

## Single Page Website Secured With TLS

- ☒ Add the Page
- ☒ Add the Server
- ☒ Add TLS
- ☒ Dockerize
- ☒ Nginx
- ☐ Docker Compose

### Question 1

- a
    - <https://stackoverflow.com>: Let's Encrypt
    - <https://github.com>: DigiCert, Inc.
    - <https://about.gitlab.com>: GlobalSign nv-sa
    - <https://www.tutorialspoint.com>: DigiCert Inc
  - b
    - <https://stackoverflow.com>: no
    - <https://github.com>: no
    - <https://about.gitlab.com>: no
    - <https://www.tutorialspoint.com>: no
  - c
    - <https://stackoverflow.com>: February 2, 2022
    - <https://github.com>: March 31, 2022
    - <https://about.gitlab.com>: November 19, 2022
    - <https://www.tutorialspoint.com>: December 1, 2022
  - d
    - <https://stackoverflow.com>: SHA-256 with RSA Encryption
    - <https://github.com>: ECDSA with SHA-256
    - <https://about.gitlab.com>: SHA-256 with RSA Encryption
    - <https://www.tutorialspoint.com>: SHA-256 with RSA Encryption
  - e
    - <https://stackoverflow.com>: RSA
    - <https://github.com>: Elliptic Curve P-256
    - <https://about.gitlab.com>: RSA
    - <https://www.tutorialspoint.com>: RSA
  - f
    - <https://stackoverflow.com>: extracted with openssl
- ```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnnR4op27mxXFQRA/b1b4
zCn/KPr3NDX3grqVZQOC35WpvtT+qxhZZb+OGQpf5KWe9dbTDefE1CIud1clo5yI
oe0cPwyKt0mknvVyJb+UexDrg1b6jBY7c10HV5gDk1Ui48v9YNbBiCYs1HssnVg
VwkYhVrcxtAoc3K1Q08NJ5rT/cy90U01Cd2pXaY4GA8h0Wt60XUyHgHyd7+KhMOM
ZkbqleQL4cQ5McbPM5PG2EahQacV2INXXNRwiyRtoH7f8KahlzBHfHwOnYeyfAQm
5GmU0uPROSroSn9+KvaXOMI3li4pK7VZTkP+IvN6cmBBAQdrLVbgu+ER0iqEQei+
tQIDAQAB
```

```

-----END PUBLIC KEY-----
- https://github.com: extracted with openssl
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAErfb3dbHTSVQKXRBxvdw1BksiHKIj
Tp+h/rnQjL05vAwjx8+RppBa2EWRAx0+wSN6ucTInUf21uC5dmtQNmb3DQ==
-----END PUBLIC KEY-----
- https://about.gitlab.com: extracted with openssl
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtnVz0wp+fYpFksh2WAQp
gy/OtJVy5wDrxa0FXDJbWbcb/zZeTaSj7k3KxMLHgOM15FHYRmQjE3ZhoLZ14ac5
7uvojQyJBWu+3mIELrxi+bHJsFLRenAW84n0kWqXdDQjw/x0rf0T14Pm3L7M1Ick
EkvnS84zU02MN84FC9MZVAyDKj17dKIF6LyQQw185WajnGctmPcSV0m0hUrXylhg
N84SSSFaXs15ukpC2j50MoVvPwBsnuvh3YKb0mJLvofxWzBZR3c9qEufBNi81MbS
8RQi/Hk5/m0k1J6bkD6Wib5kFw5mbTz81M3XCosdb35X04/czr5TKMhHIwsmF12c
SQIDAQAB
-----END PUBLIC KEY-----
- https://www.tutorialspoint.com: extracted with openssl
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtnVz0wp+fYpFksh2WAQp
gy/OtJVy5wDrxa0FXDJbWbcb/zZeTaSj7k3KxMLHgOM15FHYRmQjE3ZhoLZ14ac5
7uvojQyJBWu+3mIELrxi+bHJsFLRenAW84n0kWqXdDQjw/x0rf0T14Pm3L7M1Ick
EkvnS84zU02MN84FC9MZVAyDKj17dKIF6LyQQw185WajnGctmPcSV0m0hUrXylhg
N84SSSFaXs15ukpC2j50MoVvPwBsnuvh3YKb0mJLvofxWzBZR3c9qEufBNi81MbS
8RQi/Hk5/m0k1J6bkD6Wib5kFw5mbTz81M3XCosdb35X04/czr5TKMhHIwsmF12c
SQIDAQAB
-----END PUBLIC KEY-----

```

## Question 2

giallery.com found here. certificate is also included along side this report.

## Question 3

- en.wikipedia.com: extracted with openssl
  - Serial Number: 031A6B6D125D7706BC61A22BCE280534 Revocation Date: Jun 17 15:09:35 2021 GMT
  - Serial Number: 0C40FB9449BF2E9D2F2912BE9CA27924 Revocation Date: Jun 17 15:09:36 2021 GMT
  - Serial Number: 04B439CB22317491A5AB479E9F5BB629 Revocation Date: Jun 22 15:14:56 2021 GMT
  - Serial Number: 0E066FD67EEC3E47699DAC681C4A2D5B Revocation Date: Jun 22 15:38:18 2021 GMT
  - Serial Number: 0A461ABB1944D9E52D7AC59FB13238C9 Revocation Date: Jun 29 16:13:31 2021 GMT
- dictionary.com: no crl uri was provided by the certificate

## Question 4

### What I've Done, TL;DR

- First we need a webserver which is located at `main.go` serving the contents of `static` directory which contains `index.html`. This is single page website and nothing more. The webserver's code is also super simple.
- After that we had a website running, it was time to Dockerize the project with image name being `sinashk/tlswebsite`.
- I also tried to use `docker-compose` and move `nginx` and `website` on there but had some issues and failed in doing so.
- Then I used a domain `shantech.ir` on virtual machine from arvan cloud and got a certificate from let's encrypt and configured nginx.

### Steps in Securing With SSL

Keep in mind that the packages used are for ubuntu server you might have the same packages or not, check the name of these packages in your own linux distribution. - first updated my DNS record with arvan's dns. - then sshed into the server and did some updates and installed `nginx` and `certbot` and `python3-certbot-nginx` - then created `www.shantech.ir.conf` inside `/etc/nginx/conf.d/` and inside it was this content:

```
# file /etc/nginx/conf.d/www.shantech.ir.conf
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    root /var/www/html;
    server_name shantech.ir www.shantech.ir;
}
```

- then we reload `nginx`. I had some problems with this operation saying configuration already exists. The reason was that my config was listening to `default_server`, so as 2 other configs scattered around. I simply deleted them you can change the `default_server` to something else both work.

```
$ sudo nginx -t && nginx -s reload
```

- then ran the following command with `certbot` to generate certificates and also update `www.shantech.ir.conf`

```
sudo certbot --nginx -d shantech.ir -d www.shantech.ir
```

- After this operation `certbot` asked to update the `nginx` config so that it would redirect all http traffic to https and I said yes. the final config is included in the root directory of the project with the name `nginx.conf`.
- Now just update the config and your locations. I added `/` to go to `localhost:8080` which I'm going to run the webserver on that port later. this is the part I added:

```
# file /etc/nginx/conf.d/www.shantech.ir.conf
server {
    root /var/www/html;
    server_name shantech.ir www.shantech.ir;

    listen [::]:443 ssl ipv6only=on; # managed by Certbot
    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/shantech.ir/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/shantech.ir/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

##### I ADDED #####
    location ~ ^/ {
        proxy_pass http://localhost:8080;
    }
#####
}
server {
    if ($host = www.shantech.ir) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    if ($host = shantech.ir) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    listen 80 default_server;
    listen [::]:80 default_server;
    server_name shantech.ir www.shantech.ir;
    return 404; # managed by Certbot
}
```

- Then i pulled the image with `docker pull sinashk/tlswebsite`. You might need to login to your account for this one with `docker login` and you might also need a vpn ;)
- After the image was pulled, we can simply run it with:

```
$ docker run -p 127.0.0.1:8080:8080 sinashk/tlswebsite
```

- Well there is one more thing we need block other traffics otherwise some can ignore tls by going straigh to port 8080 so we need to activate our firewall. I will use `ufw`. NOTE: `ufw` cannot prevent traffic to access a port mapped by docker since docker modifies iptables directly. So with an enabled firewall you can still visit `shantech.ir:8080` and bypass TLS

that's why we need to add 127.0.0.1 at first to restrict the traffic to be coming from the machine itself.

```
# IMPRTANT otherwise you will lose your session and probably won't be able to connect to you
$ sudo ufw allow ssh
$ sudo ufw allow https
$ sudo ufw allow http
# now enable the firewall
$ sudo ufw enable
# check you firewall status
$ sudo ufw status
```

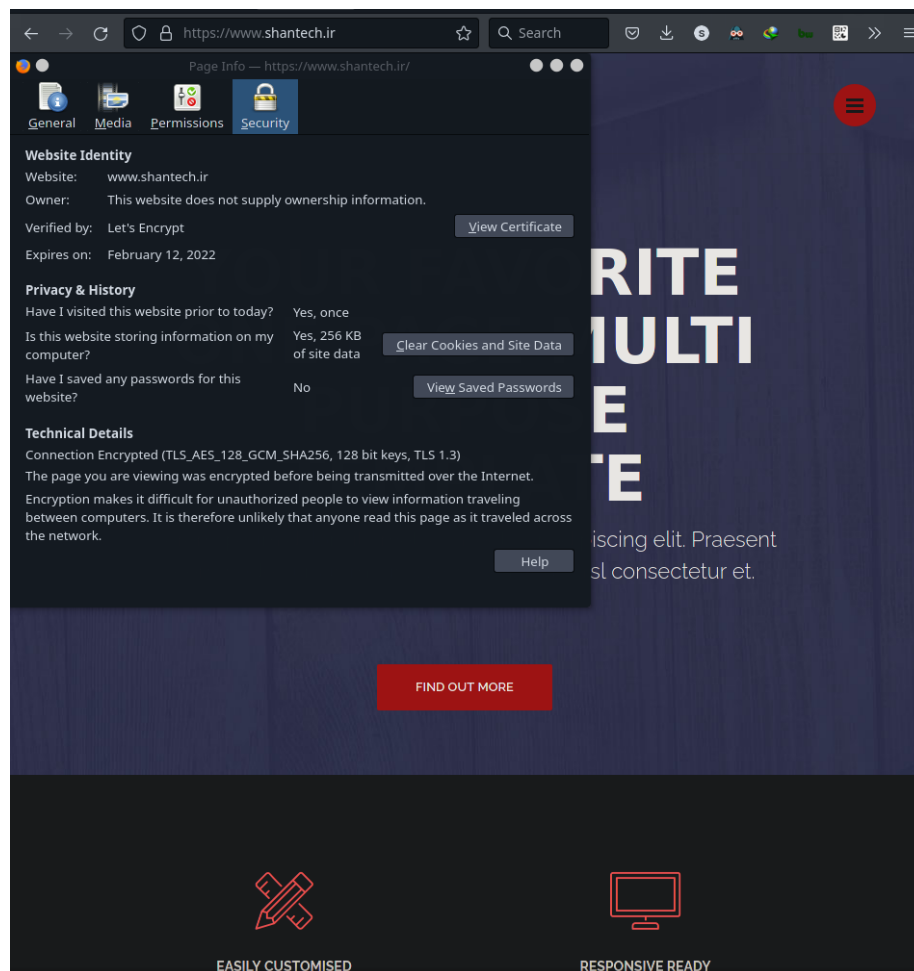


Figure 1: proof

- Enjoy your secure website :). It's still sad that i couldn't make docker

compose work :(.

## Question 5

First of all this is public ip so i will not share it in this document and configure wireshark to show the domain name instead of IP address. I will also hide the IP in packets. By going to **View > Name Resolution** and checking **Resolve Network Addresses** IP addresses will be replaced by domain name. Now my system's name is `loopspc` so you will see this instead of `192.168.1.111` which is my private IP address.

Now when you open up **wireshark** you will be presented with a list of network devices to select and capture packet on. My network interface is `enp9s0`. You can find yours by running `ip addr` in the **terminal**.

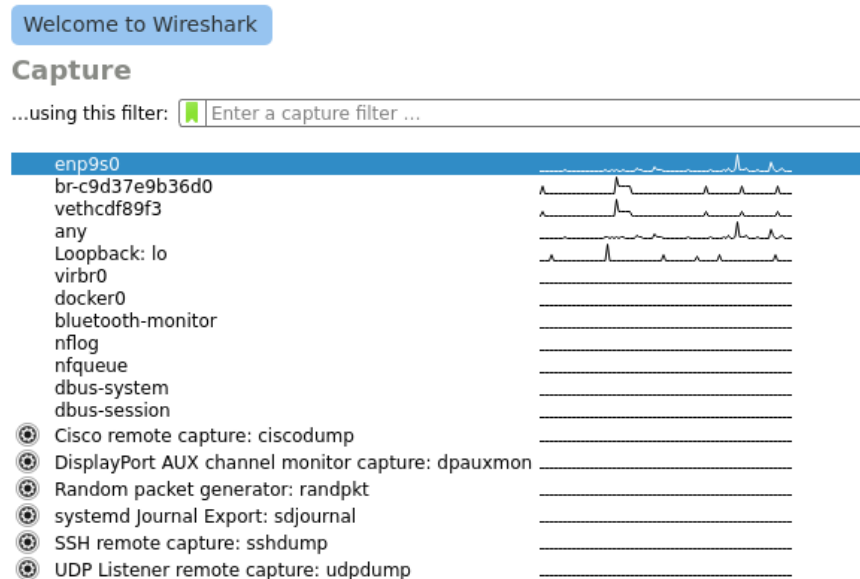


Figure 2: Wireshark select net dev

After selecting the interface we need to filter the output because it's not on Loopback and there so many packets we can filter based on destination IP and source IP, and we don't need to specify the IP since we have checked that box before. So type this filter in:

ip.dst == www.shantech.ir or ip.src == www.shantech.ir

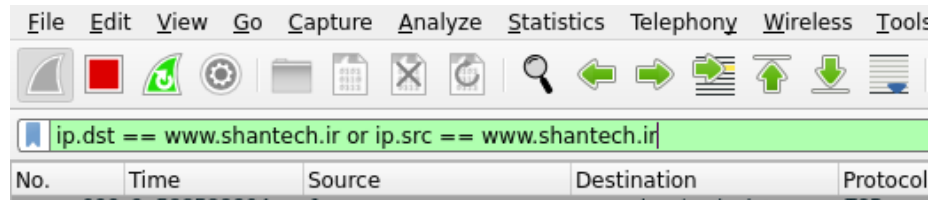


Figure 3: Wireshark filter

It's kinda weird to see ip.dst being equal to www.shantech.ir but it is what it is.

Now if we visit www.shantech.ir and come back to wireshark we will see that there are a lot of packets captured to wireshark.

A screenshot of the Wireshark packet list. The top toolbar shows various icons. The filter bar contains the text 'ip.dst == www.shantech.ir or ip.src == www.shantech.ir'. Below the filter bar is a table with columns: No., Time, Source, Destination, Protocol, and Length. The table contains several rows of network packets, including TCP, TLSv1.3, and Application Data. The first row is highlighted in blue.

| No. | Time        | Source          | Destination     | Protocol | Length |
|-----|-------------|-----------------|-----------------|----------|--------|
| 840 | 5.440177883 | loopspc         | www.shantech.ir | TCP      | 74     |
| 841 | 5.44062336  | loopspc         | www.shantech.ir | TCP      | 74     |
| 842 | 5.440971467 | loopspc         | www.shantech.ir | TCP      | 74     |
| 843 | 5.447499868 | www.shantech.ir | loopspc         | TCP      | 66     |
| 844 | 5.407161297 | loopspc         | www.shantech.ir | TCP      | 66     |
| 845 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 846 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 847 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 848 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 849 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 850 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 851 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 852 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 853 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 854 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 855 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 856 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 857 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 858 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 859 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 860 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 861 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 862 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 863 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 864 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 865 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 866 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 867 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 868 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 869 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 870 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 871 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 872 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 873 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 874 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 875 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 876 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 877 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 878 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 879 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 880 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 881 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 882 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 883 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 884 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 885 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 886 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |
| 887 | 5.408419978 | www.shantech.ir | loopspc         | TCP      | 66     |

Figure 4: wire shark packets

You can see Client Hello and Server Hello which belongs to TLS. Here is some of the metadata attached to Client Hello Packet:

Things like: - session token - cipher suites - supported versions - ...

And Here is Sever Hello:

Things like: - Selected cipher suit - Session ID - ...

Now to decrypt TLS, we use SSL Log File since it works for most situations. All we need to do is set an environment variable and then open a browser and visit the website.

```
# set the environment variable
$ export SSLKEYLOGFILE=/home/loop/sslkeylogfile
```

# now open a browser. keep in mind that the browser

| No.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Time        | Source  | Destination     | Protocol | Length | Info         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------|-----------------|----------|--------|--------------|
| 849                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 5.489178439 | loopspc | www.shantech.ir | TLSv1.3  | 571    | Client Hello |
| ▶ Frame 849: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface enp9s0, id 0<br>▶ Ethernet II, Src: loopspc (1c:1b:0d:06:fa:49), Dst: homerouter.cpe (10:b1:f8:c1:cc:32)<br>▶ Internet Protocol Version 4, Src: loopspc (192.168.1.111), Dst: www.shantech.ir (192.168.1.111)<br>▶ Transmission Control Protocol, Src Port: 36342, Dst Port: 443, Seq: 1, Ack: 1, Len: 517                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |         |                 |          |        |              |
| ▾ Transport Layer Security <ul style="list-style-type: none"> <li>▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello               <ul style="list-style-type: none"> <li>Content Type: Handshake (22)</li> <li>Version: TLS 1.0 (0x0301)</li> <li>Length: 512</li> <li>▾ Handshake Protocol: Client Hello                   <ul style="list-style-type: none"> <li>Handshake Type: Client Hello (1)</li> <li>Length: 508</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Random: 2ade7c227d53255f0eb49e2b2a861a2b00cc82e1cc49dd82c1675ab49fe97d19</li> <li>Session ID Length: 32</li> <li>Session ID: 266f9fe8c7b6d663b9e515523af918942530946f170899facaf19202dcaf0a7e</li> <li>Cipher Suites Length: 32</li> <li>▾ Cipher Suites (16 suites)                       <ul style="list-style-type: none"> <li>Compression Methods Length: 1</li> <li>Compression Methods (1 method)</li> <li>Extensions Length: 403</li> <li>Extension: Reserved (GREASE) (len=0)</li> <li>Extension: server_name (len=16)</li> <li>Extension: extended_master_secret (len=0)</li> <li>Extension: renegotiation_info (len=1)</li> <li>Extension: supported_groups (len=10)</li> <li>Extension: ec_point_formats (len=2)</li> <li>Extension: session_ticket (len=0)</li> <li>Extension: application_layer_protocol_negotiation (len=14)</li> <li>Extension: status_request (len=5)</li> <li>Extension: signature_algorithms (len=18)</li> <li>Extension: signed_certificate_timestamp (len=0)</li> <li>Extension: key_share (len=43)</li> <li>Extension: psk_key_exchange_modes (len=2)</li> <li>Extension: supported_versions (len=11)</li> <li>Extension: compress_certificate (len=3)</li> <li>Extension: Unknown type 17513 (len=5)</li> <li>Extension: Reserved (GREASE) (len=1)</li> <li>Extension: padding (len=200)</li> </ul> </li> </ul> </li> </ul> </li> </ul> |             |         |                 |          |        |              |

Figure 5: Wireshark client hello

| No.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Time       | Source          | Destination | Protocol | Length | Info                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------|-------------|----------|--------|----------------------------------------------------|
| 861                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 5.51523194 | www.shantech.ir | loopspc     | TLSv1.3  | 2174   | Server Hello, Change Cipher Spec, Application Data |
| ▶ Frame 861: 2774 bytes on wire (22192 bits), 2774 bytes captured (22192 bits) on interface enp9s0, id 0<br>▶ Ethernet II, Src: homerouter.cpe (10:b1:f8:c1:cc:32), Dst: loopspc (1c:1b:0d:06:fa:49)<br>▶ Internet Protocol Version 4, Src: www.shantech.ir (192.168.1.111), Dst: loopspc (192.168.1.111)<br>▶ Transmission Control Protocol, Src Port: 443, Dst Port: 36342, Seq: 1, Ack: 518, Len: 2720                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |                 |             |          |        |                                                    |
| ▾ Transport Layer Security <ul style="list-style-type: none"> <li>▾ TLSv1.3 Record Layer: Handshake Protocol: Server Hello               <ul style="list-style-type: none"> <li>Content Type: Handshake (22)</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Length: 122</li> <li>▾ Handshake Protocol: Server Hello                   <ul style="list-style-type: none"> <li>Handshake Type: Server Hello (2)</li> <li>Length: 118</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Random: 79181856e1866dd3713eeb26ebce1f964ca356cb82c9cf8d075f170e7448f30</li> <li>Session ID Length: 32</li> <li>Session ID: 266f9fe8c7b6d663b9e515523af918942530946f170899facaf19202dcaf0a7e</li> <li>Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)</li> <li>Compression Method: null (0)</li> <li>Extensions Length: 46</li> <li>Extension: supported_versions (len=2)</li> <li>Extension: key_share (len=36)</li> </ul> </li> </ul> </li> <li>▾ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec               <ul style="list-style-type: none"> <li>Content Type: Change Cipher Spec (20)</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Length: 1</li> <li>Change Cipher Spec Message</li> </ul> </li> <li>▾ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls               <ul style="list-style-type: none"> <li>Opaque Type: Application Data (23)</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Length: 42</li> <li>Encrypted Application Data: fdda9fc9b577fefb5c4d77f53971ba04f22a2599aa1ab4386f50d1e0a23bbabcd43f4837..</li> <li>[Application Data Protocol: http-over-tls]</li> </ul> </li> </ul> |            |                 |             |          |        |                                                    |

Figure 6: Wireshark server hello



```
# should be opened from this shell since you set
# the variable in this shell not hte entire system
$ firefox https://www.shantech.ir
```

Now we just need to point wireshark to that file. Go to Edit > Preferences and under protocol section find TLS and write the path of the sslkeylogfile to (Pre)-Master-Secret log filename

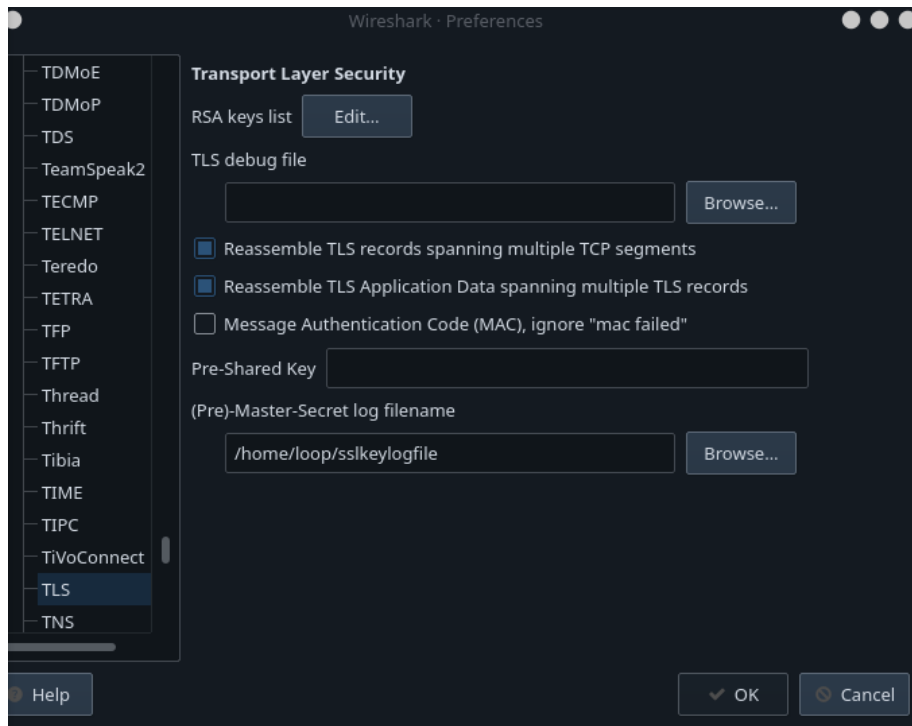


Figure 7: setting key log

After saving the changes we can see that packets are decrypted and here is proof of that.

Now after decrypting TLS packets, the protocol encapsulated inside of it is visible and you can see it in the above picture as well.

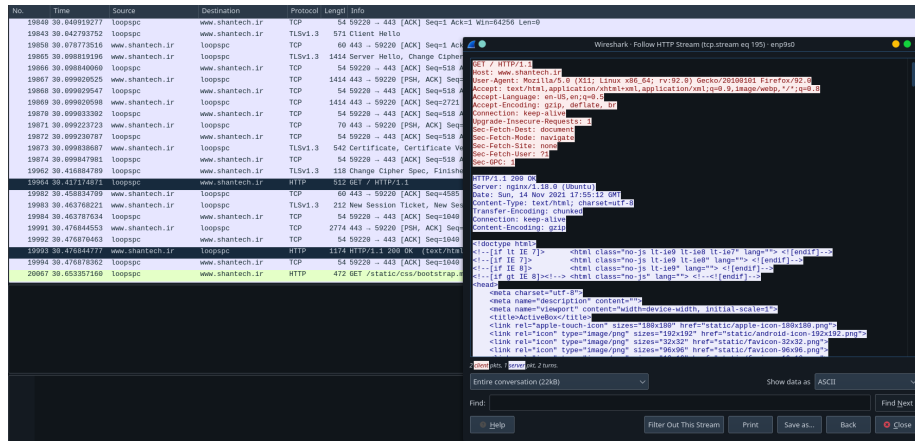


Figure 8: wireshark decrypt proof