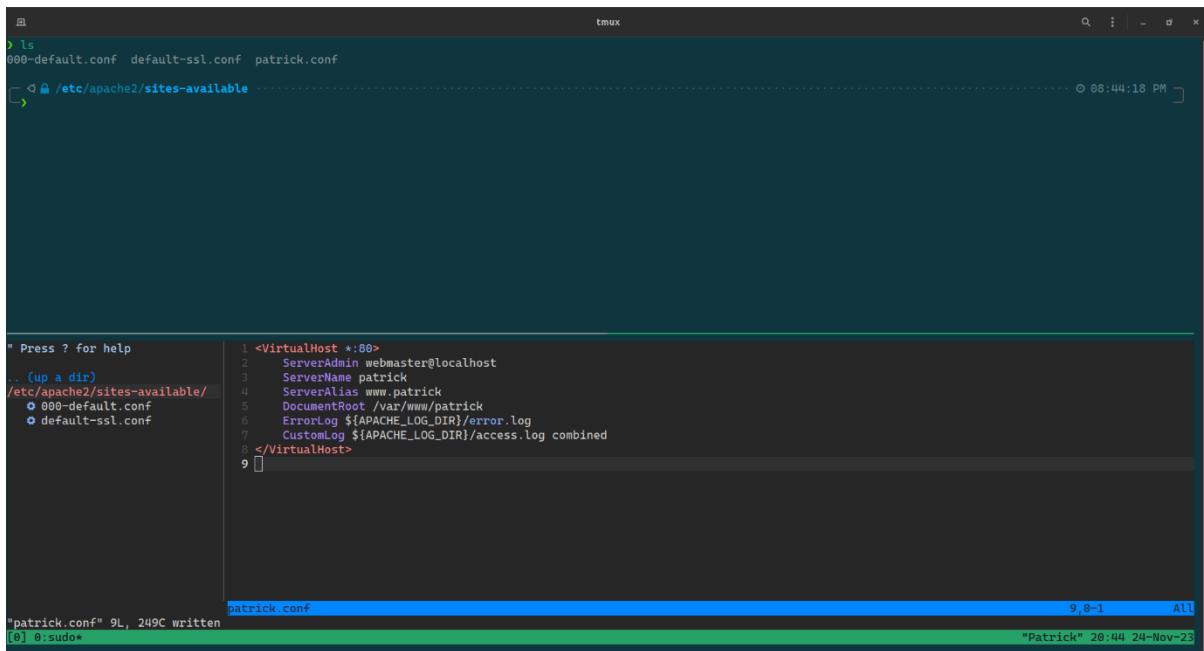
The screenshot shows a tmux session with two panes. The top pane displays terminal commands: `sudo mkdir patrick`, `sudo chown -R \$USER:\$USER patrick`, and `sudo chmod -R 755 patrick`. The bottom pane shows a file editor with the content of index.html. The file contains the HTML code provided above. The status bar at the bottom indicates the file is 9L, 167C written, and the session is titled "Patrick".

حال به کمک دستور و مقادیر زیر، این virtual host را کانفیگ می‌کنیم:

```
sudo nvim /etc/apache2/sites-available/patrick.conf
```

مقدار زیر را در آن قرار می‌دهیم:

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  ServerName patrick
  ServerAlias www.patrick
  DocumentRoot /var/www/patrick
  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```



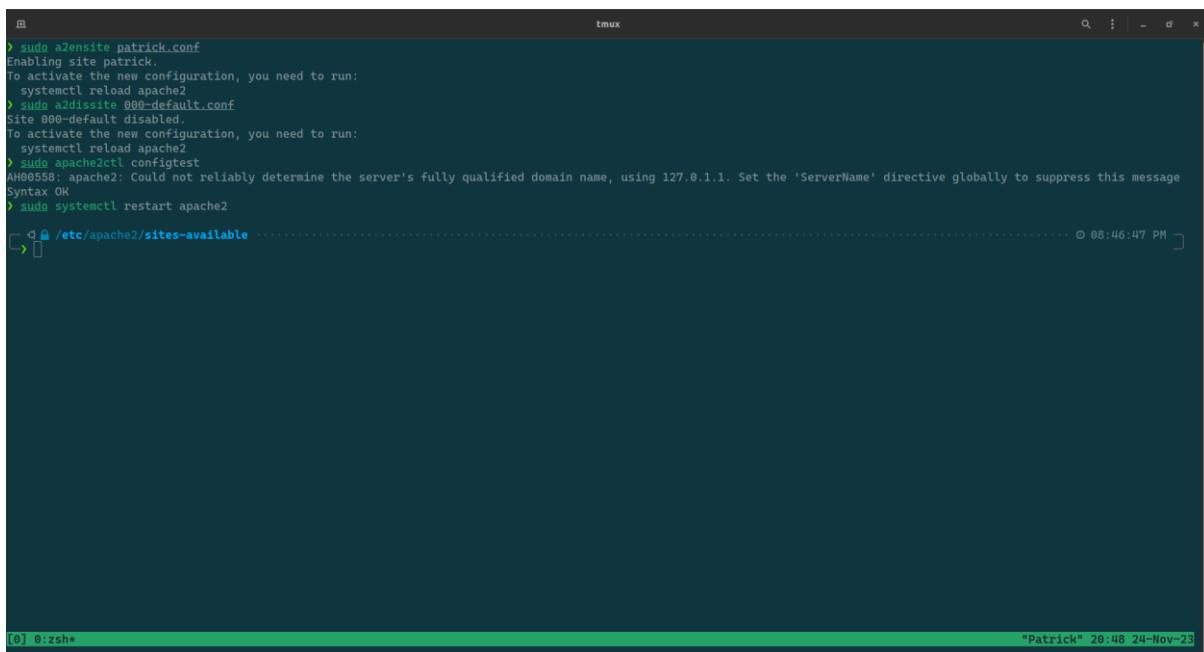
A screenshot of a tmux session titled "tmux". The session has two panes. The left pane shows the command `ls` run in the directory `/etc/apache2/sites-available`, listing files: `000-default.conf`, `default-ssl.conf`, and `patrick.conf`. The right pane shows the contents of the `patrick.conf` file:

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName patrick
    ServerAlias www.patrick
    DocumentRoot /var/www/www.patrick
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

The status bar at the bottom indicates "patrick.conf" was written with 9L, 249C, and shows the date "24-Nov-23".

حال با استفاده از دستورات زیر، ابتدا سایت قبلی را غیر فعال کرده، سایت جدید را فعال کرده، درستی کانفیگ را تست کرده و سرویس apache را ریاستارت می‌کنیم:

```
sudo a2ensite patrick.conf
sudo a2dissite 000-default.conf
sudo apache2ctl configtest
sudo systemctl restart apache2
```



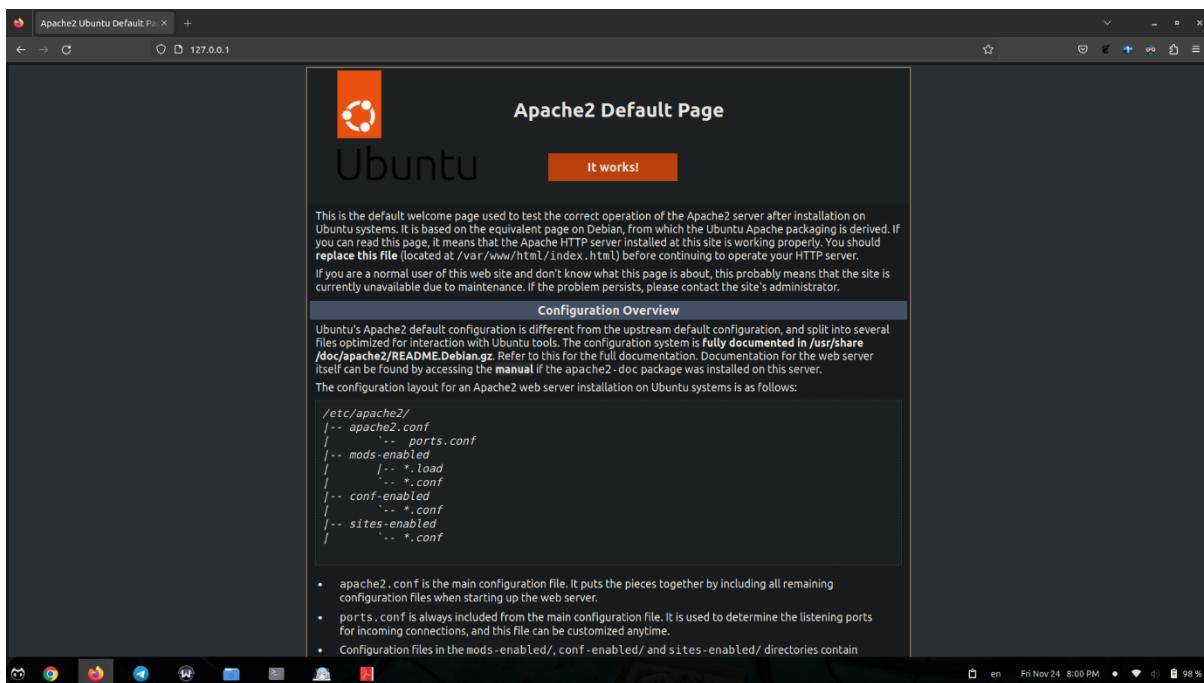
A screenshot of a tmux session titled "tmux". The session has two panes. The left pane shows the execution of the following commands:

```
sudo a2ensite patrick.conf
Enabling site patrick.
To activate the new configuration, you need to run:
  systemctl reload apache2
sudo a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
sudo systemctl restart apache2
```

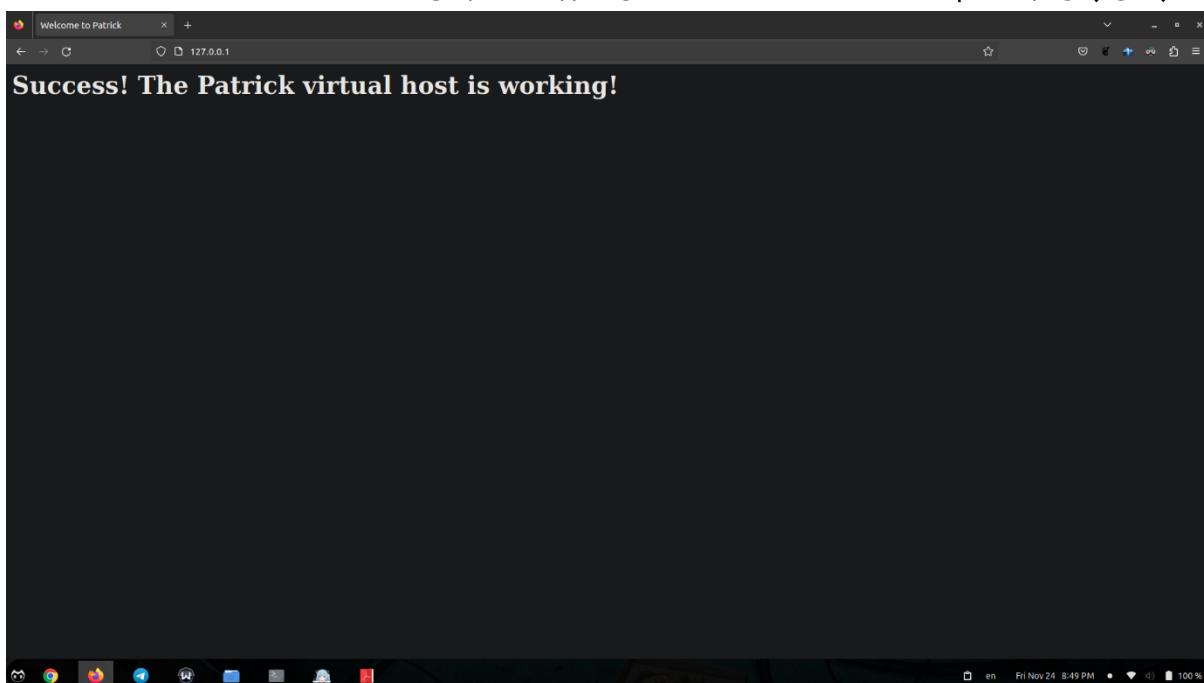
The right pane shows the command `ls` run in the directory `/etc/apache2/sites-available`. The status bar at the bottom indicates the date "24-Nov-23".

2. مشاهده صفحه سایت

پیش از تنظیم virtual host، صفحه نمایش داده شده به صورت زیر است:



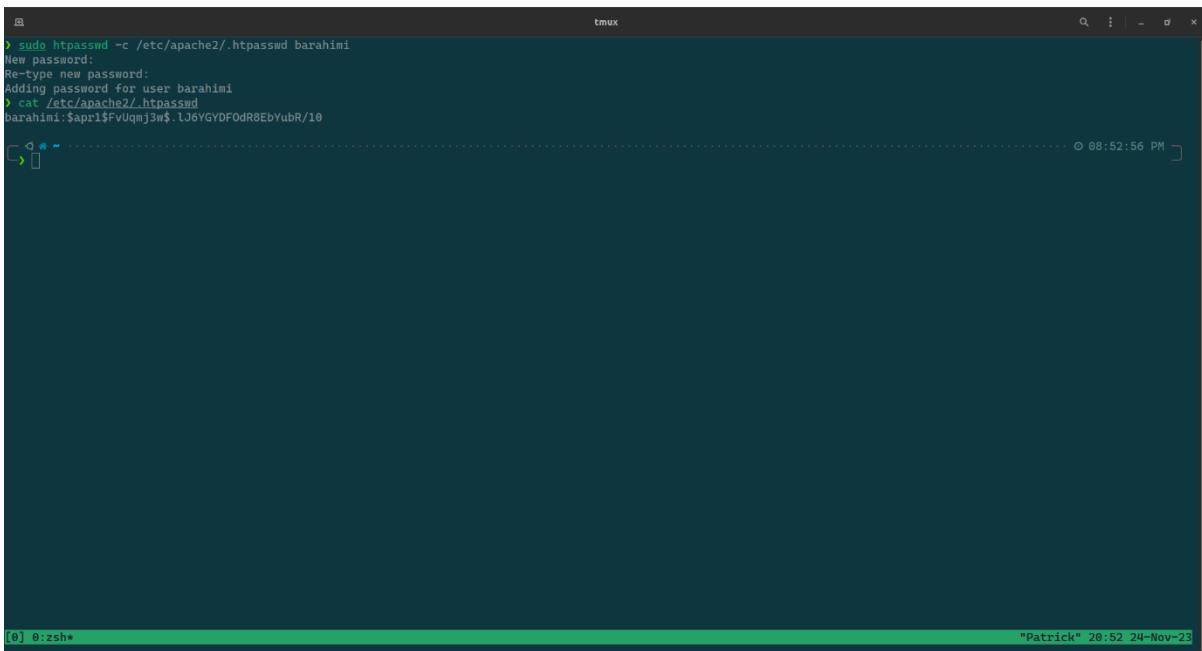
همچنین پس از تنظیم سایت patrick، صفحه به این صورت تغییر می‌کند:



3. تنظیم احراز هویت برای سرویس

ابتدا با استفاده از دستور زیر، یک یوزر جدید تعریف کرده و سپس مقدار قرار داده شده در فایل را مشاهده می‌کنیم. در این بخش، یوزرنیم برابر با barahimi و پسورد برابر با 1234 است.

```
sudo htpasswd -c /etc/apache2/.htpasswd barahimi
cat /etc/apache2/.htpasswd
```



```
tmux
> sudo htpasswd -c /etc/apache2/.htpasswd barahimi
New password:
Re-type new password:
Adding password for user barahimi
> cat /etc/apache2/.htpasswd
barahimi:$apr1$FvU0mJ3m$,L36YGYDF0dR8EbYubR/10
[0] 0:zsh*                                         "Patrick" 20:52 24-Nov-23
```

حال باید کانفیگ قبلی را طوری عوض کرده که از این فایل برای authorization استفاده کند.

```
sudo nvim /etc/apache2/sites-available/patrick.conf
```

مقدار زیر را به این فایل اضافه می‌کنیم:

```
<Directory "/var/www/patrick">
    AuthType Basic
    AuthName "Restricted Content"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
</Directory>
```

سپس دستورات زیر را اجرا می‌کنیم:

```
sudo apache2ctl configtest
sudo systemctl restart apache2
sudo systemctl status apache2
```

The screenshot shows a tmux session with one window titled "tmux". Inside the window, several terminal commands are being run:

```
> ls
000-default.conf default-ssl.conf patrick.conf
> sudo apache2ctl configtest
[sudo] password for pasha:
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
syntax OK
> sudo systemctl restart apache2
> sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-11-24 21:23:21 +0330; 3s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Process: 17338 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 17348 (apache2)
   Tasks: 55 (limit: 18382)
    Memory: 5.0M
      CPU: 46ms
     CGroup: /system.slice/apache2.service
             ├─17342 /usr/sbin/apache2 -k start
             ├─17343 /usr/sbin/apache2 -k start
             └─17344 /usr/sbin/apache2 -k start

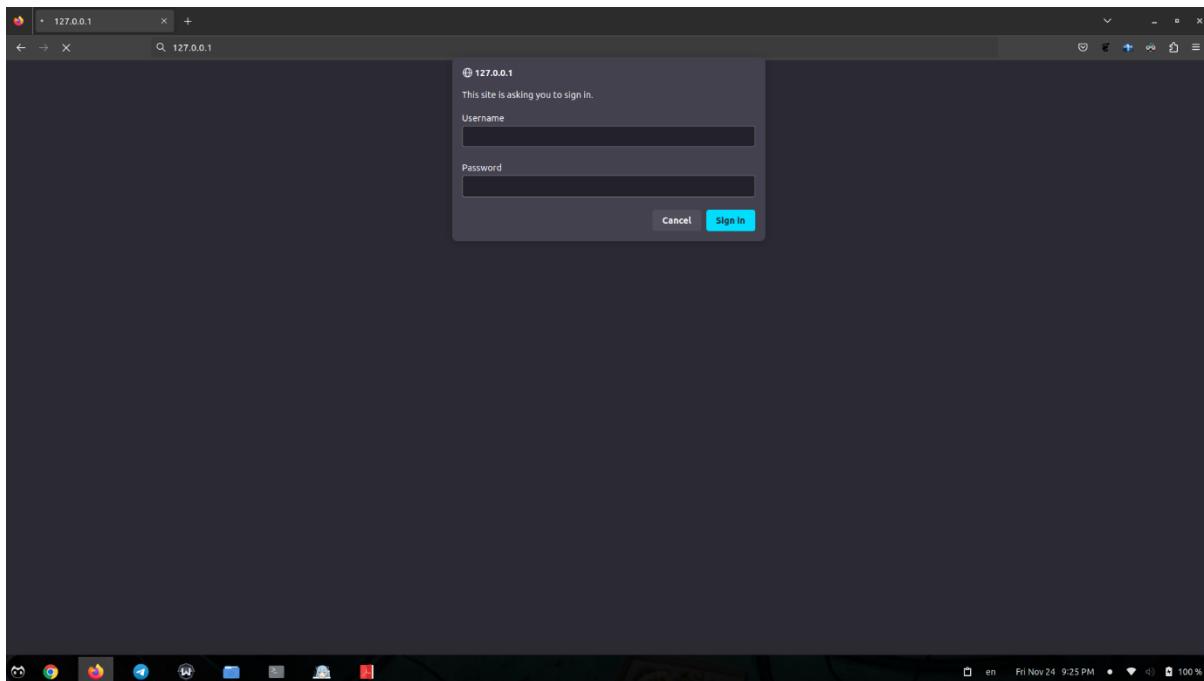
* Press ? for help
.. (up a dir)
/etc/apache2/sites-available/
  • 000-default.conf
  • default-ssl.conf
  • patrick.conf

1 <VirtualHost *:80>
2   ServerAdmin webmaster@localhost
3   ServerName patrick
4   ServerAlias www.patrick
5   DocumentRoot /var/www/patrick
6   ErrorLog ${APACHE_LOG_DIR}/error.log
7   CustomLog ${APACHE_LOG_DIR}/access.log combined
8
9   <Directory "/var/www/patrick">
10     AuthType Basic
11     AuthName "Restricted Content"
12     AuthUserFile /etc/apache2/.htpasswd
13     Require valid-user
14   </Directory>
15 </VirtualHost>
16

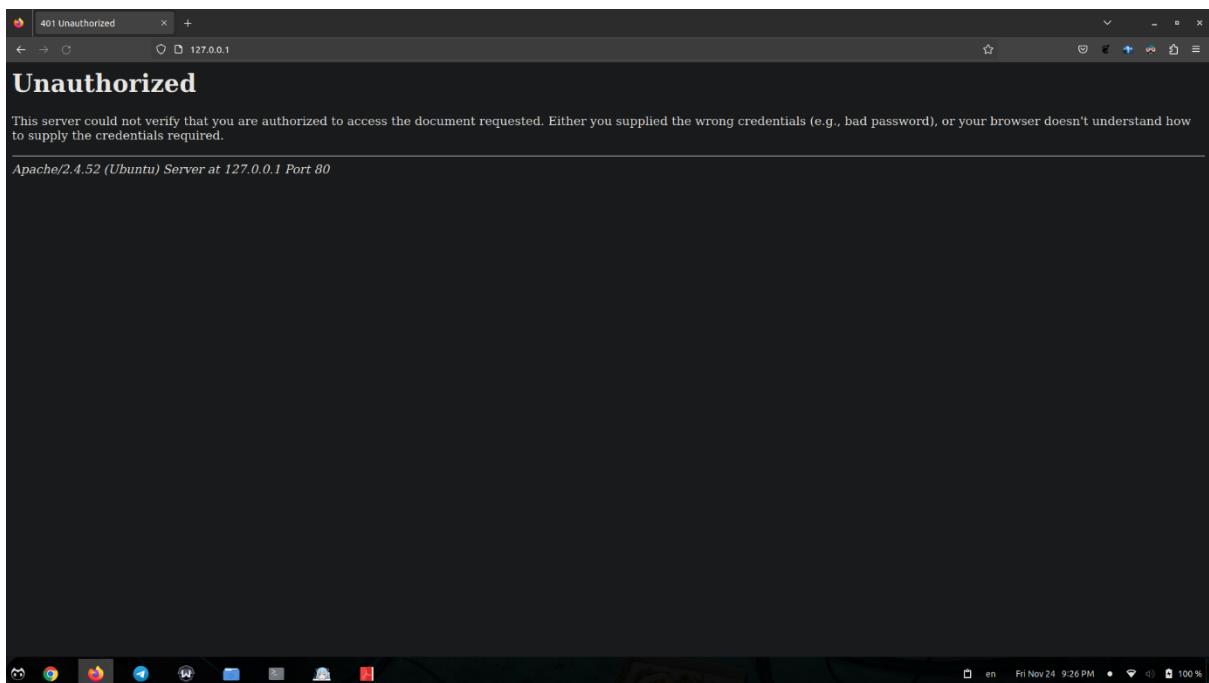
patrick.conf" 16L, 434C written
[6] 0:[tmux]*
```

The terminal also shows the current file being edited is "patrick.conf". The status bar at the bottom indicates the file was written at 21:23 on Friday, November 24, 2023.

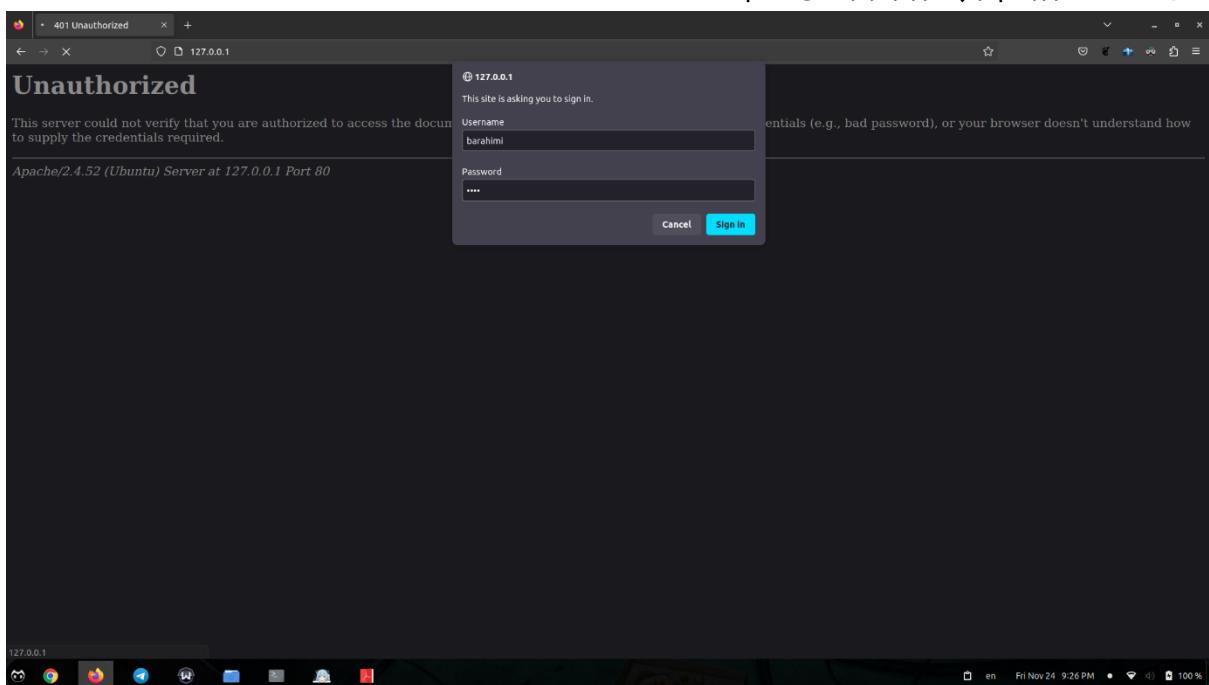
حال اگر صفحه را ریلود کنیم، مشاهده می‌کنیم که یوزرنیم و پسورد از ما خواسته می‌شود:



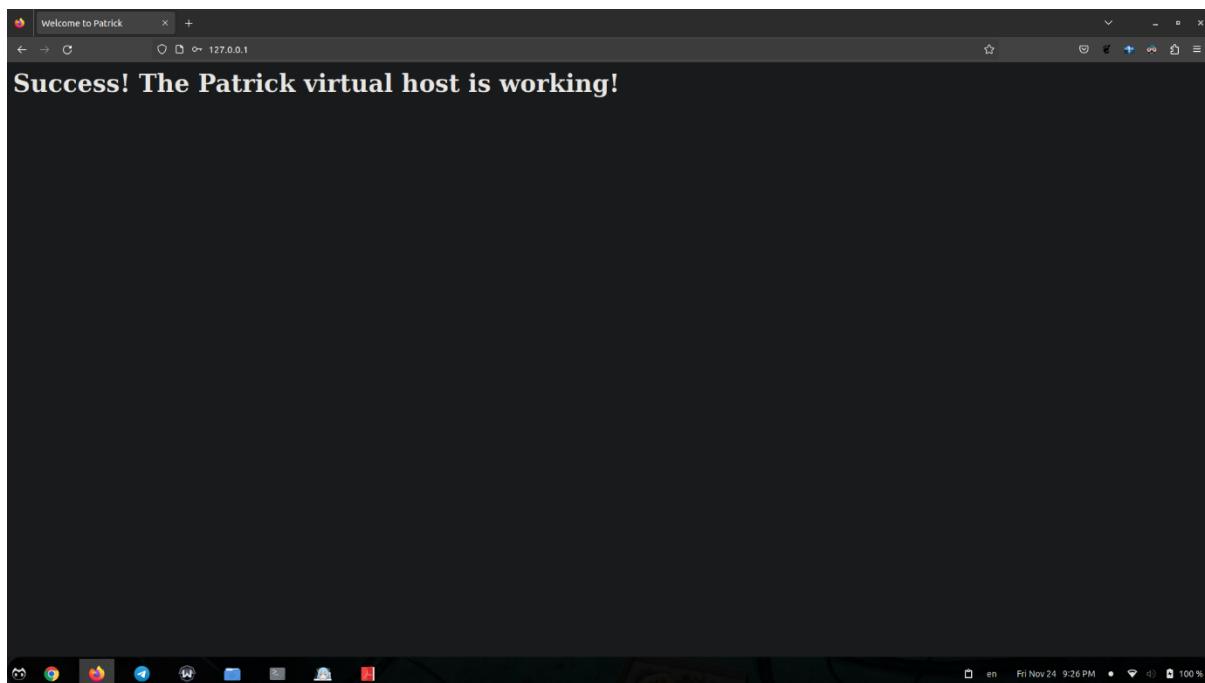
اگر این موارد را وارد نکنیم و یا اشتباه وارد کنیم، با صفحه زیر مواجه می‌شویم:



حال مجدداً یوزرنیم و پسورد را وارد می‌کنیم:

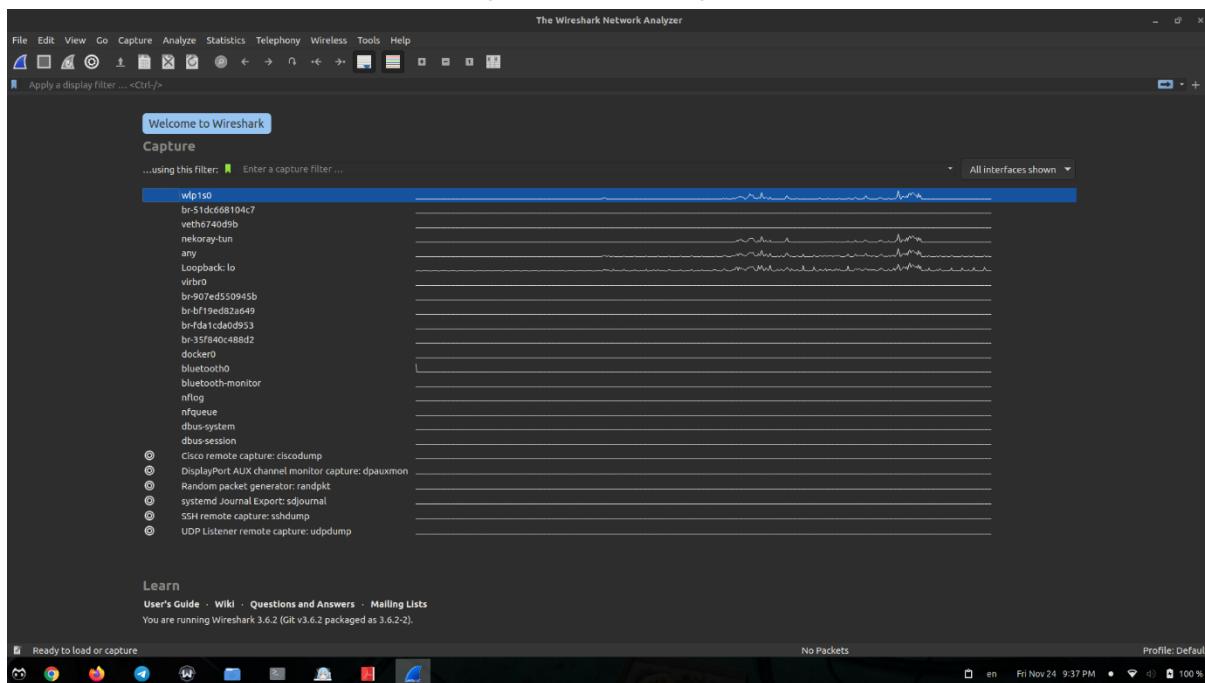


و با صفحه زیر مواجه می‌شویم:



4. نصب wireshark

در این مرحله اقدام به نصب wireshark می‌کنیم. با توجه به اینکه این برنامه از پیش روی سیستم من نصب بوده است، تنها به گذاشتن تصویری از این نرم‌افزار بسنده می‌کنم:

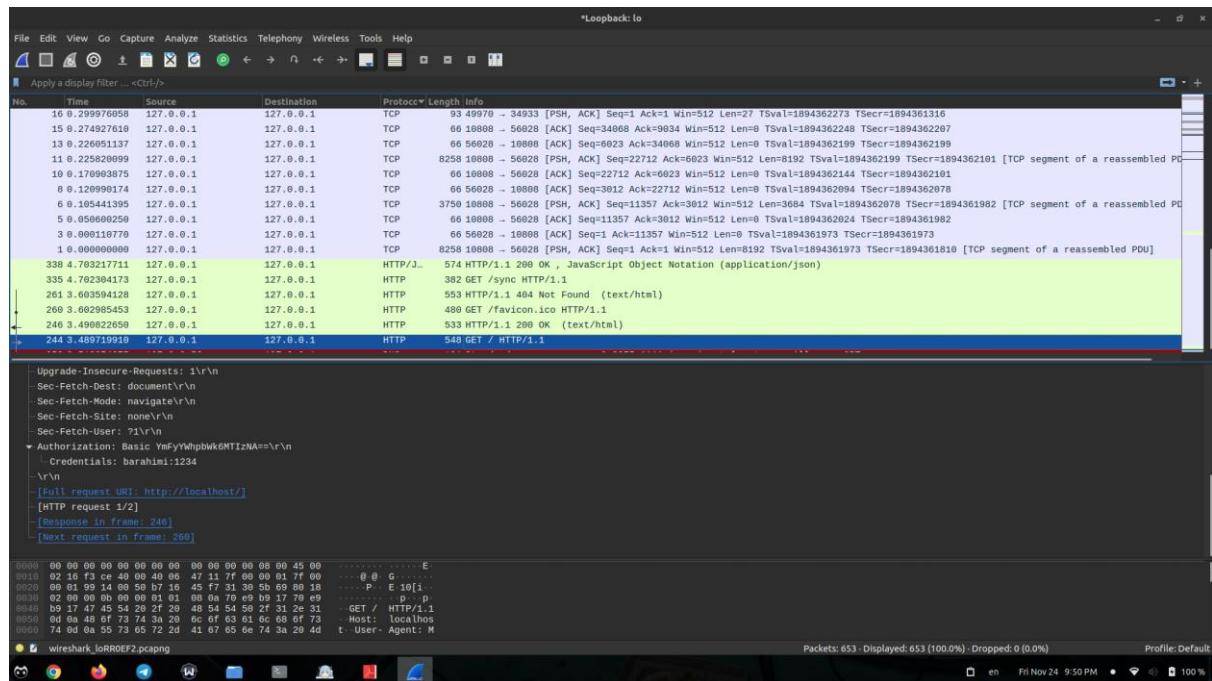


5. ضبط بسته‌های HTTP

در این زمان wireshark را روی (lo) interface قرار داده و ضبط را شروع می‌کنیم. مجدداً صفحه سایت را ریلود کرده و یوزرنیم و پسورد را وارد می‌کنیم و سپس، ضبط wireshark را متوقف می‌کنیم. برخی از بسته‌های دریافت شده به صورت زیر هستند:

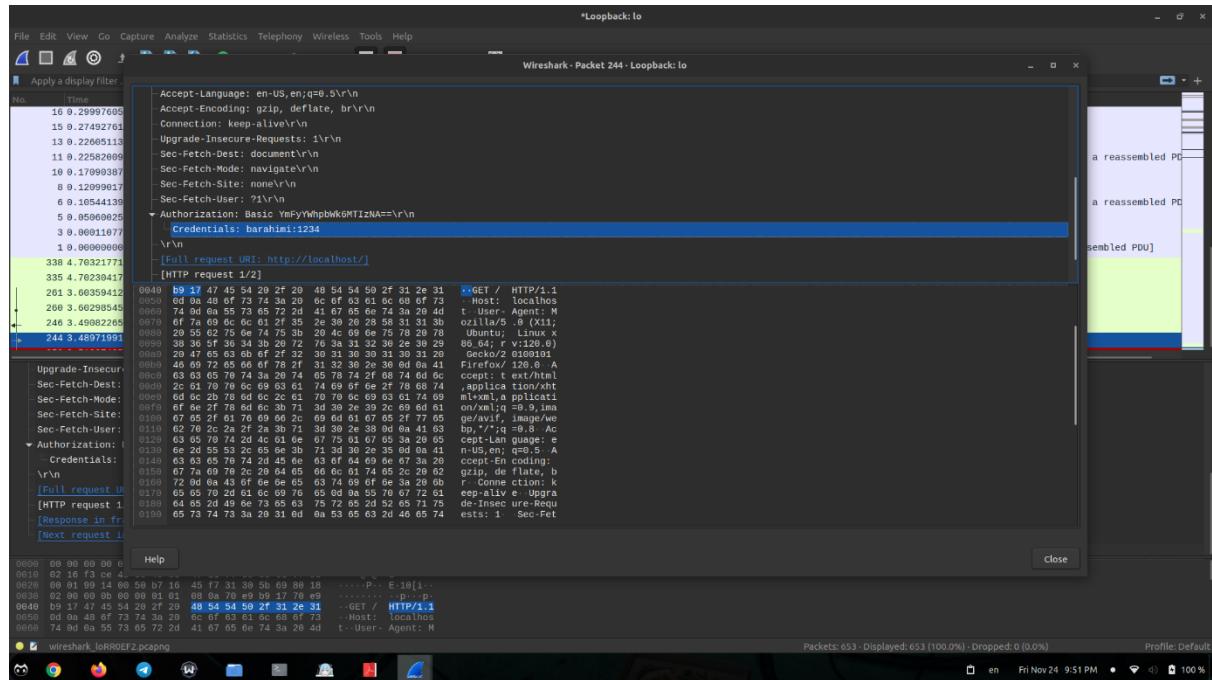
مبانی امنیت شبکه‌های کامپیوتری

تمرین کامپیوتری اول



6. مشاهده اطلاعات بسته ضبط شده

حال یکی از بسته‌های HTTP را باز کرده و بخش Authorization را مشاهده می‌کنیم:



همانطور که مشاهده می‌شود، در فیلد barahimi:1234، عبارت credentials می‌دانیم که قرار داده شده و یوزرنیم و پسورد به راحتی قابل مشاهده هستند.

7. علت امکان شنود اطلاعات احراز هویت کاربری

می‌دانیم که پسورد کاربر به صورت hash شده در سرور ذخیره شده و فرآیند انجام این hash را خود سرور انجام می‌دهد. در نتیجه لازم است کلاینت سوزرنیم و پسورد را به صورت خام برای سرور ارسال کند تا سرور بتواند با بررسی پسورد، اجازه ورود دهد. از طرفی در پروتکل HTTP هیچ‌گونه رمزگاری‌ای وجود ندارد و کل داده

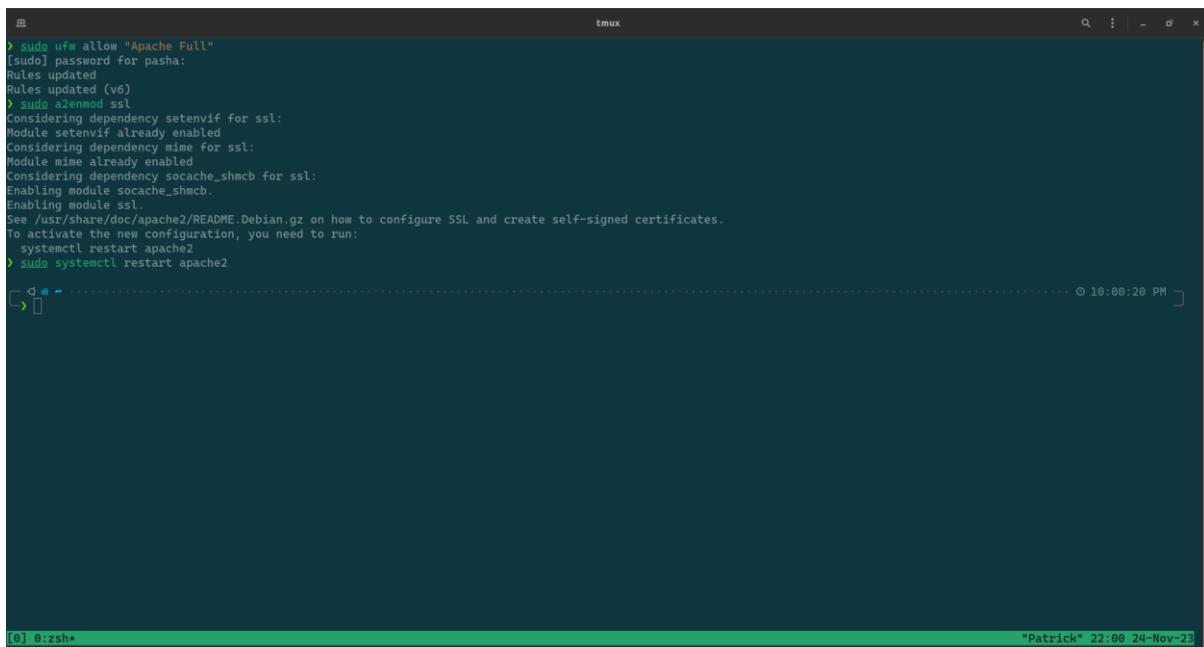
به صورت plain text برای سرور ارسال می‌شود. به همین دلیل، اگر کسی در میانه راه بتواند بسته را شنود کند، بدون نیاز به انجام کاری می‌تواند کل داده رد و بدل شده را بخواند که در بین این داده‌ها، یوزرنیم و پسورد کاربر هم وجود دارد.

راهاندازی سرور HTTPS با احراز هویت کاربری

1. ایجاد گواهی SSL

ابتدا با استفاده از دستورات زیر، دسترسی apache به پورت 443 را آزاد کرده، مازول ssl را فعال کرده، و سرویس apache را ریاستارت می‌کنیم:

```
sudo ufw allow 'Apache Full'  
sudo a2enmod ssl  
sudo systemctl restart apache2
```



```
sudo ufw allow "Apache Full"  
[sudo] password for pasha:  
Rules updated  
Rules updated (v6)  
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  
sudo systemctl restart apache2  
[0] 0:zsh* 22:00 24-Nov-23
```

حال با استفاده از دستور زیر، یک گواهی SSL به صورت Self-Signed می‌سازیم:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout  
/etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-  
selfsigned.crt
```

این دستور یک گواهی SSL به همراه کلیدش در آدرس‌های ذکر شده تولید می‌کند. مقدار common name به همراه کلیدش در آدرس‌های ذکر شده تولید می‌کند. مقدار localhost در ادامه این دستور، برابر با قرار داده شده است.

مبانی امنیت شبکه‌های کامپیوتری تمرین کامپیوتری اول

```

tmux
* sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
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]:IR
State or Province Name (Full name) [Some-State]:Tehran
Locality Name (eg, city) []:Tehran
Organization Name (eg, company) [Internet Widgits Pty Ltd]:University of Tehran
Organizational Unit Name (eg, section) []:CE
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:webmaster@example.com
[0] 0:sudo*

```

این گواهی در تصویر زیر نمایش داده شده است:

```

tmux
* Press ? for help
.. (up a dir)
/etc/apache2/sites-available/
* 000-default.conf
* default-ssl.conf
* patrick.conf
1 -----BEGIN CERTIFICATE-----
2 MIIETCDAwBgAwIBAqUWcmVxxdBy4OGdca5EL05i5iS4wDQYJkoZIhvcNAQEL
3 B0AwgZUxCzAjBgNBAYTAkLSMQ8wDQYDVQoIDAZUZhnyYw4xDzANBgNVBAcMBRl
4 aHJhbEdMbsGA1UECgwUVv5pdmiVc210eSBvZiBUZhlyYw4xczAjBgNVBAsMAkNF
5 MRTwEAYDVQoDDA1sb2NhbGhv3QxjDA1BgkqhkiG9w0BCQEWfXdlYm1hc3RlckB1
6 eGftcGxLmVbTAefw0yhZEYXjoxD0wMjRaPiw0yNDE.XHJMxoD0wMjRaMiTGjWQs
7 CQDVQGEW3JUJiEPmA0GA1UECAwGVVocmFu0jQ8iDQYDVQoHDIAZUZhlyYw4xhTAB
8 BgIVBAoMFVuaX1cnnpdHgb2ygvGVocmFu0jQ8iDQYDVQoLDwJDRTE5MBAGA1UE
9 AwJbG9jYXob3N0MjQwIjgJKoZIhvcNAkBFhv3Zj0jYXN0ZjXAZXhbXbzSSj
10 b2wpgE1MA0GCsQGS1h3DQEBAQUAA1TBdwAwrgeKA0tBAQDABp0aDznGp1XXcC
11 Ad9kIKaGTajimlDhek1Cmn9tzjwQ24tze2h1.25byNRwqHSe5sNhmMkoTATgjII
12 Yb5G2j4VnvaZISXvcnP485.6FvVmeZT5isvJaa0TX2LcgsWmBaUhKh/pexYzZ
13 JA0REMS9ojw47L0sNU9bn392KezoURX188zZ0k59iYMsK0MzV2GaeVP93aUcn
14 93fKEtbox1yg0gFWYEaqqaV/CTx01xqHICU+1M2UYBRi/yW1X067HkP9jZ6wIQj
15 fu/MkgfKE1Ad12BYiFFhE0Ynh208m4.iH+HQm/wKa7jw77kDE8A91HEQuIgeK8+
16 X1HZaghBAAGjUzBRB0GA1UDgQWBBS<3h5zT3j_lpmLr/ykPb6G/VnraZAfBgNV
17 HSfEG0dNgBS<3h5zT3j_lpmLr/ykPb6G/vn+ZaPBgnVHRMBAf8EBTADAQjW/H0G
18 CSqGSD1D3QEBcWUA41BAQAcaVS+1Pyj2yld5mZUKWZQlWInlu2gZ02evedu1Noq
19 b5xFHwPBj457PxBanw7cNHubM6NpVjFMlad8RzpeJNQuoBP36eGd16V3YQh
20 7F3ev+Rr+uqXYJCJmOEViC7DyOVL6p1+HNSA7edSF-Hp-bw9LzDnAzLVRF-g8Lzb
21 D1n5bflobiy9LE21ka1MnPmkmj1r60arlxREByrkl/RtHPzh3+60nhK+nT/8
22 6zLcfPneInaDktsN054dghykj2ueCWPdSyh1tm7Nl3Ygjh3z0614LB0uPK51zY
23 LQuUvT/cpvL6Pipv83pk/W0hPghTSqM6CL1ZMvvsun
24 -----END CERTIFICATE-----

```

حال باید این گواهی را به کانفیگ apache اضافه کنیم. برای این کار از دستور زیر استفاده کرده و فایل کانفیگ را ادیت می‌کنیم:

`sudo nvim /etc/apache2/sites-available/patrick.conf`

و سپس فایل را طوری تغییر داده که مقادیر زیر را داشته باشد:

```
<VirtualHost *:443>
    ServerName patrick
    DocumentRoot /var/www/patrick

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>
```

و با استفاده از دستورات زیر، کانفیگ را چک کرده و سرویس را ریلود می‌کنیم:

```
sudo apache2ctl configtest  
sudo systemctl reload apache2
```

```
tmux
> ls
000-default.conf default-ssl.conf patrick.conf
> sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
> sudo systemctl reload apache2
-> cd /etc/apache2/sites-available
-> vim patrick.conf

  * Press ? for help
  .. (up a dir)
/etc/apache2/sites-available/
  • 000-default.conf
  • default-ssl.conf
  • patrick.conf

  1 <VirtualHost *:443>
  2   ServerAdmin webmaster@localhost
  3   ServerName patrick
  4   ServerAlias www.patrick
  5   DocumentRoot /var/www/patrick
  6   ErrorLog ${APACHE_LOG_DIR}/error.log
  7   CustomLog ${APACHE_LOG_DIR}/access.log combined
  8
  9   SSLEngine on
 10  SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
 11  SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
 12
 13  <Directory "/var/www/patrick">
 14    AuthType Basic
 15    AuthName "Restricted Content"
 16    AuthUserFile /etc/apache2/.htpasswd
 17    Require valid-user
 18  </Directory>
 19 </VirtualHost>

patrick.conf
patrick.conf" 20L, 578C written
[0] 0:zsh
  19,14          Top
  "Patrick" 22:14 24-Nov-23
```

حال اگر سایت را با HTTP بررسی کنیم، میبینیم که صفحه اولیه apache لود شده و صفحه ما لود نمیشود. این به این دلیل است که سایت جدید فقط بر روی HTTPS است و برای HTTP تنظیم نشده است. به همین دلیل، مجددا کانفیگ را تغییر داده و HTTP را به HTTPS ریدایرکت میکنیم. برای این کار، مقدار زیر را به فایل کانفیگ اضافه میکنیم:

```
<VirtualHost *:80>
    ServerName patrick
    Redirect / https://localhost/
</VirtualHost>
```

سیس مجددا کانفیگ را ریپلود می‌کنیم:

The screenshot shows a tmux session with two panes. The top pane displays a terminal session with the following commands and output:

```
> ls
000-default.conf default-ssl.conf patrick.conf
> sudo apachectl configtest
[sudo] password for pasha:
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
syntax OK
> sudo systemctl reload apache2
[6] 0:tmux
```

The bottom pane shows the Apache configuration file (`patrick.conf`) with the following content:

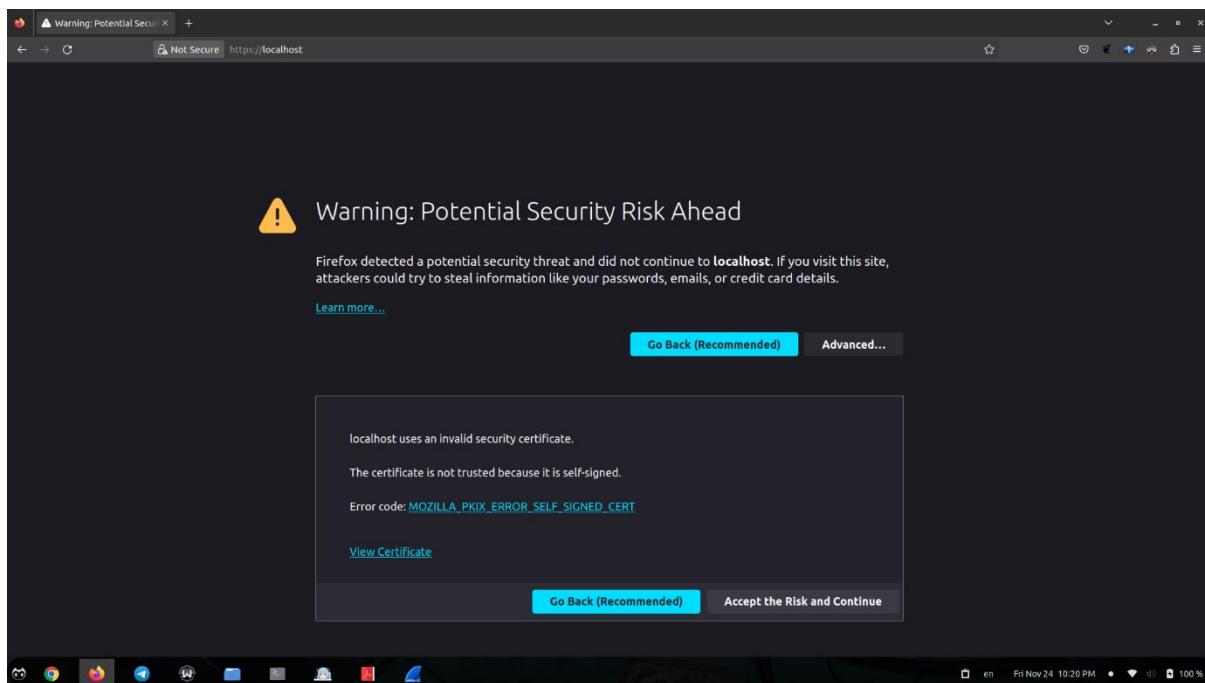
```
Press ? for help
...
SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

<Directory "/var/www/patrick">
    AuthType Basic
    AuthName "Restricted Content"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
</Directory>
</VirtualHost>
<VirtualHost *:80>
    ServerName patrick
    Redirect / https://localhost/
</VirtualHost>
```

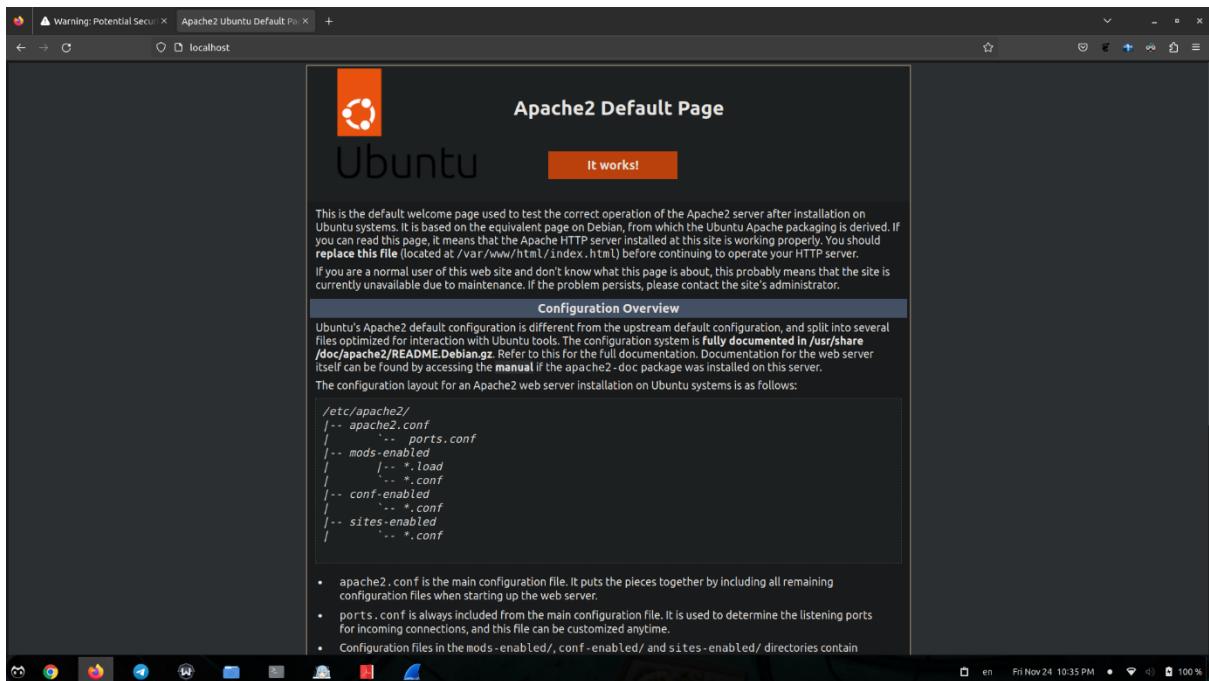
Terminal command: `"patrick.conf" 25L, 664C written`

Bottom status bar: "Patrick" 22:38 24-Nov-23

2. صفحه سایت در حالت HTTPS

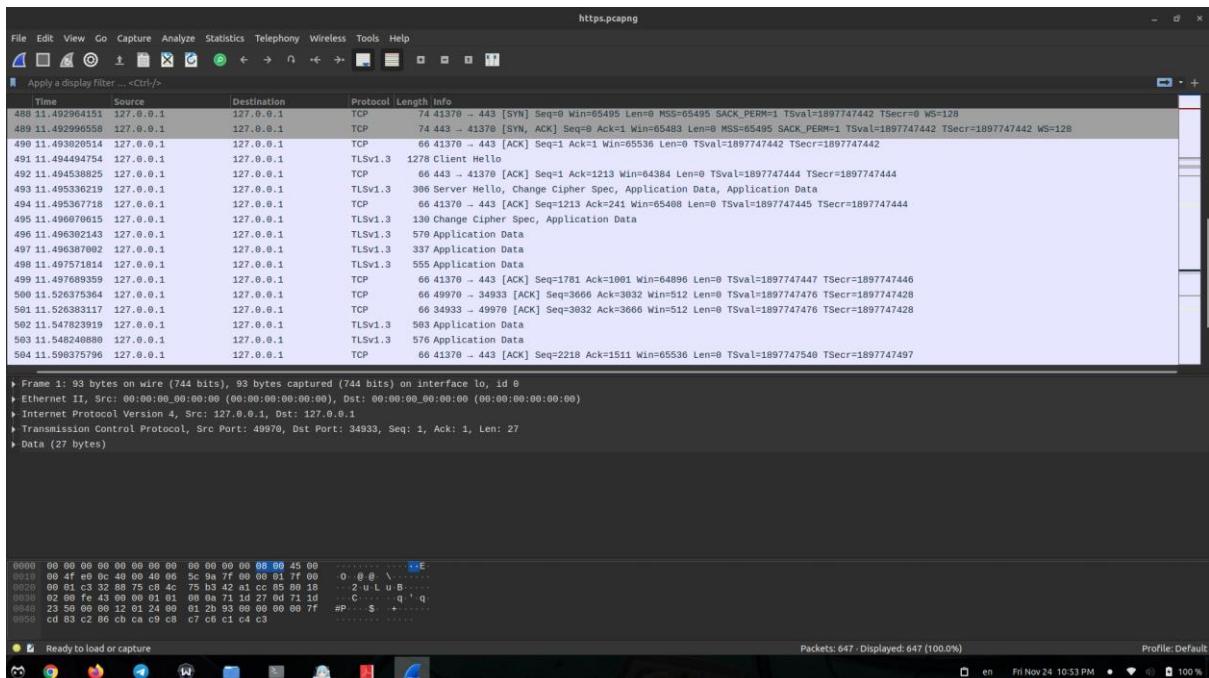


همچنین پیش از تنظیم HTTP، در حالت Redirection به صورت زیر باز می‌شد:



3. ضبط پسته‌های HTTPS توسط wireshark

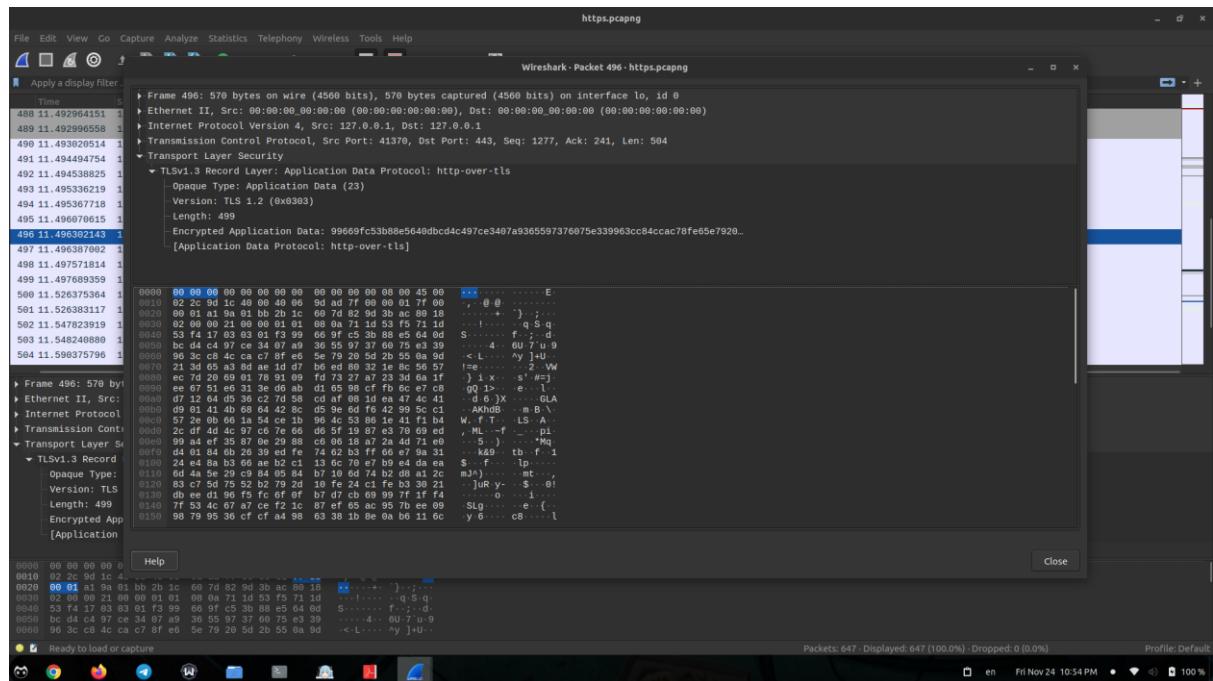
پس از شروع ضبط wireshark و وارد کردن یوزرنیم و پسورد، صفحه wireshark به صورت زیر است:



مشاهده می‌کنیم که دیگر پکت‌های HTTP وجود ندارند و تنها پکت‌های TCP و TLS را داریم.
حال یکی از این بسته‌ها را مشاهده می‌کنیم:

مبانی امنیت شبکه‌های کامپیوتری

تمرین کامپیوتری اول



طبق تصویر، می‌بینیم که هیچ اطلاعات **Authorization**-ای وجود ندارد و تنها یک فیلد **Application Data** داریم و اطلاعات به صورت رمزگاری شده ارسال می‌شوند و کسی نمی‌تواند یوزرنیم و پسورد را مشاهده کند.

4. علت عدم امکان شنود اطلاعات احراز هویت کاربری

زمانی که از HTTPS استفاده می‌کنیم، ابتدای اتصال به کمک یک الگوریتم نامتقارن، کلاینت و سرور یک کلید رمزگاری متقارن را با همدیگر تبادل می‌کنند. از طرفی سرور خود را برای کلاینت ارسال کرده و کلاینت با بررسی صحت آن، از اینکه فرد دیگری خود را به جای سرور جا نزده مطمئن می‌شود. مراحل کامل انجام این کار در بخش بعدی توضیح داده شده است.

از این پس، تمام اطلاعاتی که بین سرور و کلاینت رد و بدل شده به صورت رمز شده (توسط کلید متقارن انتخاب شده) ارسال می‌شوند و فردی نمی‌تواند با خواندن بسته، اطلاعات آن را بدست آورد زیرا رمزگشایی آن نیازمند دانستن کلید رمزگاری متقارن است که چون این کلید به صورت plain text منتقل نشده و توسط یک الگوریتم نامتقارن رد و بدل شده است، این امکان برای آن فرد وجود نداشته و حمله MITM خنثی می‌شود.

5. مراحل **handshake** و بسته‌های رد و بدل شده

این مراحل به صورت زیر هستند:

Client Hello

کلاینت این بسته را برای سرور ارسال کرده که حاوی اطلاعات زیر است:

- ورژن‌های TLS که ساپورت می‌کند
- لیست cipher suite-هایی که ساپورت می‌شوند
- یک مقدار به نام

Server Hello

سرور پس از دریافت بسته Client Hello این بسته با محتویات زیر را ارسال می‌کند:

- ورژن انتخاب شده TLS
- Cipher suite انتخاب شده
- یک مقدار رندوم به نام Server Random

Change Cipher Spec

این پکت به این معنی است که از سرور از کلاینت می‌خواهد ارتباط را به حالت رمزگاری شده تغییر دهد.

Multiple Application Datas

این پکت‌ها شامل Certificate Server و Server Finished هستند که به صورت رمزگاری شده ارسال می‌شوند.

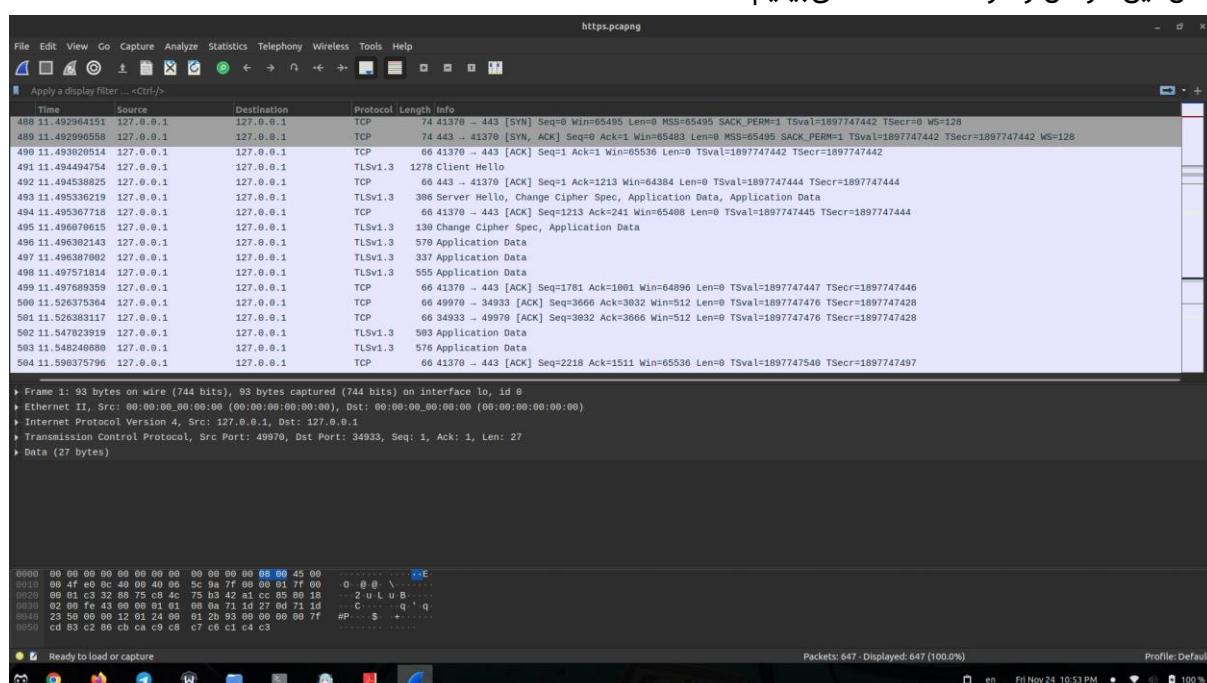
Change Cipher Spec

این پکت از طرف کلاینت به سرور ارسال می‌شود و از او می‌خواهد که ارتباط رمزگاری شود.

Application Data

این پکت مجدداً شامل Client Finished است که به صورت رمزگاری شده ارسال می‌شود.

حال این مراحل را در wireshark می‌بینیم:

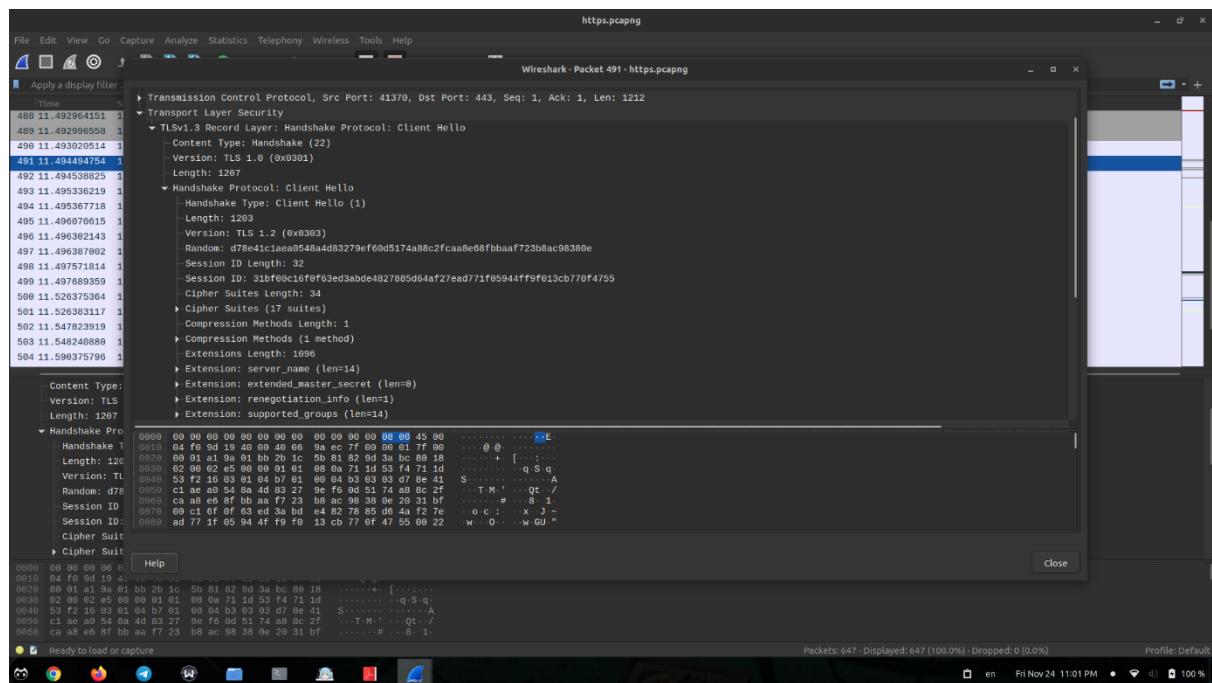


می‌بینیم که ابتدا پکت‌های Syn-Ack و Ack را برای برقراری ارتباط TCP داریم.

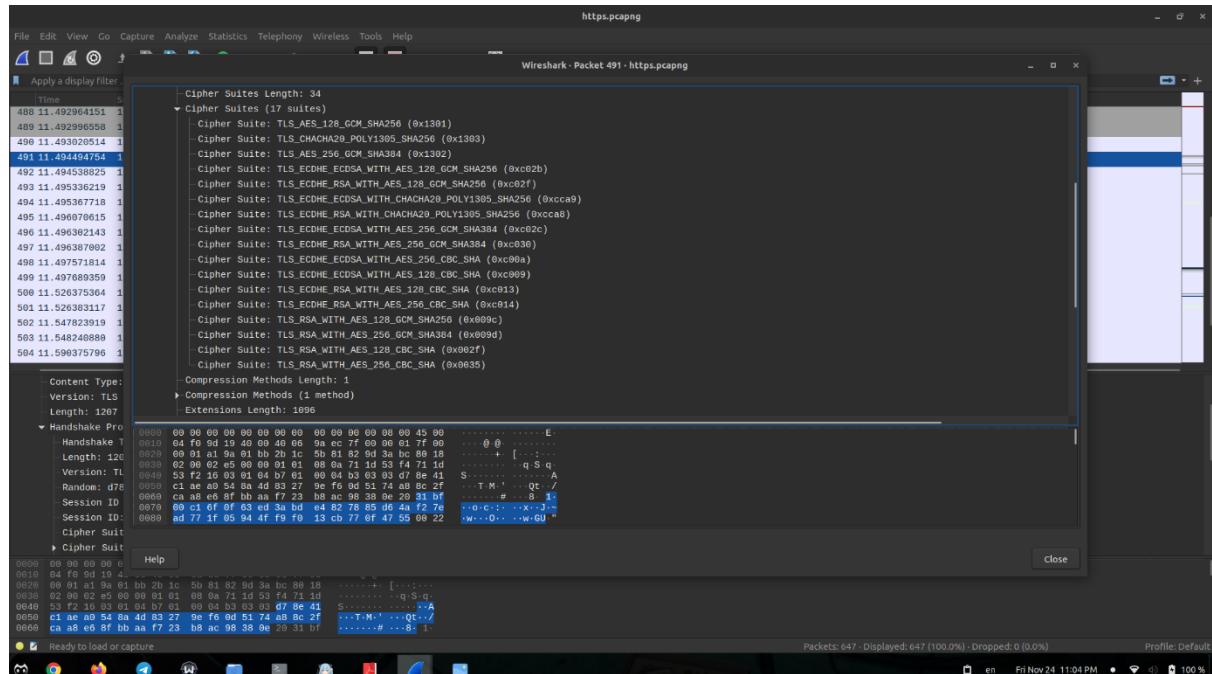
پس از آن، به پکت Client Hello می‌رسیم:

مبانی امنیت شبکه‌های کامپیوتری

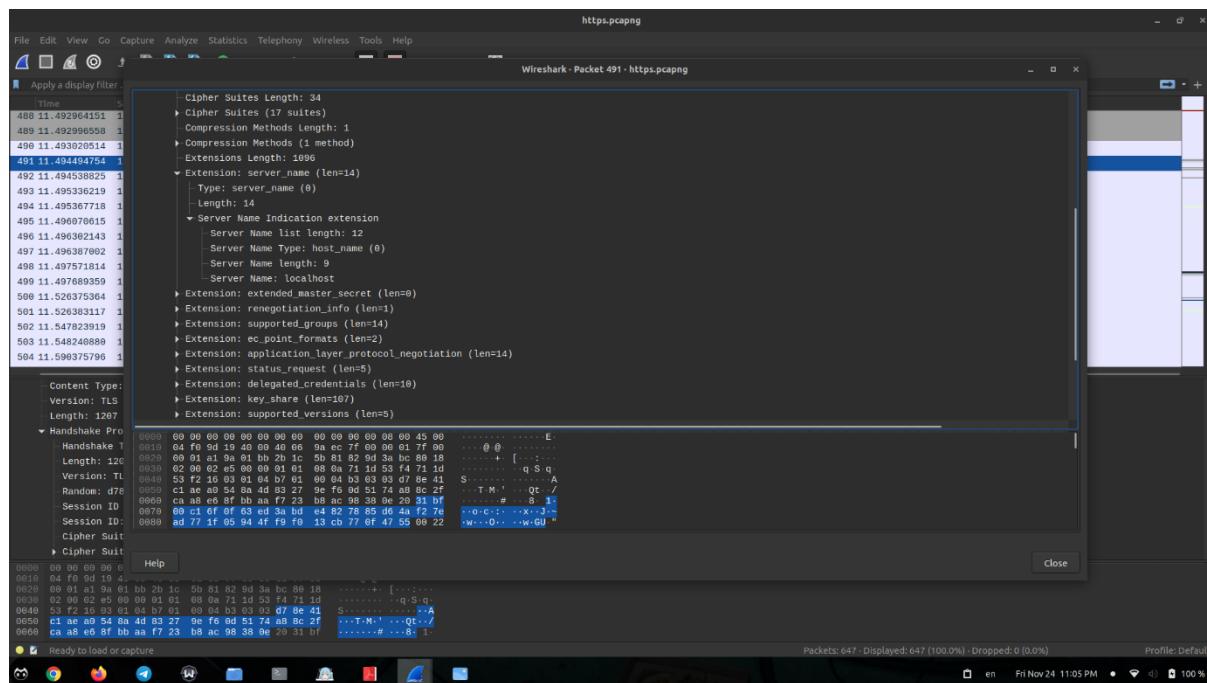
تمرین کامپیوتری اول



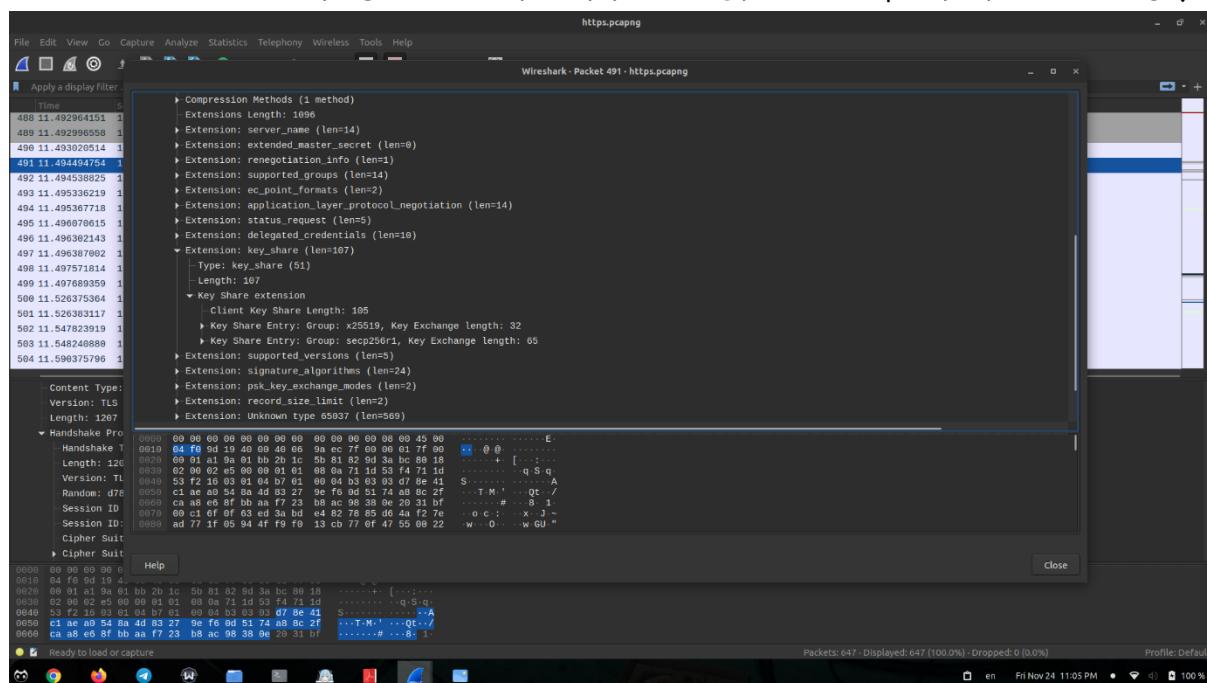
در این بخش می‌بینیم که ورژن TLS برابر با 1.2 انتخاب شده که صرفا برای Backward Compatibility است. پس از آن یک مقدار Random داریم که با عنوان Client Random می‌شناسیم. سپس تعدادی مورد پذیرش داریم که در ادامه نشان داده شده‌اند:



پس از آن، server_name را خواهیم داشت که در این بخش، localhost است.

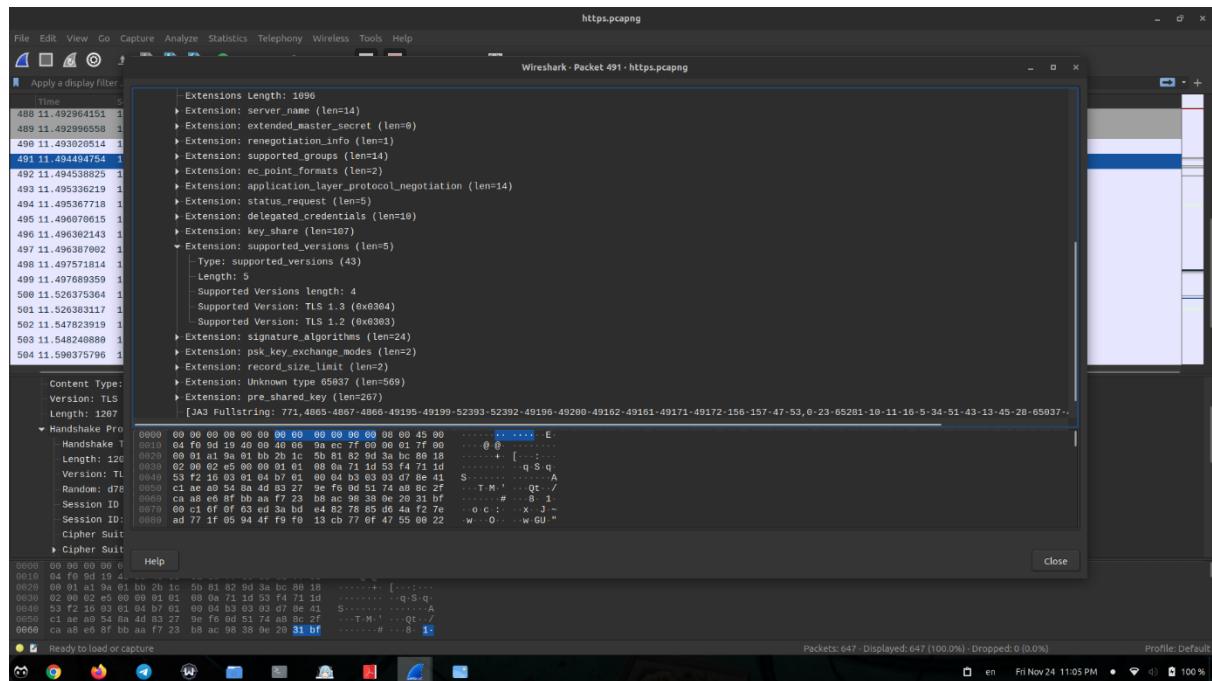


سپس key_share را خواهیم داشت که برای ساخت رمز متقاضون استفاده می‌شود.

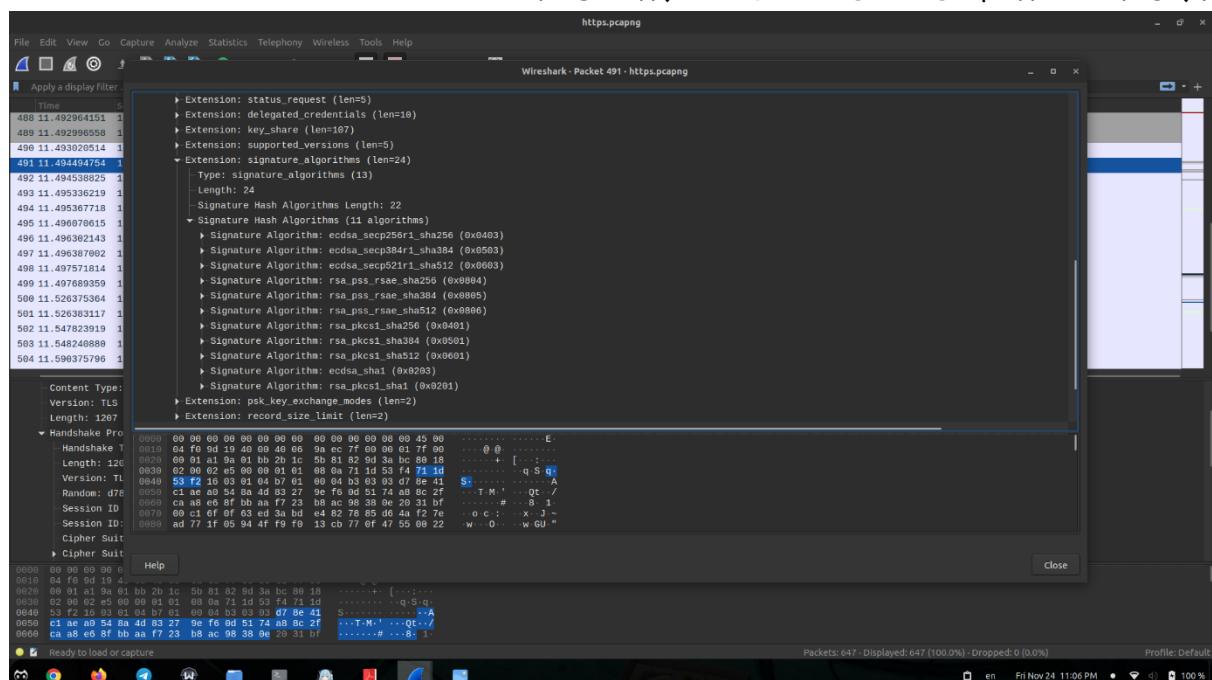


سپس ورژن‌های TLS که ساپورت می‌شوند:

مبانی امنیت شبکه‌های کامپیوتری تمرین کامپیوتری اول

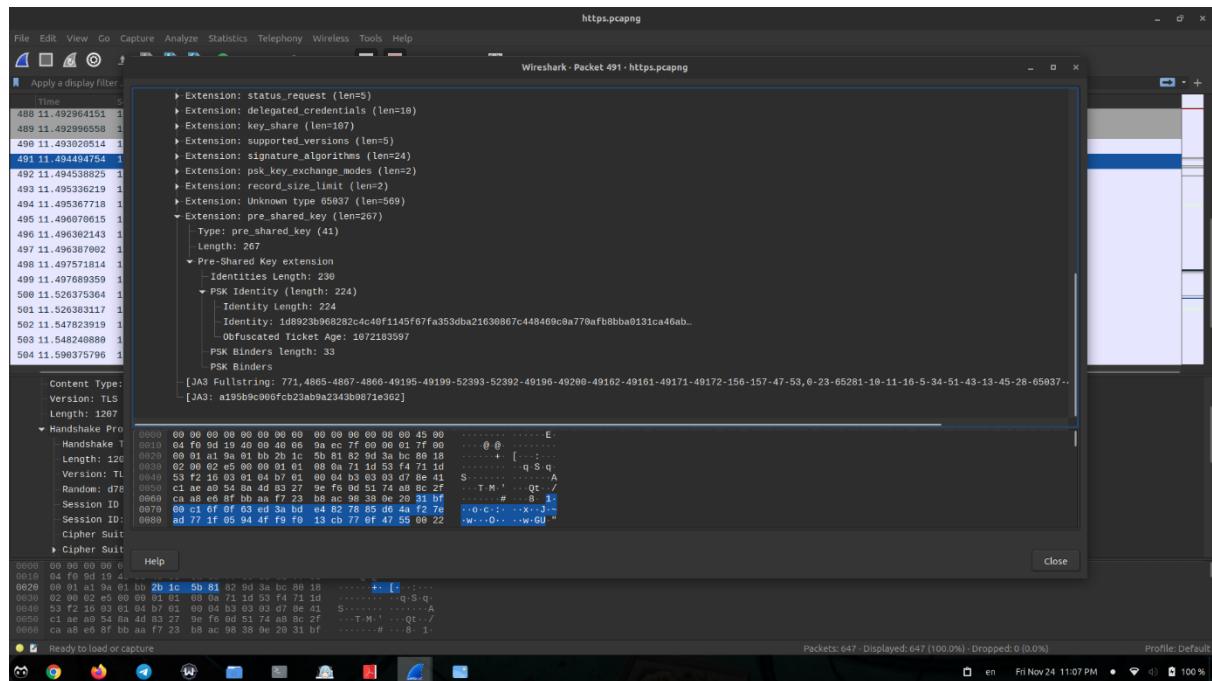


و پس از آن، الگوریتم‌های امضای دیجیتال که ساپورت می‌شوند:

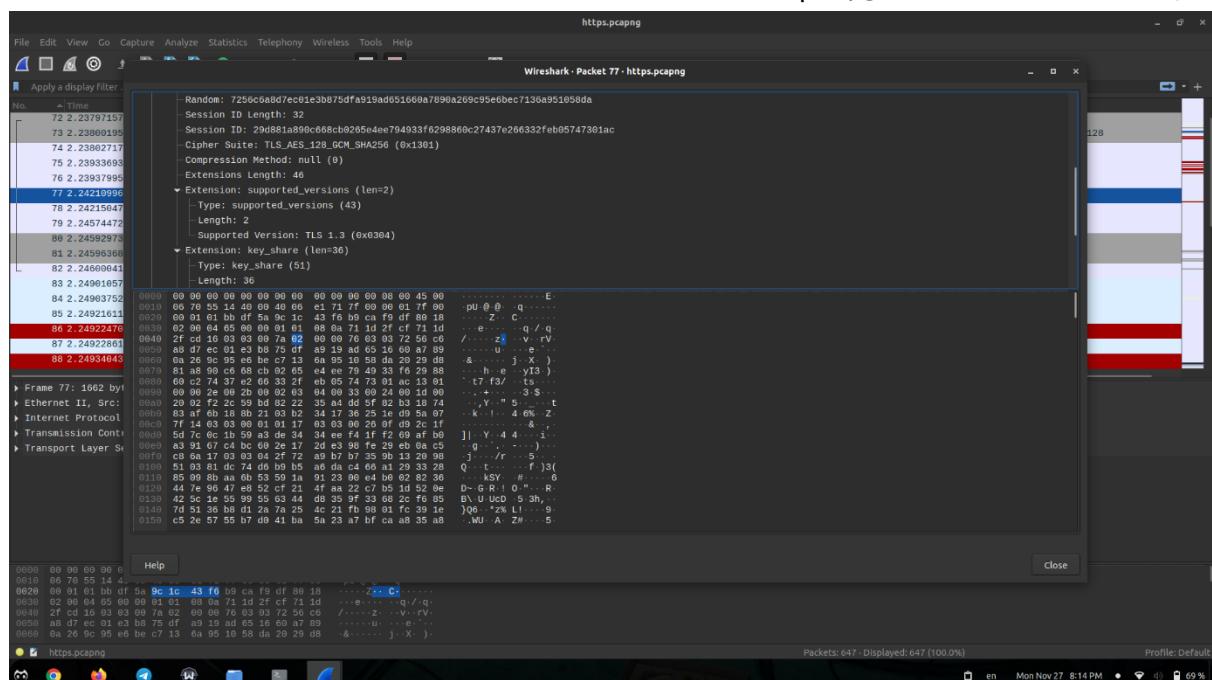


در نهایت Key Exchange را خواهیم داشت که بخشی از الگوریتم PreSharedKey است.

مبانی امنیت شبکه‌های کامپیوتری تمرین کامپیوتری اول



حال به بسته Server Hello می‌رسیم:



می‌بینیم که مقادیر Random و Cipher Suite انتخاب شده و ساپورت شده (1.3) و (1.3) را داریم.

پس از آن، پکت‌های Finished و Change Cipher Spec را از هر دو طرف می‌بینیم. همانطور که مشاهده کردیم، تمام بسته‌های لازم ارسال شده و در Wireshark ضبط شده‌اند. در واقع سرور و کلاینت با مقادیری که در بسته‌های hello دریافت کرده‌اند و key-private key-های خودشان، می‌توانند به یک کلید متقاضی یکسان برسند و پیام‌های خود را رمزگاری کنند.

در بخش Application Data تعداد چهار ChangeCipherText انتقال یافته که دو مورد از آن‌ها ذکر شده و از بین بقیه، می‌تواند شامل Certificate Request (به صورت اختیاری) باشد.