Ex.No.11 29/09/2024	**ANALYSIS OF SECURITY PROTOCOLS AT TRANSPORT AND APPLICATION LAYER**

AIM:

To study the working principle of security protocols like SSL/TLS using Wireshark and PGP using chrome plugin – Mailvelope.

THEORY:

Wireshark:

Wireshark is a free and open-source packet analyser .Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

SSL/TLS:

1. SSL: - Secure Socket Layer (SSL) is a cryptographic protocol designed to provide secure communication over a computer network. It was developed by Netscape in the 1990s to establish an encrypted link between the web server and a web browser. SSL operates by using encryption to secure the transmission of data ensuring that sensitive information such as credit card details and personal data remains confidential.
2. TLS: - The Transport Layer Security (TLS) is the successor to SSL and is designed to provide improved security and efficiency. TLS was developed as an enhancement of SSL to the address various vulnerabilities and to the incorporate modern cryptographic techniques. The first version, TLS 1.0 was based on SSL 3.0 but included significant improvements. TLS continues to evolve with the newer versions offering enhanced the security features.

PGP:

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

WORKSHEET (using sample.pcap)

1. What version of SSL is supported by the client?

The version of SSL Supported by client is **SSL 2.0 (0x0002)**

2. List the cryptographic algorithms supported by the client in Client Hello message.

```
▾ Cipher Suites (20 suites)
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
```

3. List the various parameters present in the public key certificate of the server.

Certificate	a814d7366b78535271ccf60d293e60004b54c40bb16ce5a1d3f917439782fc06

4. Identify the public key of the server? Can you trust the same?

Public Key	4e6feeee7e3558966013f9e64027f156218b5c918f1ebe00742a0e9041cfe233

Yes, we can trust this because it has been issued by a certificate authority.

5. Identify the length of key exchanged by the Client?

The length of key exchanged by client is 128bits.

```
Handshake Protocol: Server Key Exchange
   Handshake Type: Server Key Exchange (12)
   Length: 361
▾  EC Diffie-Hellman Server Params
     Curve Type: named_curve (0x03)
     Named Curve: secp384r1 (0x0018)
     Pubkey Length: 97
     Pubkey: 04fd3897955947a7b28a8aa87f78183838384ae32c96a5e6e1063
   ▸ Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
     Signature Length: 256
     Signature […]: 60640f9c4634e092a752f6b4eada6cea6dadeb07abf7c5
```

6. What algorithm is used for encrypting the session key?

```
Random: 670272ee922eda5c418995282fe9c94509abac2bd67c0ce7c589c62e6238890d
Session ID Length: 32
Session ID: 730f000048f7af7b630d400b93a3e72b36057e342b59379b31e240e1d6999755
```

7. List the various parameters specified in the Encrypted handshake message.

```
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 1300
    Encrypted Application Data […]: ef751b68ef1ba1465140f4003f56f6f2dc2d81e6ee5
    [Application Data Protocol: Hypertext Transfer Protocol]
```

8. Calculate the time taken for completion of the entire handshake protocol.

The time taken for completion of the entire handshake protocol is 2.808775 seconds

9. Examine the certificates of gmail server, any bank server. Identify the Cerification Authority, Hierarchy of Certification Authority, Validity date, crypto algorithms used for signing etc.

```
▾ Certificates (829 bytes)
    Certificate Length: 826
  ▾ Certificate […]: 308203363082029fa003020102020101300d06092a864886f70d01010405003081a9310b3009060355040613025859311530130603550408130c536e616b6520446573657274…
    ▾ signedCertificate
        version: v3 (2)
        serialNumber: 0x01
      ▾ signature (md5WithRSAEncryption)
          Algorithm Id: 1.2.840.113549.1.1.4 (md5WithRSAEncryption)
      ▾ issuer: rdnSequence (0)
        ▾ […]rdnSequence: 7 items (pkcs-9-at-emailAddress=ca@snakeoil.dom,id-at-commonName=Snake Oil CA,id-at-organizationalUnitName=Certificate Authority,id-…
          ▸ RDNSequence item: 1 item (id-at-countryName=XY)
          ▸ RDNSequence item: 1 item (id-at-stateOrProvinceName=Snake Desert)
          ▸ RDNSequence item: 1 item (id-at-localityName=Snake Town)
          ▸ RDNSequence item: 1 item (id-at-organizationName=Snake Oil, Ltd)
          ▸ RDNSequence item: 1 item (id-at-organizationalUnitName=Certificate Authority)
          ▸ RDNSequence item: 1 item (id-at-commonName=Snake Oil CA)
          ▸ RDNSequence item: 1 item (pkcs-9-at-emailAddress=ca@snakeoil.dom)
      ▾ validity
        ▸ notBefore: utcTime (0)
        ▸ notAfter: utcTime (0)
      ▾ subject: rdnSequence (0)
        ▾ […]rdnSequence: 7 items (pkcs-9-at-emailAddress=www@snakeoil.dom,id-at-commonName=www.snakeoil.dom,id-at-organizationalUnitName=Webserver Team,id-at…
          ▸ RDNSequence item: 1 item (id-at-countryName=XY)
          ▸ RDNSequence item: 1 item (id-at-stateOrProvinceName=Snake Desert)
          ▸ RDNSequence item: 1 item (id-at-localityName=Snake Town)
          ▸ RDNSequence item: 1 item (id-at-organizationName=Snake Oil, Ltd)
          ▸ RDNSequence item: 1 item (id-at-organizationalUnitName=Webserver Team)
          ▸ RDNSequence item: 1 item (id-at-commonName=www.snakeoil.dom)
          ▸ RDNSequence item: 1 item (pkcs-9-at-emailAddress=www@snakeoil.dom)
```

10. Enlist the differences between HTTP and HTTPS.

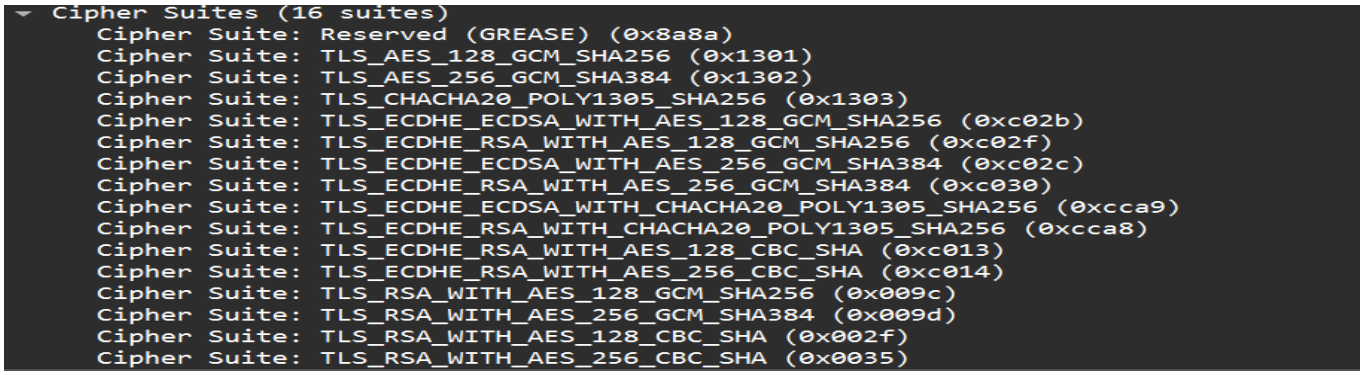
HTTP	HTTPs
HTTP uses port number 80 for communication.	HTTPs uses 443 port number for communication.
In HTTP, encryption is absent.	In HTTPs encryption is present.
HTTP does not require any certificates.	HTTPs requires SSL certificate.
HTTP works at Application Layer.	HTTPs works at Transport as well as Application Layer.

WORKSHEET (For packet captured for real time data)

1. What version of TLS is supported by the client?

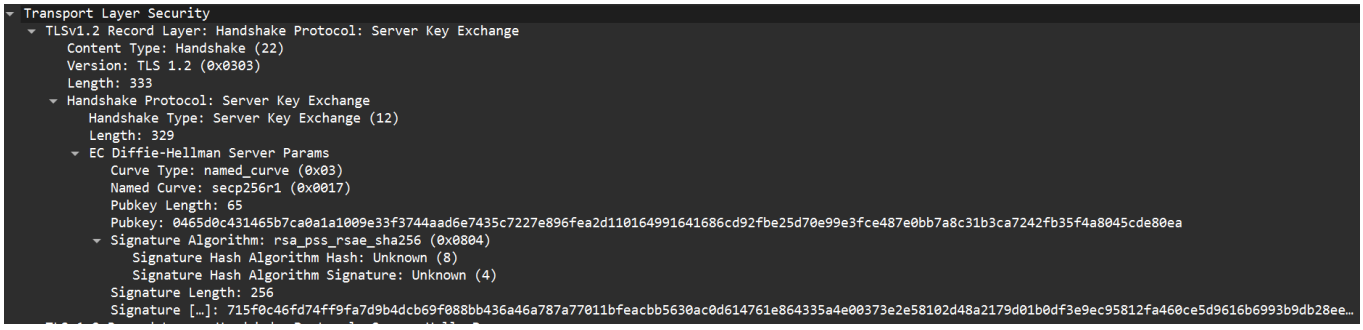
Client Supports TLS Version 1.0 (0x0301)

2. List the cryptographic algorithms supported by the client in Client Hello message.



3. List the various parameters present in the public key certificate of the server.

4. Identify the public key of the server? Can you trust the same?



Yes, we can trust it because it is being signed by the certificate authority.

5. Identify the length of key exchanged by the Client?

```
▾ Handshake Protocol: Client Key Exchange
    Handshake Type: Client Key Exchange (16)
    Length: 66
```

6. What algorithm is used for encrypting the session key?

The algorithm used to encrypt session id is RSA.

```
▾ Random: 127b41eab53322affc8ecadb8970dbd31baa47b26e010dcc21e61ec7b22cc8f1
    GMT Unix Time: Oct 29, 1979 23:24:50.000000000 India Standard Time
    Random Bytes: b53322affc8ecadb8970dbd31baa47b26e010dcc21e61ec7b22cc8f1
  Session ID Length: 32
  Session ID: 8b33a9598c9eabeb5ba79adee21cbe86576f16ec717c25bd6616fb39b284f7c6
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
```

7. List the various parameters specified in the Encrypted handshake message.

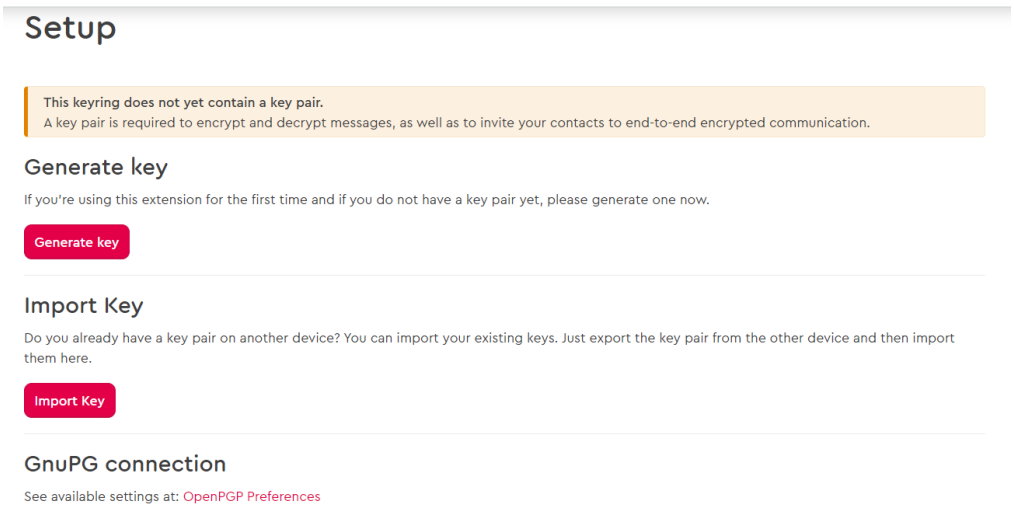
```
▾ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```

8. Calculate the time taken for completion of the entire handshake protocol.

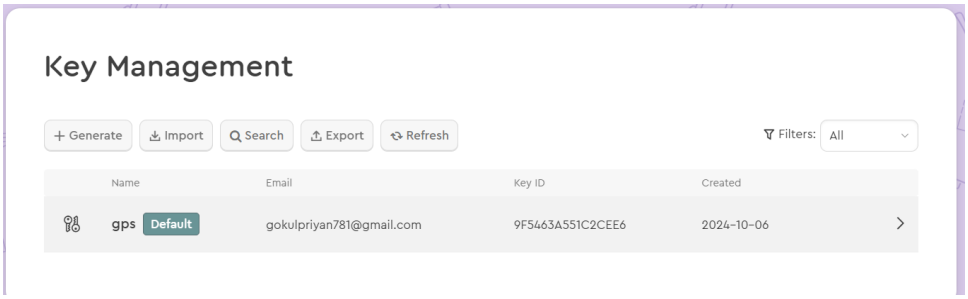
The time taken is 0.003117 seconds.

PRETTY GOOD PRIVACY - ANALYSIS

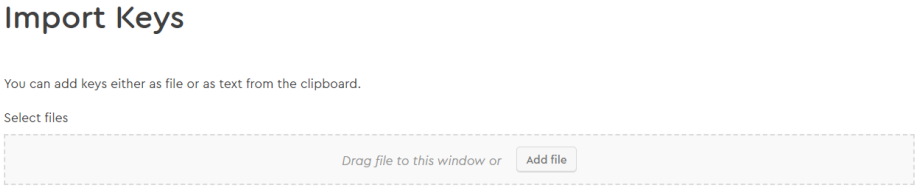
1. Installation of Mailvelope



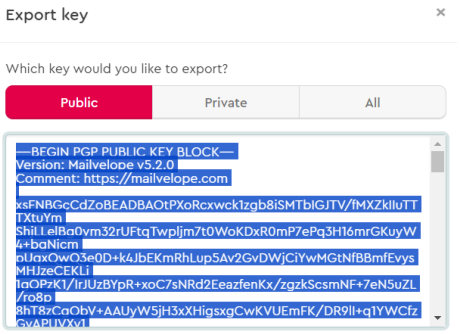
2. Generation of public-private key pair



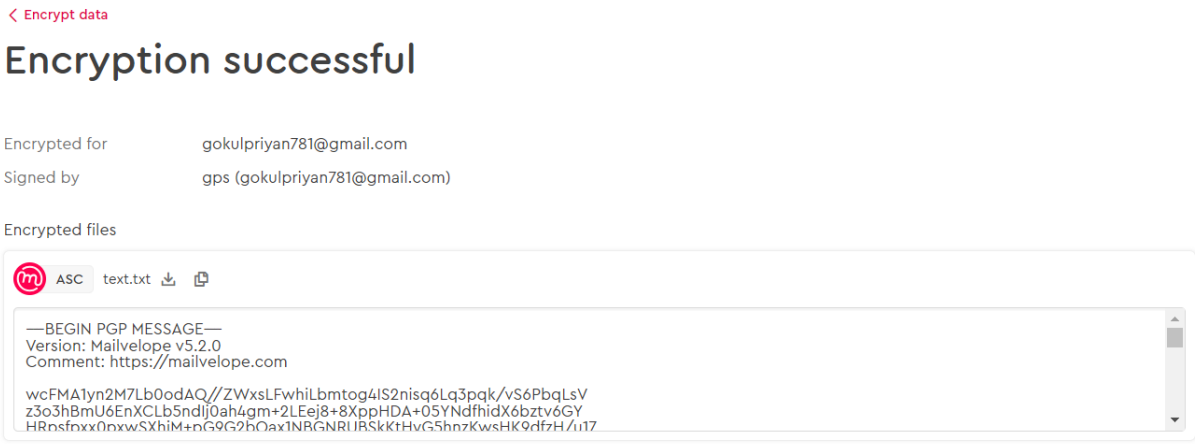
3. Import Public Key



4. Export Public Key



5. Encrypt and send a email



RESULT:

Thus, we have studied the working principle of security protocols like SSL/TLS using Wireshark and PGP using chrome plugin – Mailvelope.

Evaluation

Parameter	Max Marks	Marks Obtained
Uniqueness of the Work	15	
Completion of experiment on time	10	
Documentation	5	
Total	30	
Signature of the faculty with Date		