



***East West University***

**Mini Project-1 (Cybersecurity)**

**Course Title:** Cyber Security, Law and Ethics

**Course Code:** CSE487

**Section:** 01

**Semester:** Summer 2022

**Submitted To**

**Rashedul Amin Tuhin**

Senior Lecturer

Department of Computer Science and Engineering

**Submitted By**

**Group no.:** 01

**Group members:**

Rafiur Rahman Rafit

2018-3-60-111

Jaser Maharus

2018-3-60-070

**Submission Date**

August 25,2022

**Title:** Securing a Network System with Public Key Infrastructure (Implementing Transport Layer Security on HTTP for <https://connection>)

## For Linux:

Here we are using kali Linux as an operating system

Firstly, create a localhost in Linux and configure the web server with Apache2 on that Linux Host. For this the instructions are:

1. Install Apache2 server (sudo apt install apache2)

```
(hm@hmwd)-[~]
$ sudo apt install apache2
[sudo] password for hm:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.54-2).
apache2 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

2. Start Apache2 server (sudo service apache2 start)

```
(hm@hmwd)-[~]
$ sudo service apache2 start

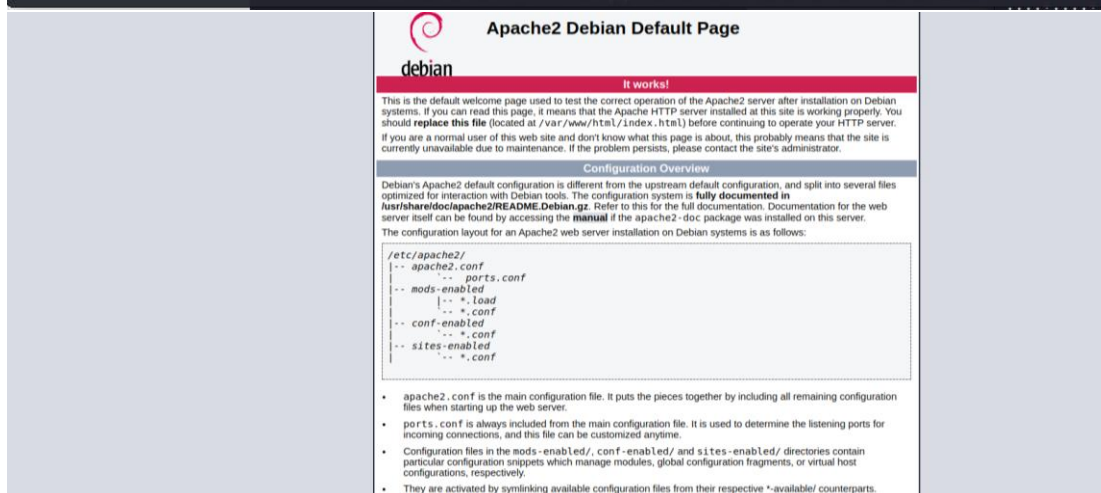
(hm@hmwd)-[~]
$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2022-07-22 11:42:41 +06; 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2868 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 2885 (apache2)
    Tasks: 6 (limit: 9178)
   Memory: 19.2M
      CPU: 52ms
   CGroup: /system.slice/apache2.service
           └─2885 /usr/sbin/apache2 -k start
           └─2887 /usr/sbin/apache2 -k start
           └─2888 /usr/sbin/apache2 -k start
```

3. Check IP or type local host in browser by following these steps (here IP Change due to Network Connectivity):

```
File Actions Edit View Help
(hm@hmwd)-[~]
$ sudo ifconfig
[sudo] password for hm:
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 30:d0:42:00:65:6e txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1627 bytes 190874 (186.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1627 bytes 190874 (186.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.248.61 netmask 255.255.255.0 broadcast 192.168.248.255
    inet6 fe80::fc17:57bb:b060:ef1b prefixlen 64 scopeid 0<link>
    ether 5c:ba:ef:20:b9:5f txqueuelen 1000 (Ethernet)
    RX packets 40093 bytes 47661566 (45.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22251 bytes 3198398 (3.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



Our server is running but it is not secure, so we must use SSL Certificate and make browser trust that our certificate is real. For doing this the instructions are:

1. Install open SSL in kali Linux (sudo apt-get install openssl)

```
(hm@hmwd)-[~]
$ sudo apt-get install openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl is already the newest version (3.0.3-8).
openssl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.

(hm@hmwd)-[~]
$
```

Create SSL certificate ("s sudo openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -nodes \ -keyout /etc/ssl/private/server.key -out /etc/ssl/certs/server.crt -subj "/CN=www.acmesecureserver.com" \ -addext "subjectAltName=DNS:www.acmesecureserver.com,DNS:\*.webview.acmesecureserver.com,IP:192.168.60.61")

```
(hm@hmd)~$ sudo openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -nodes \
-keyout /etc/ssl/private/server.key -out /etc/ssl/certs/server.crt -subj "/CN=www.acmesecureserver.com" \
-addext "subjectAltName=DNS:www.acmesecureserver.com,DNS:*.webview.acmesecureserver.com,IP:192.168.60.61"
```

2.

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:nakuna matata
Organizational Unit Name (eg, section) []:hm
Common Name (e.g. server FQDN or YOUR name) []:rafit
Email Address []:rafiurrahmanrafit
```

3. sudo a2enmod ssl
4. restart server(systemctl restart apache2)
5. sudo ln -s /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/000-default-ssl.conf
6. edit file (/etc/apache2/sites-enabled/000-default-ssl.conf)

```
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

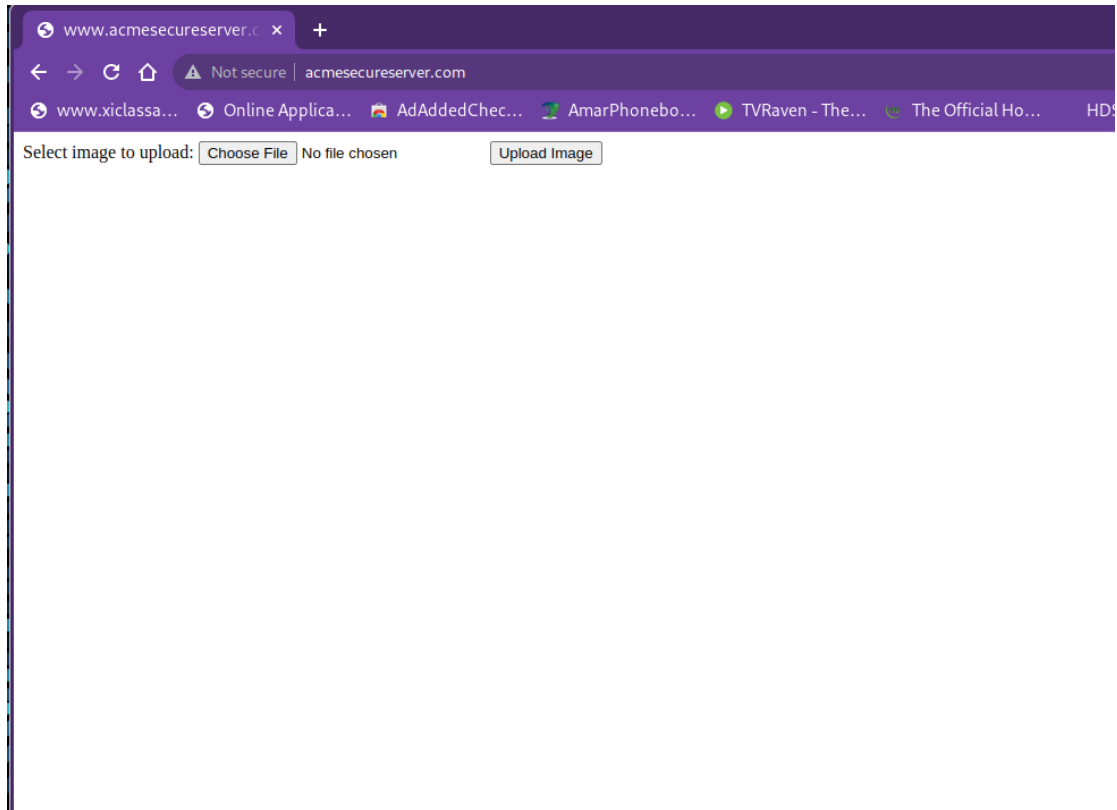
#
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

#
# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key

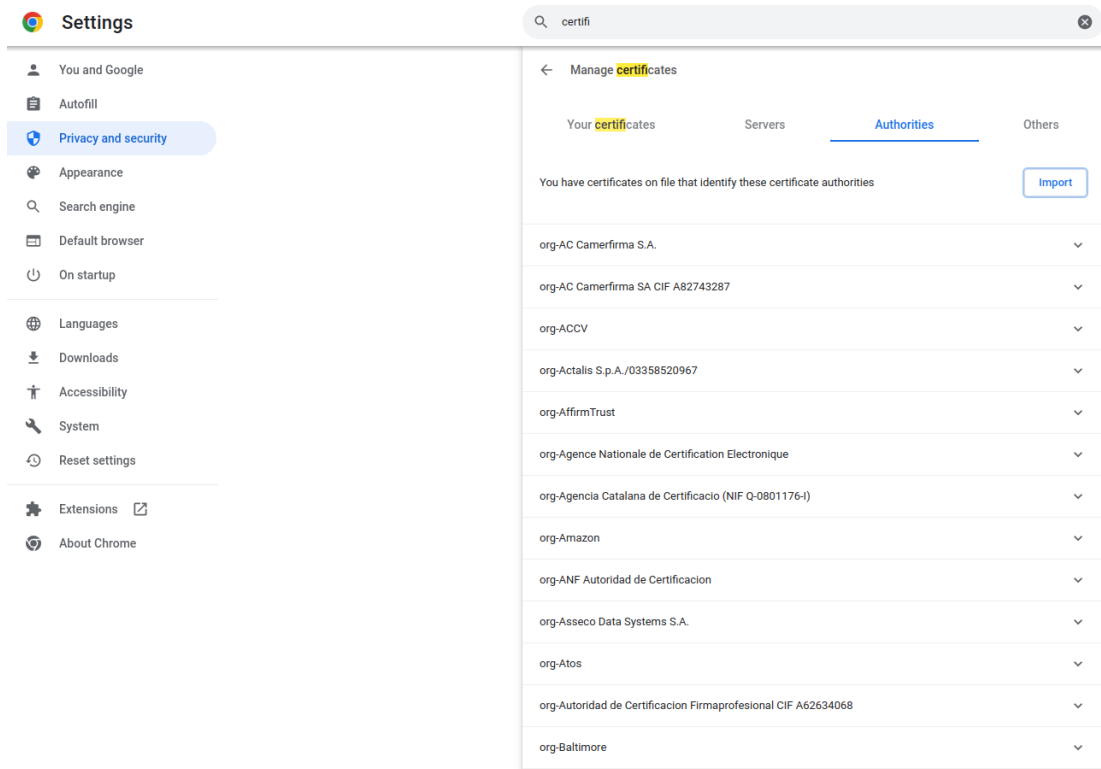
#
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

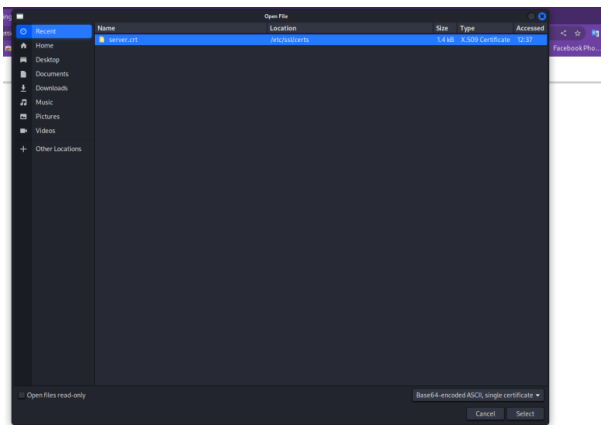
#
# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
```

## 7. reboot server



## 8. Now in chrome we must add certificate. For doing this the instructions are:





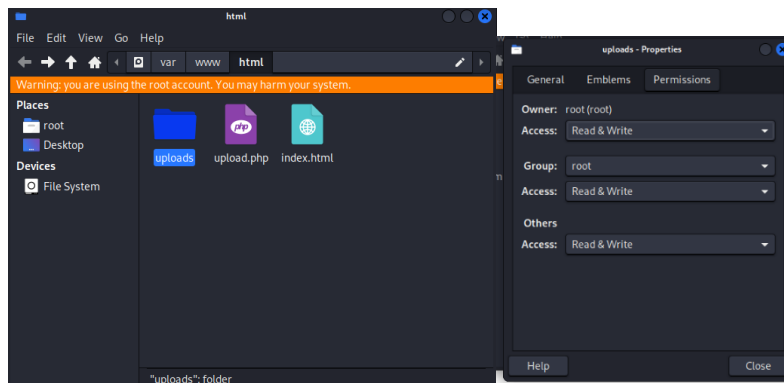
org-VeriSign, Inc.

org-WiSeKey

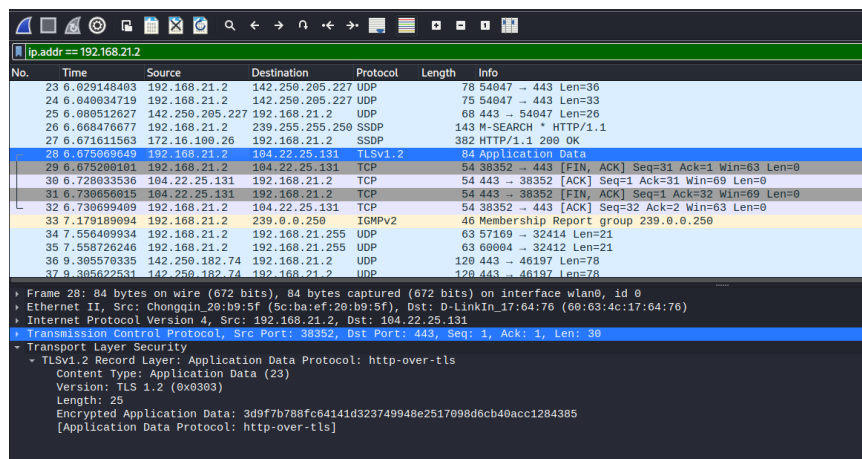
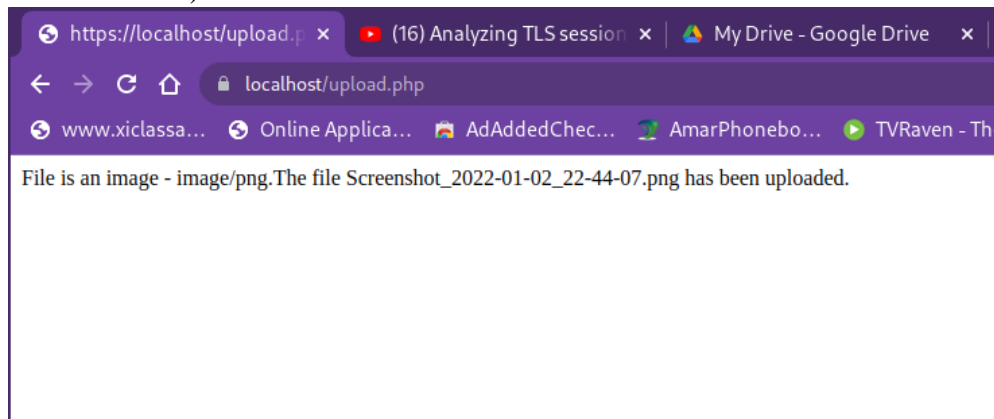
org-www.acmesecureserver.com

org-XRamp Security Services Inc

9. Now Create simple upload page, simply create an upload html page with PHP language for uploading a file. and give read and write permission to upload folders also. The instructions for doing this are:



10. Test security in Wireshark (Open wire Wireshark app, filter it by giving the IP address of the web server and start Wireshark)

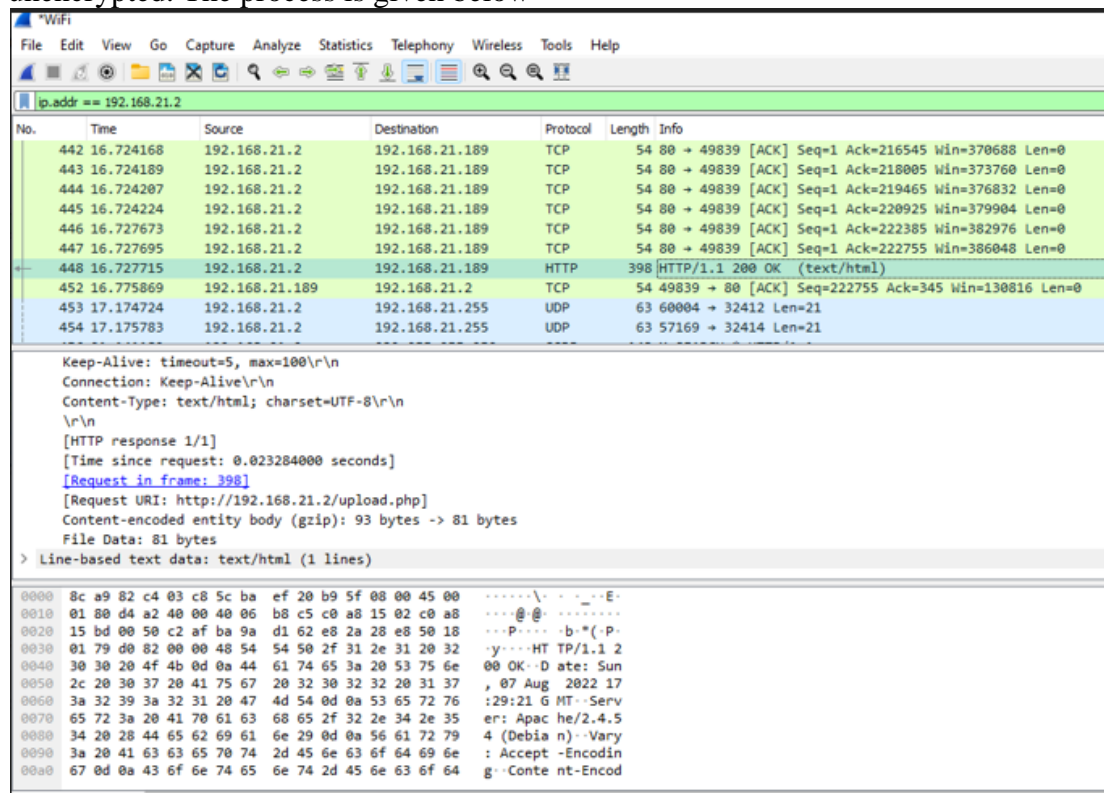


TLS 1.3/1.2 is the latest version of the internet's most deployed security protocol, which encrypts data to provide a secure communication channel between two endpoints.

Here wire shark file link has been given

[https://drive.google.com/file/d/1p2smKi6Q\\_ISCHFRFV2k-KA4CWSHN0mXm/view?usp=sharing](https://drive.google.com/file/d/1p2smKi6Q_ISCHFRFV2k-KA4CWSHN0mXm/view?usp=sharing)

Now from client pc where certificate is not installed in the browser, when we run Wireshark on that we see our data is unencrypted. The process is given below-



<https://drive.google.com/file/d/1vOPDZMaIhRj8hH8QNZ999k0Ioe9E7f3/view?usp=sharing>

Now to remove Certificate we need to type command in Linux. The instructions are:

- a2dissite default-ssl.conf
- a2enmod ssl

**Now For IDS System, we install SNORT, it is supported for Ubuntu system. To install SNORT, we need to add Ubuntu Repository in Kali Linux**

```
# deb cdrom:[Ubuntu 20.04 LTS _Focal Fossa_ - Release amd64 (20200423)]/ focal main restricted
```

```
# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to  
# newer versions of the distribution.
```

```
deb http://archive.ubuntu.com/ubuntu focal main restricted  
# deb-src http://in.archive.ubuntu.com/ubuntu/ focal main restricted
```

```
deb http://archive.ubuntu.com/ubuntu focal-updates main restricted  
# deb-src http://in.archive.ubuntu.com/ubuntu/ focal-updates main restricted
```

```
deb http://archive.ubuntu.com/ubuntu focal universe  
# deb-src http://in.archive.ubuntu.com/ubuntu/ focal universe  
deb http://archive.ubuntu.com/ubuntu focal-updates universe  
# deb-src http://in.archive.ubuntu.com/ubuntu/ focal-updates universe
```

```
deb http://archive.ubuntu.com/ubuntu focal multiverse  
# deb-src http://in.archive.ubuntu.com/ubuntu/ focal multiverse  
deb http://archive.ubuntu.com/ubuntu focal-updates multiverse  
# deb-src http://in.archive.ubuntu.com/ubuntu/ focal-updates multiverse
```

```
deb http://archive.ubuntu.com/ubuntu focal-backports main restricted universe multiverse  
# deb-src http://in.archive.ubuntu.com/ubuntu/ focal-backports main restricted universe multiverse
```

```
# deb http://archive.canonical.com/ubuntu focal partner  
# deb-src http://archive.canonical.com/ubuntu focal partner
```

```
deb http://archive.ubuntu.com/ubuntu focal-security main restricted  
# deb-src http://security.ubuntu.com/ubuntu focal-security main restricted  
deb http://archive.ubuntu.com/ubuntu focal-security universe  
# deb-src http://security.ubuntu.com/ubuntu focal-security universe  
deb http://archive.ubuntu.com/ubuntu focal-security multiverse  
# deb-src http://security.ubuntu.com/ubuntu focal-security multiverse
```

**Then type these commands -**

- `sudo apt update`
- `sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 3B4FE6ACC0B21F32`
- `sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 871920D1991BC93C`
- `sudo apt-get -y install snort`



## Then start SNORT

The instruction for this is:

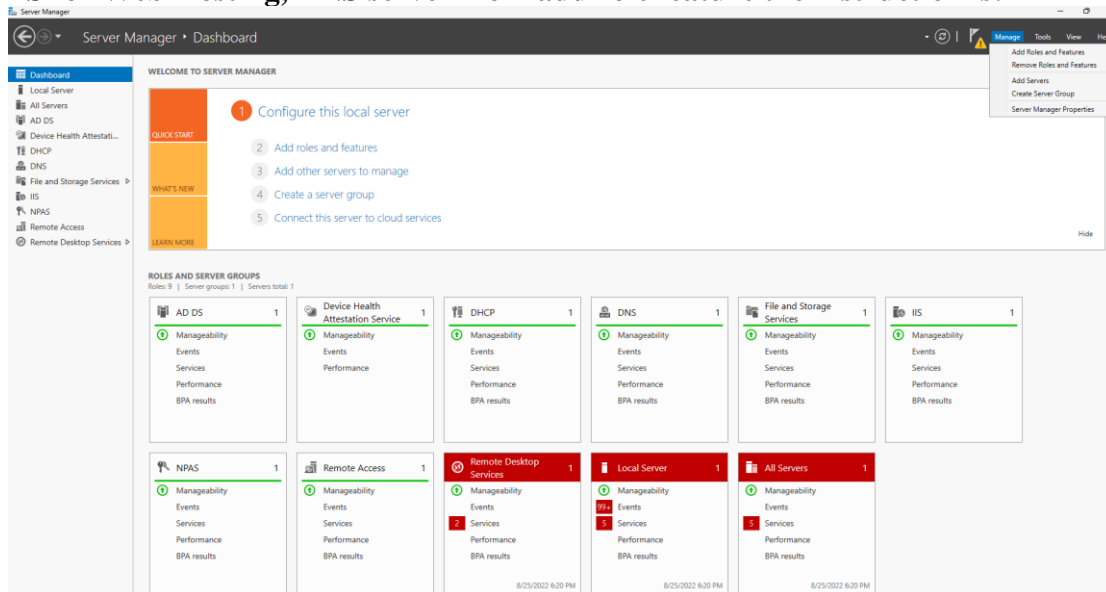
`sudo snort -vde`

```
hm@hmdw: ~  
File Actions Edit View Help  
08/25-22:08:38.716525 5C:BA:EF:20:B9:5F → 60:63:4C:17:64:76 type:0x800 len:0x5A  
192.168.21.2:56248 → 142.250.82.44:19305 UDP TTL:64 TOS:0x0 ID:30894 IpLen:20 DgmLen:76 DF  
Len: 48  
AF CD 00 06 93 9D 87 8B 19 69 13 DD 09 3F EC FC .....i...?..  
1D 0E 88 34 5D 57 7B 22 37 2A 1F D5 49 15 C0 28 ...4]W{'7*..I..(  
EF E1 F1 43 82 D3 EC B0 30 D8 3C DB 80 00 0A C7 ...C...0.<.....  
  
=====
```

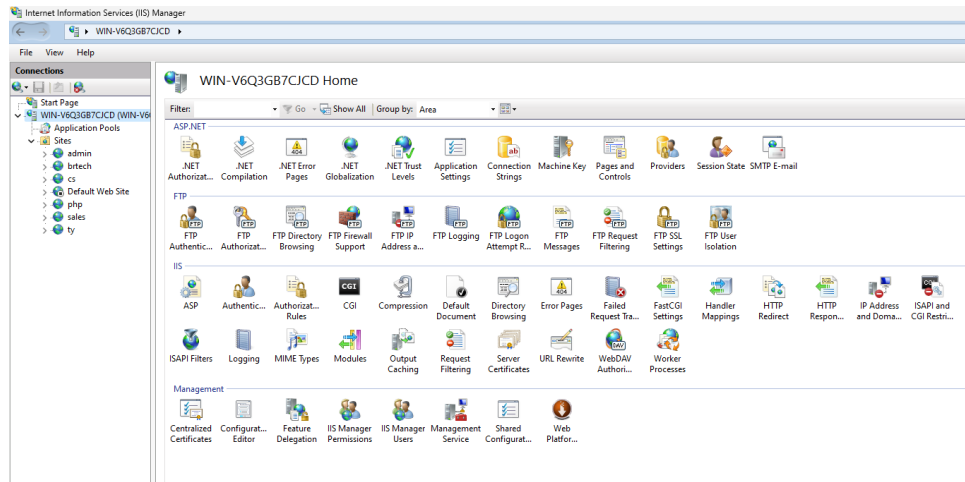
```
WARNING: No preprocessors configured for policy 0.  
08/25-22:08:38.765830 60:63:4C:17:64:76 → 5C:BA:EF:20:B9:5F type:0x800 len:0xAE  
142.250.82.44:19305 → 192.168.21.2:56248 UDP TTL:122 TOS:0x60 ID:51476 IpLen:20 DgmLen:160  
Len: 132  
81 C8 00 0C 00 00 1A 0A B3 F8 1A F5 65 C7 12 4F .....e..0  
18 6A 62 36 04 BD 05 24 32 2B 29 67 9D 9F 63 B9 .jb6...$2+)g..c.  
9E 11 87 87 1C 9B 93 AE 08 CF 76 C4 27 B5 F8 75 .....v..'..u  
8A F9 74 9E CA 95 9F 08 E1 82 90 64 4F B0 93 08 ..t.....d0...  
D5 B6 71 0E 15 F2 83 40 B5 95 B5 F7 26 4E 3C C9 ..q....@....6N<.  
1F 0C 7B AA 39 B4 A0 1C 16 05 61 26 BD B7 5E 81 ..{.9.....aδ...^.  
D2 AD 12 EE 85 64 E2 ED AA 7B 13 E3 5E 88 C5 5F .....d...{...^..  
20 6C 5A B0 D8 C8 F5 F8 16 67 84 CA EF 9D 50 B7 ..LZ.....g....P.  
80 00 01 B1 .....  
  
=====
```

**In this Project We are also making website using Windows Server 2022 and securing that site using SSL (Lets Encrypt)**

To install IIS for Web Hosting, DNS server from add role feature the instruction is:



## 1. Create a Website/Web APP in IIS



## 2. Encrypt the Web using Let's Encrypt using Certbot Acme Client



## 3. Run Certbot in CMD

```
C:\Users\Administrator>certbot
Saving debug log to C:\Certbot\log\letsencrypt.log
Certbot doesn't know how to automatically configure the web server on this system. However, it can still get a certificate for you. Please run "certbot certonly" to do so. You'll need to manually configure your web server to use the resulting certificate.

C:\Users\Administrator>
```

## 4. Create SSL Certificate by giving host name, Domain Name, Email Address. For this the instruction is:

```
C:\Users\Administrator>certbot certonly --standalone
Saving debug log to C:\Certbot\log\letsencrypt.log
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): blackrocktech.xyz
Requesting a certificate for blackrocktech.xyz
```

## 5. Allowing Particular Port in Firewall Settings and by default 80 and 443 port is opened

The screenshot displays the Windows Defender Firewall with Advanced Security console. The left pane shows the hierarchy: Windows Defender Firewall with Advanced Security > Inbound Rules. The main pane lists various inbound rules, including Core Networking, Delivery Optimization, Desktop App Web Viewer, DFS Management, DHCP Server, and BranchCache Hosted Cache Server (HTTP-In). The right pane shows the Actions for the selected rule, including New Rule, Filter by Profile, Filter by State, Filter by Group, View, Refresh, Export List, Help, Disable Rule, Copy, Delete, and Properties.

The 'BranchCache Hosted Cache Server (HTTP-In)' rule is selected, and its properties are displayed in the 'BranchCache Hosted Cache Server (HTTP-In) Properties' dialog box. The 'General' tab is active, showing the rule name, description, and action.

**BranchCache Hosted Cache Server (HTTP-In) Properties**

**General**

This is a predefined rule and some of its properties cannot be modified.

**Name:** BranchCache Hosted Cache Server (HTTP-In)

**Description:** Inbound rule for BranchCache to allow communication between a hosted cache and its clients [TCP]

☐ Enabled

**Action**

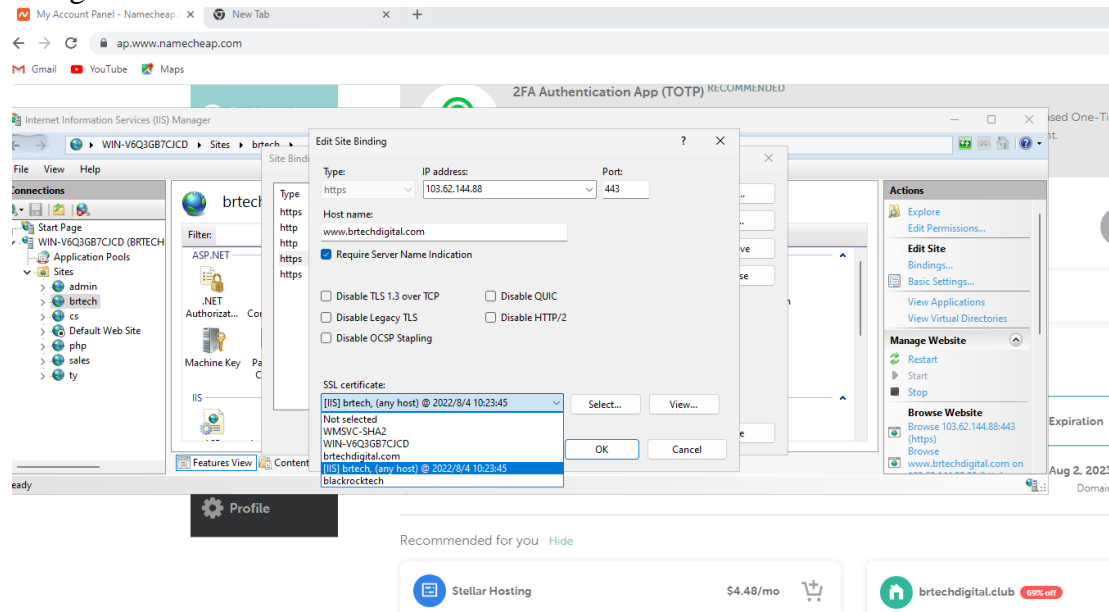
☒ Allow the connection

☐ Allow the connection if it is secure

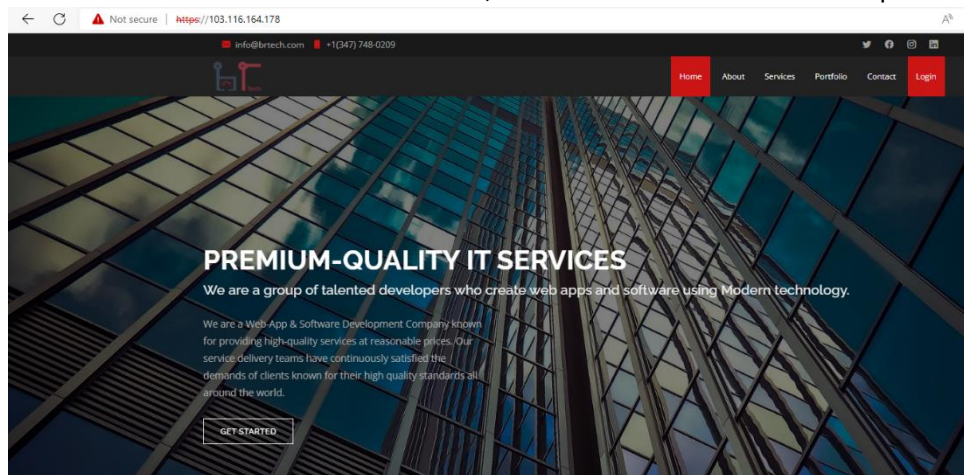
☐ Block the connection

Buttons: OK, Cancel, Apply

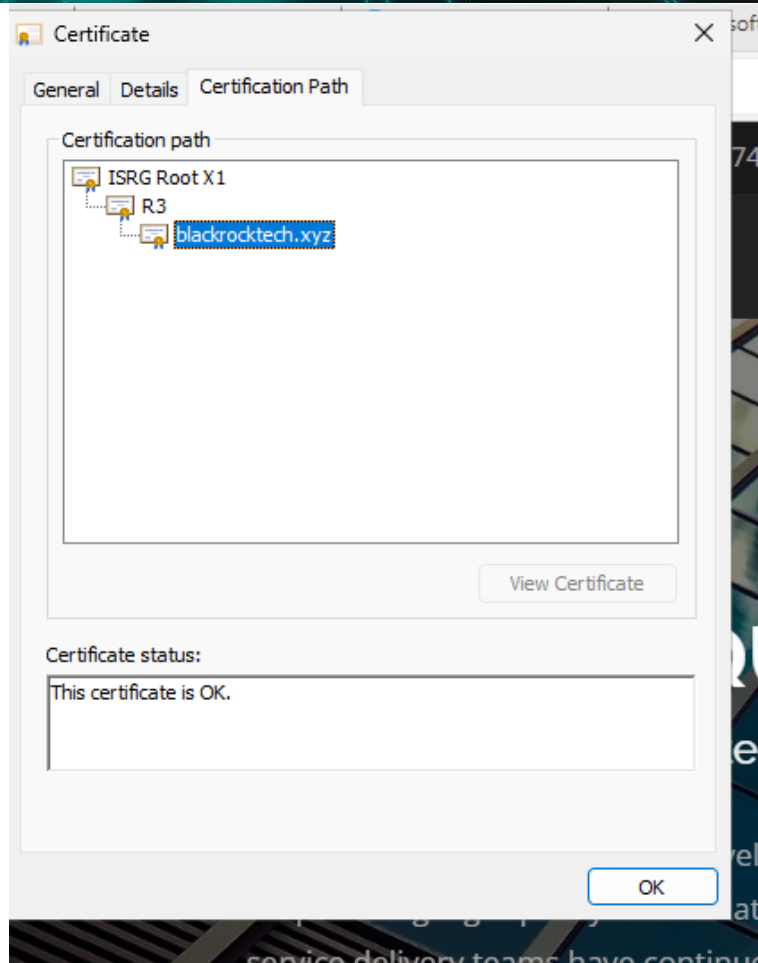
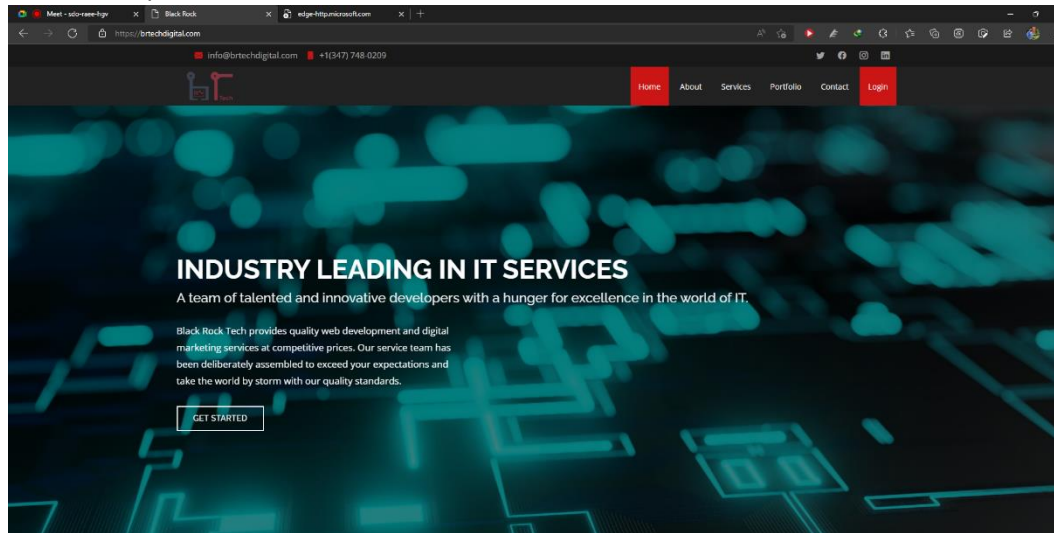
6. Declare server IP address, here we are using public IP and for domain name we are using Namecheap. Our Domain cost is 12 dollars (private-company domain). Add the SSL certificate that was generated.



7. Domain Name must be same as SSL certificate domain, or its certificate will not be accepted



## 8. Finally, our website is protected



9. Now From Any Device our device will show secure SSL certificate
10. Now we add DNS Configuration also

DNS Manager

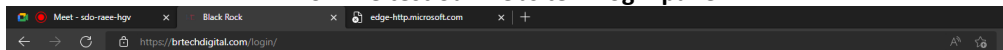
File Action View Help

DNS

- BRTECH
  - Forward Lookup Zones
    - \_msdcs.brtechedigital.com
      - brtechedigital.com
        - \_msdcs
        - \_sites
        - \_tcp
        - \_udp
        - DomainDnsZones
        - ForestDnsZones
        - (same as parent folder) Start of Authority (SOA) [261], brtech.brtechedigital.com. static
        - (same as parent folder) Name Server (NS) brtech.brtechedigital.com. static
        - (same as parent folder) Host (A) 103.62.144.88 8/24/2022 1:00:00 PM
        - (same as parent folder) Host (A) 103.116.164.178 8/24/2022 1:00:00 PM
    - Reverse Lookup Zones
      - 144.62.103.in-addr.arpa
      - 164.116.103.in-addr.arpa
    - Trust Points
    - Conditional Forwarders

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[261], brtech.brtechedigital.com.	static
(same as parent folder)	Name Server (NS)	brtech.brtechedigital.com.	static
(same as parent folder)	Host (A)	103.62.144.88	8/24/2022 1:00:00 PM
(same as parent folder)	Host (A)	103.116.164.178	8/24/2022 1:00:00 PM
(same as parent folder)	Host (A)	103.62.144.88	static
(same as parent folder)	Host (A)	103.116.164.178	static
DESKTOP-53IHCDI	Host (A)	192.168.10.189	8/24/2022 7:00:00 PM
DESKTOP-59138IG	Host (A)	192.168.12.253	8/24/2022 1:00:00 PM
DESKTOP-5H2J69Q	Host (A)	192.168.10.199	8/24/2022 6:00:00 PM
DESKTOP-72ET3NQ	Host (A)	192.168.10.105	8/24/2022 7:00:00 PM
DESKTOP-B553N8V	Host (A)	192.168.10.195	8/24/2022 6:00:00 PM
DESKTOP-CS0C3V6	Host (A)	192.168.10.3	8/24/2022 6:00:00 PM
DESKTOP-GO78RUJ	Host (A)	192.168.12.243	8/10/2022 11:00:00 AM
DESKTOP-I2DSA17	Host (A)	192.168.12.245	8/24/2022 1:00:00 PM
DESKTOP-Q9KGVTVU	Host (A)	192.168.12.244	8/10/2022 11:00:00 AM
Facebook-Team	Host (A)	192.168.10.122	8/24/2022 6:00:00 PM
whitedevil	Host (A)	192.168.0.163	8/4/2022 2:00:00 PM

Now in windows server, our website brtechedigital.com is encrypted with let's encrypt.  
now we test our website in login panel



LOGIN

### Stay With Us for Further Explore

Enter your personal details and start journey with us

SIGN UP

LOGIN

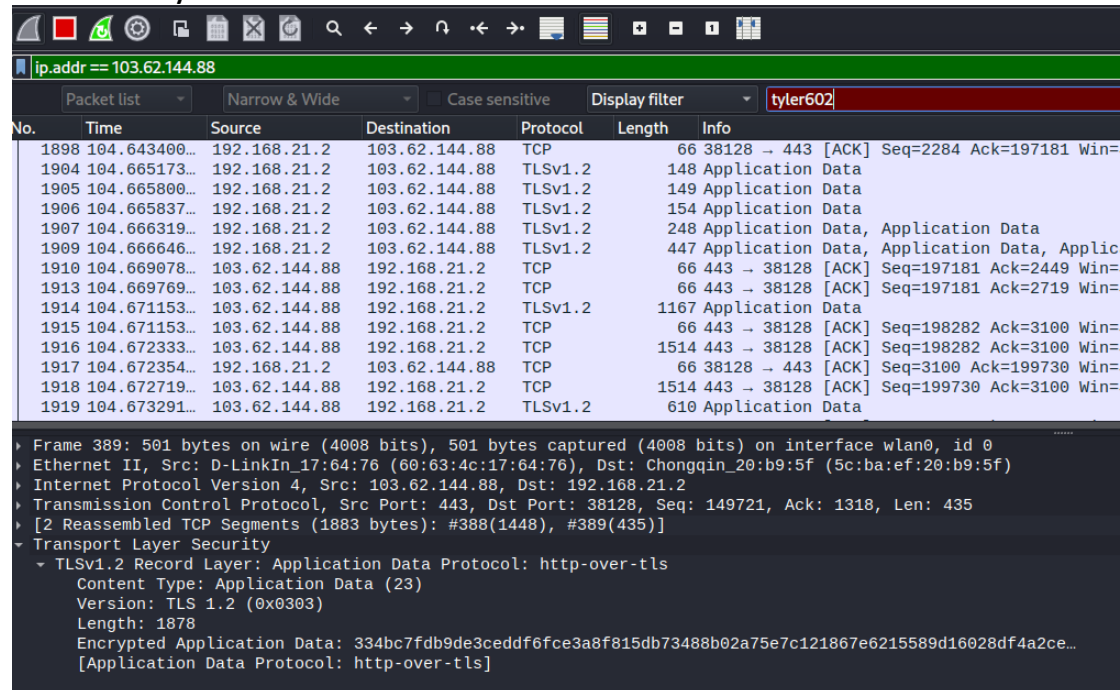
### Stay With Us for Further Explore

Enter your personal details and start journey with us

SIGN UP



## Running Wireshark from any devices.



Wireshark packet capture showing traffic from 103.62.144.88 to 192.168.21.2. The display filter is 'tyler602'. The packet list shows multiple TLSv1.2 application data packets. The packet details pane shows the structure of a TLSv1.2 record, including the application data protocol (http-over-tls).

No.	Time	Source	Destination	Protocol	Length	Info
1898	104.643400...	192.168.21.2	103.62.144.88	TCP	66	38128 → 443 [ACK] Seq=2284 Ack=197181 Win=
1904	104.665173...	192.168.21.2	103.62.144.88	TLSv1.2	148	Application Data
1905	104.665800...	192.168.21.2	103.62.144.88	TLSv1.2	149	Application Data
1906	104.665837...	192.168.21.2	103.62.144.88	TLSv1.2	154	Application Data
1907	104.666319...	192.168.21.2	103.62.144.88	TLSv1.2	248	Application Data, Application Data
1909	104.666646...	192.168.21.2	103.62.144.88	TLSv1.2	447	Application Data, Application Data, Applic
1910	104.669078...	103.62.144.88	192.168.21.2	TCP	66	443 → 38128 [ACK] Seq=197181 Ack=2449 Win=
1913	104.669769...	103.62.144.88	192.168.21.2	TCP	66	443 → 38128 [ACK] Seq=197181 Ack=2719 Win=
1914	104.671153...	103.62.144.88	192.168.21.2	TLSv1.2	1167	Application Data
1915	104.671153...	103.62.144.88	192.168.21.2	TCP	66	443 → 38128 [ACK] Seq=198282 Ack=3100 Win=
1916	104.672333...	103.62.144.88	192.168.21.2	TCP	1514	443 → 38128 [ACK] Seq=198282 Ack=3100 Win=
1917	104.672354...	192.168.21.2	103.62.144.88	TCP	66	38128 → 443 [ACK] Seq=3100 Ack=199730 Win=
1918	104.672719...	103.62.144.88	192.168.21.2	TCP	1514	443 → 38128 [ACK] Seq=199730 Ack=3100 Win=
1919	104.673291...	103.62.144.88	192.168.21.2	TLSv1.2	610	Application Data

Frame 389: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface wlan0, id 0  
Ethernet II, Src: D-LinkIn\_17:64:76 (60:63:4c:17:64:76), Dst: Chongqin\_20:b9:5f (5c:ba:ef:20:b9:5f)  
Internet Protocol Version 4, Src: 103.62.144.88, Dst: 192.168.21.2  
Transmission Control Protocol, Src Port: 443, Dst Port: 38128, Seq: 149721, Ack: 1318, Len: 435  
[2 Reassembled TCP Segments (1883 bytes): #388(1448), #389(435)]  
Transport Layer Security  
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls  
Content Type: Application Data (23)  
Version: TLS 1.2 (0x0303)  
Length: 1878  
Encrypted Application Data: 334bc7fdb9de3ceddf6fce3a8f815db73488b02a75e7c121867e6215589d16028df4a2ce...  
[Application Data Protocol: http-over-tls]

Here we see our data has been encrypted and file is in the link

<https://drive.google.com/file/d/1GDYkaAFo5m3vaQBU-1NxHFgSpigXTbjY/view?usp=sharing>