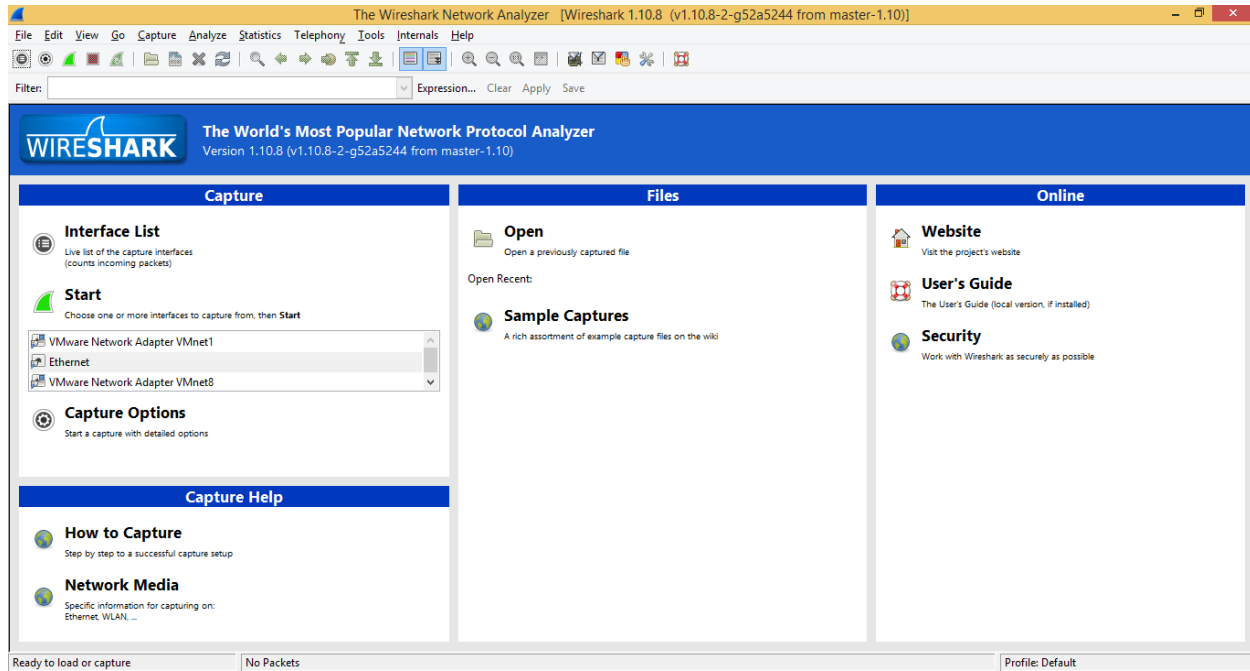


Practical no:1

Aim : Working with Sniffers for monitoring network communication

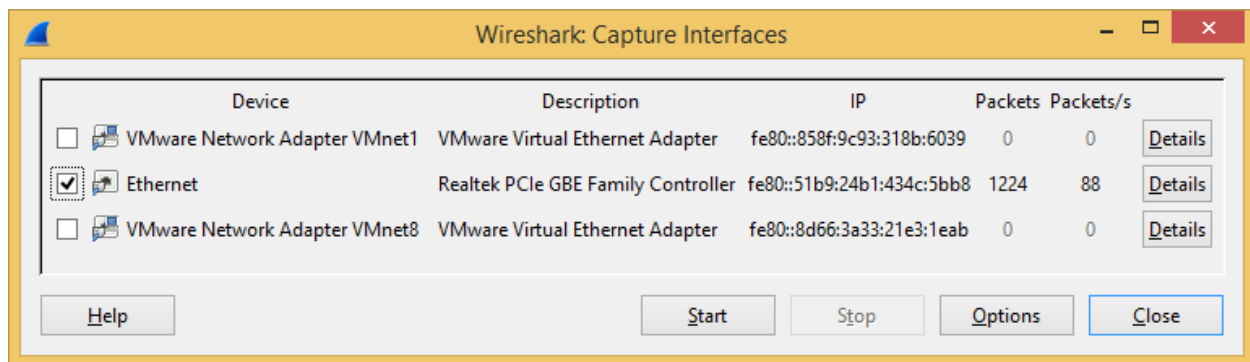
Open the Wireshark



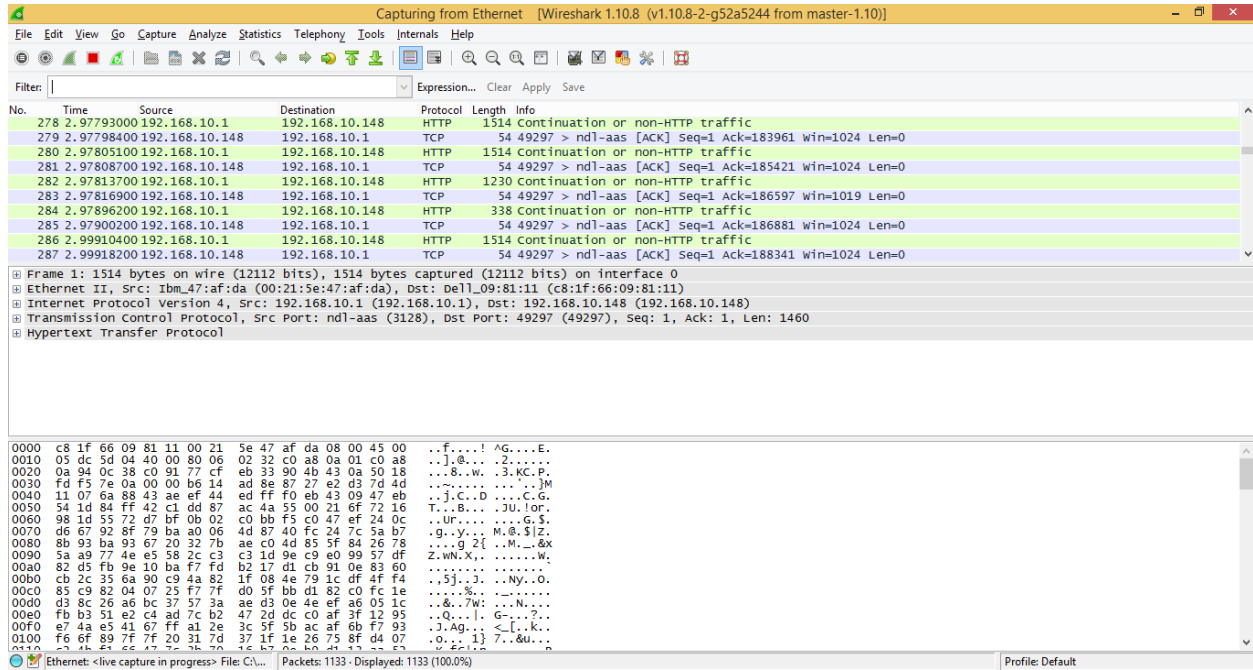
Click on the “**Interfaces**” button on the toolbar:

Check on the **Ethernet** Tab

And Click **Start**



You will get the List of all the packet arriver through your port



Click on any of the http and Expand the "Data" tab

Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic
3	0.00087100	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic
5	0.00900800	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic
7	0.02954600	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic
9	0.03041700	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic
11	0.03048000	192.168.10.1	192.168.10.148	HTTP	1230	Continuation or non-HTTP traffic
13	0.03051400	192.168.10.1	192.168.10.148	HTTP	338	Continuation or non-HTTP traffic
15	0.03457000	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic
17	0.04076600	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic
19	0.06749200	192.168.10.1	192.168.10.148	HTTP	1514	Continuation or non-HTTP traffic

Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: Idm47:af:da (00:21:5e:47:af:da), Dst: Dell_09:81:11 (c8:1f:66:09:81:11)

Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.148 (192.168.10.148)

Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 49297 (49297), Seq: 1, Ack: 1, Len: 1460

Hypertext Transfer Protocol

Data (1460 bytes)

Data: b614ad8e8727e2d37d4d11076a8843aeeff4edf7f0eb4309...

[Length: 1460]

0030 fd f5 7e 0a 00 00 b6 14 ad 8e 87 27 e2 d3 7d 4eJH

0040 11 07 68 38 23 ae ef 44 ed ff f0 eb 43 09 47 ebC.G.

0050 54 1d 84 ff 42 c1 dd 87 ac 4a 55 00 21 6f 72 1eT..B...JU.ior.

0060 98 1d 55 72 d7 bf 0b 02 c0 bb f5 c0 47 ef 24 0cUr... ..G.S.

0070 46 67 92 85 79 ba 20 06 1f 03 48 79 1c df af f4g..y...M.8.5Iz

0080 8b 93 ba 93 67 20 32 7b ae c0 4d 85 5f 84 26 78-0 21...M...&

0090 5a 99 77 4e e5 58 2c c3 c3 1d 9e ce e0 99 57 dfZ.w.N.X... ..W.

00a0 82 d5 fb 9e 10 ba f7 fd b2 17 d1 cb 91 0e 83 60

00b0 fb 2c 25 6a 90 c9 48 82 1f 03 48 79 1c df af f45J... ..Ny...0.

00c0 89 c9 82 04 07 25 f7 7f d0 5f bb d1 82 c0 fc 1e

00d0 d3 8c 26 a6 bc 37 57 3a ae d3 0e 4e ef a6 05 1c&.7w... ..N....

00e0 fb b3 51 e2 c4 ad 7c b2 47 2d cd c0 af 3f 32 95Q... ..G... ..?

00f0 ef 4a e3 41 67 ff 31 2e 3c 5f 3b ac af 6b 77 92J.Ag... ..<[.k...

0100 f6 ef 89 7f 7f 20 31 7d 37 1f 1e 26 75 8f 04 07o... ..1 7...&

0110 c2 4b f1 66 47 7c 3b 70 16 b7 0e b9 d1 13 aa 52K.FG;pR

0120 96 dd 23 09 b6 82 28 de 32 f7 03 6c 81 48 2f 8b#... ..(2...1.H/.

0130 4b dc 16 64 35 74 28 7c ee 96 34 87 86 c1 62 6aK... ..A... ..I... ..

0140 64 2d 16 64 35 74 28 7c ee 96 34 87 86 c1 62 6aK... ..A... ..I... ..

Data (data), 1460 bytes Packets: 3100 - Displayed: 1459 (47.1%) Profile: Default

Click on Hypertext Transfer Protocol

Click on Post

Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
12	0.60620400	192.168.10.148	192.168.10.1	HTTP	1126	POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0
22	0.94584200	192.168.10.148	192.168.10.1	HTTP	1043	POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0
31	1.19350300	192.168.10.1	192.168.10.148	HTTP	116	HTTP/1.0 200 OK (text/html)
38	1.35737300	fe80::293c:5b67:47af:f02::c		SSDP	208	M-SEARCH * HTTP/1.1
47	2.05527400	192.168.10.148	192.168.10.1	HTTP	1047	POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0
50	2.20731400	192.168.10.1	192.168.10.148	HTTP	116	HTTP/1.0 200 OK (text/html)
59	2.21444500	192.168.10.148	192.168.10.1	HTTP	1016	POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0
64	2.47994800	192.168.10.1	192.168.10.148	HTTP	327	HTTP/1.0 200 OK (text/html)
73	2.48340500	192.168.10.148	192.168.10.1	HTTP	1016	POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0
76	2.69309900	192.168.10.148	192.168.10.148	HTTP	990	HTTP/1.0 200 OK (text/html)

Hypertext Transfer Protocol

POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n

[Expert Info (Chat/Sequence): POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n]

[Message: POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n]

[Severity Level]: chat

[Group: Sequence]

Request Method: POST

Request URI: http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest

Request Version: HTTP/1.0

Accept-Language: en-us\r\n

Accept: */*\r\n

User-Agent: Mozilla/4.0 (compatible; win32; Commtouch Http Client)\r\n

Content-Length: 785\r\n

Host: webres1.qheal.ctmail.com\r\n

Proxy-Authorization: Basic ogm=\r\n

\r\n

0030 01 00 85 45 00 00 50 4f 53 54 20 68 74 70 3aE..P.O.st http

0040 2f 2f 63 62 72 65 73 31 2e 71 68 65 61 6c 2e//webres1.qheal.

0050 63 74 6d 61 69 6c 2e 63 6f 6d 2f 53 70 61 6d 52ctmail.c om/SpamR

0060 85 73 6f 6c 76 65 72 4e 47 2f 53 70 61 6d 32 65esolverN g/SpamRe

0070 73 6f 6c 76 65 72 4e 47 2e 64 6c 6c 3f 44 6f 4esolverNG .dll?DoN

0080 65 77 52 65 71 75 65 73 74 20 48 54 54 30 2f 31ewReques t HTTP/1

0090 2e 30 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 750. Acce pt-Langu

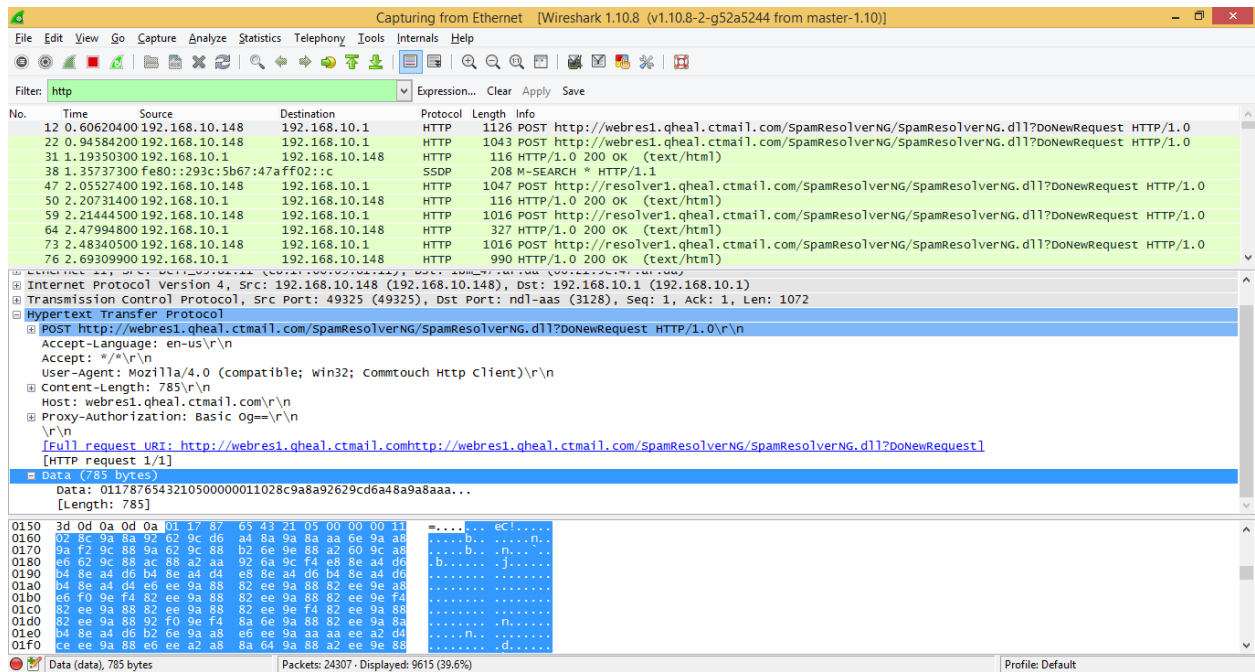
00a0 61 67 65 3a 20 65 6e 2d 75 73 0d 0a 41 63 63 65age: en-us. Acce

00b0 70 74 3a 20 2a 2f 2a 0d 0a 35 73 65 72 2d 41 67pt: */*. User-Ag

00c0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 3a 2e 30ent: Moz illa/4.0

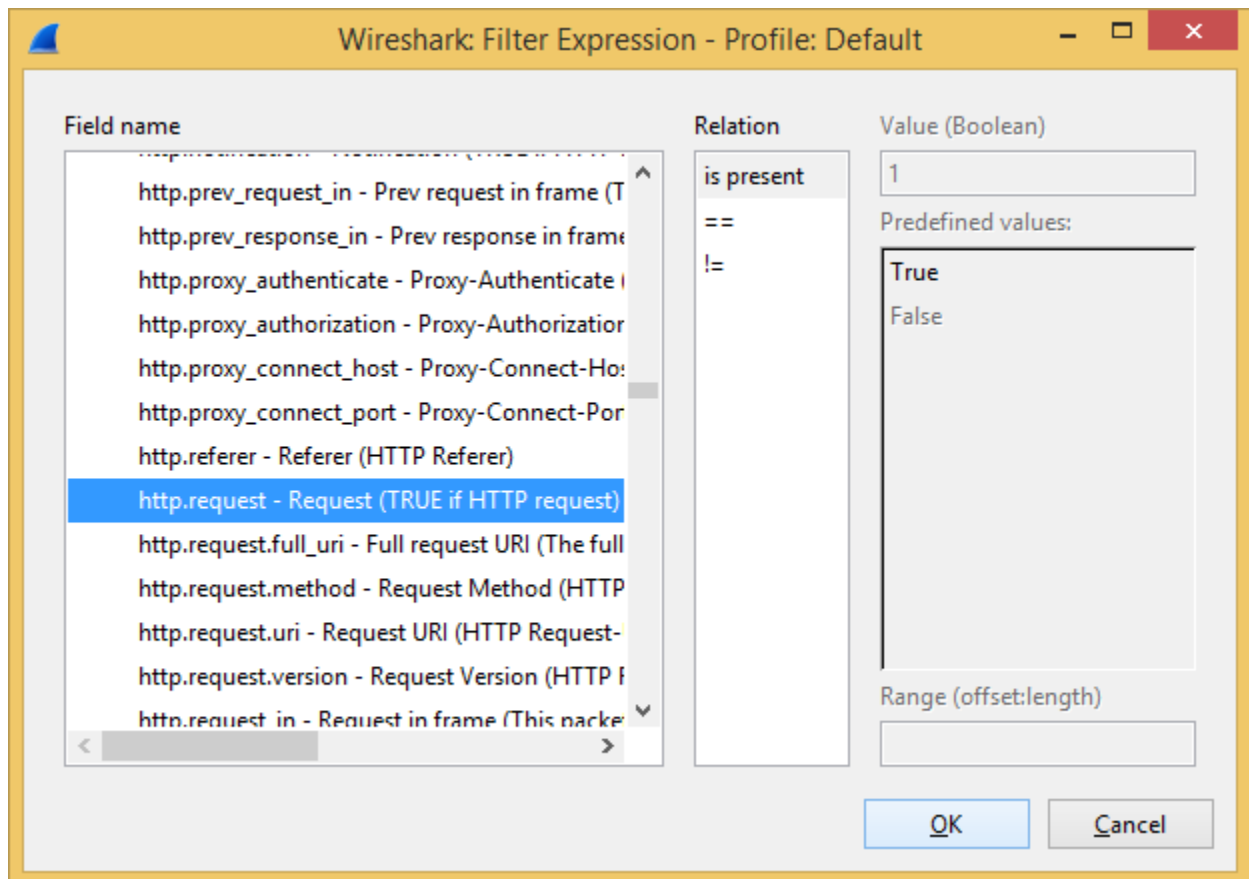
00d0 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 57 69(compat ible; wi

Text item (text), 94 bytes Packets: 3264 - Displayed: 2458 (46.7%) Profile: Default

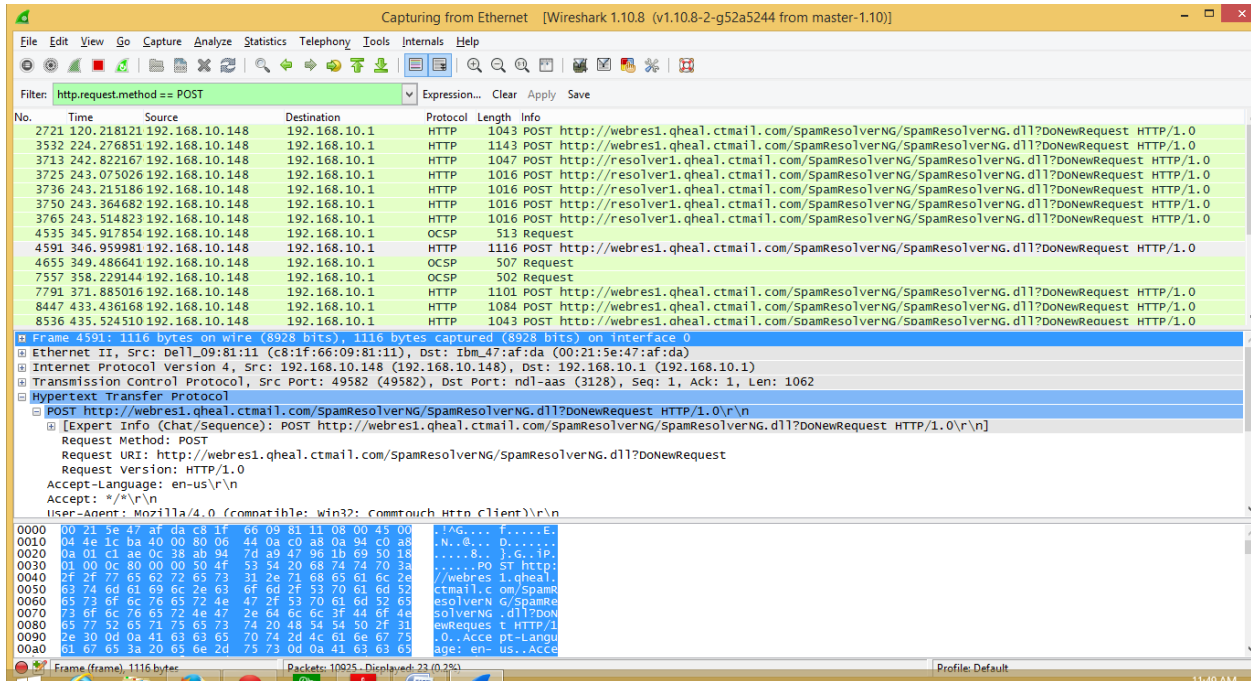


Go to **Expression** Tab Near the Filter Tab

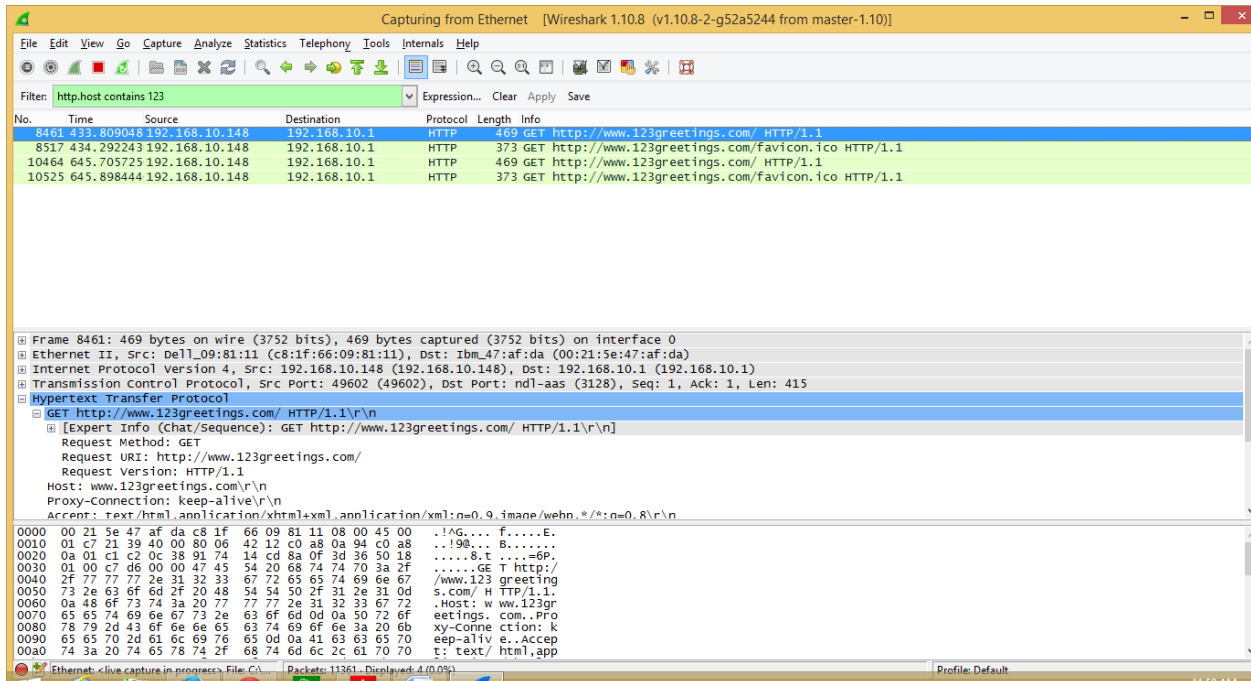
Click on "http.request - Request(True if HTTP request)"



Enter this command "**http.request.method == POST**" into Filter tab



Enter "**http.host contains 123**" in the Filter Tab



Enter "http.request.uri contains 123" in the Filter Tab

The screenshot shows the Wireshark interface with the filter 'http.request.uri contains 123' applied. The packet list pane shows four captured packets, all of which are HTTP GET requests to 'http://www.123greetings.com/'. The packet details pane for the selected packet (No. 8461) shows the following structure:

- Frame 8461: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface 0
- Ethernet II, Src: Dell_09:81:11 (c8:1f:66:09:81:11), Dst: Ibm_47:af:da (00:21:5e:47:af:da)
- Internet Protocol Version 4, Src: 192.168.10.148 (192.168.10.148), Dst: 192.168.10.1 (192.168.10.1)
- Transmission Control Protocol, Src Port: 49602 (49602), Dst Port: ndl-aas (3128), Seq: 1, Ack: 1, Len: 415
- Hypertext Transfer Protocol
 - GET http://www.123greetings.com/ HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET http://www.123greetings.com/ HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: http://www.123greetings.com/
 - Request Version: HTTP/1.1
 - Host: www.123greetings.com\r\n
 - Proxy-Connection: keep-alive\r\n
 - Accent: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

The packet bytes pane shows the raw data of the request, including the GET method, URI, and headers.

Enter http.referer contains 123 "simple2" in the Filter Tab

The screenshot shows the Wireshark interface with the filter 'http.referer contains simple2' applied. The packet list pane shows one captured packet, which is an HTTP GET request to 'http://www.scf.usc.edu/~csci571/Special/HTTP/USCBullet1.gif'. The packet details pane for the selected packet (No. 14781) shows the following structure:

- Frame 14781: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) on interface 0
- Ethernet II, Src: Dell_09:81:11 (c8:1f:66:09:81:11), Dst: Ibm_47:af:da (00:21:5e:47:af:da)
- Internet Protocol Version 4, Src: 192.168.10.148 (192.168.10.148), Dst: 192.168.10.1 (192.168.10.1)
- Transmission Control Protocol, Src Port: 49692 (49692), Dst Port: ndl-aas (3128), Seq: 860, Ack: 433, Len: 385
- Hypertext Transfer Protocol
 - GET http://www.scf.usc.edu/~csci571/Special/HTTP/USCBullet1.gif HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET http://www.scf.usc.edu/~csci571/Special/HTTP/USCBullet1.gif HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: http://www.scf.usc.edu/~csci571/Special/HTTP/USCBullet1.gif
 - Request Version: HTTP/1.1
 - Host: www.scf.usc.edu\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0\r\n
 - Accent: image/png,image/jpeg,*/*;q=0.8,*/*;q=0.5\r\n

The packet bytes pane shows the raw data of the request, including the GET method, URI, and headers.

Enter "http.response.code == 404" in the Filter Tab

The screenshot shows the Wireshark interface with the filter "http.response.code == 404" applied. The packet list pane shows a single packet (No. 14243) at Time 1020.77753, Source 192.168.10.1, Destination 192.168.10.148, Protocol HTTP, Length 60, and Info HTTP/1.0 404 Not Found (text/html). The packet details pane shows the Hypertext Transfer Protocol section with the status code 404 and response phrase "Not Found". The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
14243	1020.77753	192.168.10.1	192.168.10.148	HTTP	60	HTTP/1.0 404 Not Found (text/html)

```
Frame 14243: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: IbmL47:af:da (00:21:5e:47:af:da), Dst: Dell_09:81:11 (c8:1f:66:09:81:11)
Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.148 (192.168.10.148)
Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 49691 (49691), Seq: 626, Ack: 346, Len: 0
[3 Reassembled TCP Segments (625 bytes): #14240(325), #14241(300), #14243(0)]
Hypertext Transfer Protocol
  HTTP/1.0 404 Not Found\r\n
  [Expert Info (Chat/Sequence): HTTP/1.0 404 Not Found\r\n]
    Request version: HTTP/1.0
    Status Code: 404
    Response Phrase: Not Found
    Date: Fri, 07 Nov 2014 06:20:52 GMT\r\n
    Server: Apache/1.3.31 (Unix) PHP/4.3.9 mod_javout/3.0.3\r\n
0000 c8 1f 66 09 81 11 00 21 5e 47 af da 08 00 45 00  ..f....! AG....E.
0010 00 28 3d 37 40 00 80 06 27 b3 c0 a8 0a 01 c0 a8  ..?m@...$......
0020 0a 94 0c 38 c2 1b b3 3e b0 0c 98 df bc 3d 50 11  ..8...(.T...P.
0030 fe a6 94 8a 00 00 00 00 00 00 00 00 00 00 00  ..#...G! F89a....
.....l.
.....m..l. ....T..Q
.....S 3NH;161.
```

Enter http.content_type == "image/gif" in the Filter Tab

The screenshot shows the Wireshark interface with the filter "http.content_type == 'image/gif'" applied. The packet list pane shows a single packet (No. 14787) at Time 1033.82055, Source 192.168.10.1, Destination 192.168.10.148, Protocol HTTP, Length 230, and Info HTTP/1.0 200 OK (GIF89a). The packet details pane shows the Hypertext Transfer Protocol section with the status code 200 and response phrase "OK". The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
14787	1033.82055	192.168.10.1	192.168.10.148	HTTP	230	HTTP/1.0 200 OK (GIF89a)

```
Frame 14787: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0
Ethernet II, Src: IbmL47:af:da (00:21:5e:47:af:da), Dst: Dell_09:81:11 (c8:1f:66:09:81:11)
Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.148 (192.168.10.148)
Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 49692 (49692), Seq: 882, Ack: 1245, Len: 176
[2 Reassembled TCP Segments (625 bytes): #14786(449), #14787(176)]
Hypertext Transfer Protocol
  HTTP/1.0 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.0 200 OK\r\n]
    Request version: HTTP/1.0
    Status Code: 200
    Response Phrase: OK
    Date: Fri, 07 Nov 2014 06:21:05 GMT\r\n
    Server: Apache/1.3.31 (Unix) PHP/4.3.9 mod_javout/3.0.3\r\n
0000 c8 1f 66 09 81 11 00 21 5e 47 af da 08 00 45 00  ..f....! AG....E.
0010 00 d8 3f 6d 40 00 80 06 24 cd c0 a8 0a 01 c0 a8  ..?m@...$......
0020 0a 94 0c 38 c2 1c c4 28 cd 34 94 b8 1c 81 50 18  ..8...(.T...P.
0030 fb 23 6c a0 00 00 47 49 46 38 39 61 12 0a 00  ..#...G! F89a....
0040 c4 ff 00 ff ff f9 ff ff d3 ff ff c6 ff ea a9 fd  ..#...G! F89a....
0050 e8 90 fd dd 93 f0 d5 8f ef cf 85 dc bd 6c d1 b6  ..#...G! F89a....
0060 6f cf b3 6d cb ae 69 c0 c0 c0 94 87 54 8f 82 51  o..m..l. ....T..Q
0070 78 6d 44 5e 56 35 5b 53 33 4e 48 2c 3b 36 21 00  xmdV[S 3NH;161.
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..#...G! F89a....
```

Practical no: 2

Aim : Using open SSL for web server - browser communication

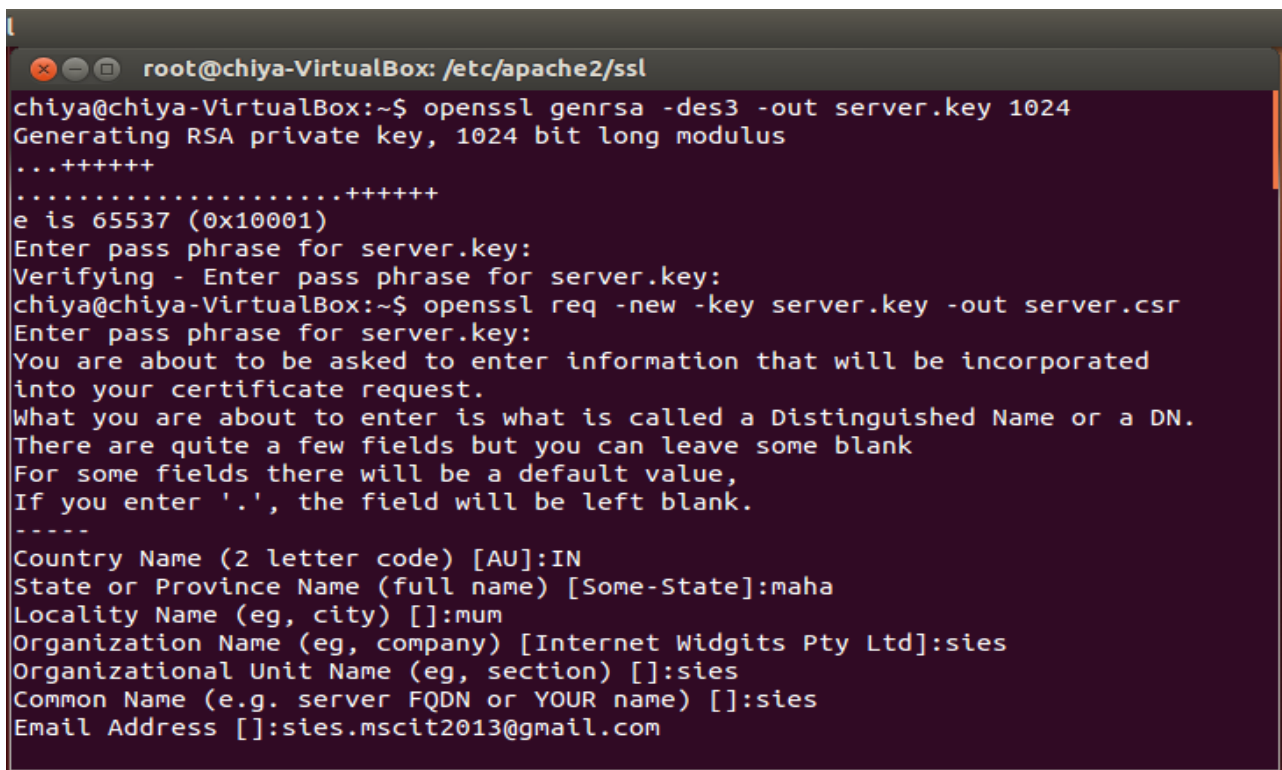
- Install apache if it is not installed
- Install openssl if it is not installed

Generate the RSA Key

openssl genrsa -des3 -out server.key 2048

[enter a password]

[confirm your password]



```
root@chiya-VirtualBox: /etc/apache2/ssl
chiya@chiya-VirtualBox:~$ openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
...+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
chiya@chiya-VirtualBox:~$ openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:maha
Locality Name (eg, city) []:mum
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sies
Organizational Unit Name (eg, section) []:sies
Common Name (e.g. server FQDN or YOUR name) []:sies
Email Address []:sies.mscit2013@gmail.com
```


Certificate Signing Request (CSR)

```
openssl req -new -key server.key -out server.csr
```

[enter your private key password]

[enter your two character country code]

[enter your full state or province name]

[enter your city name]

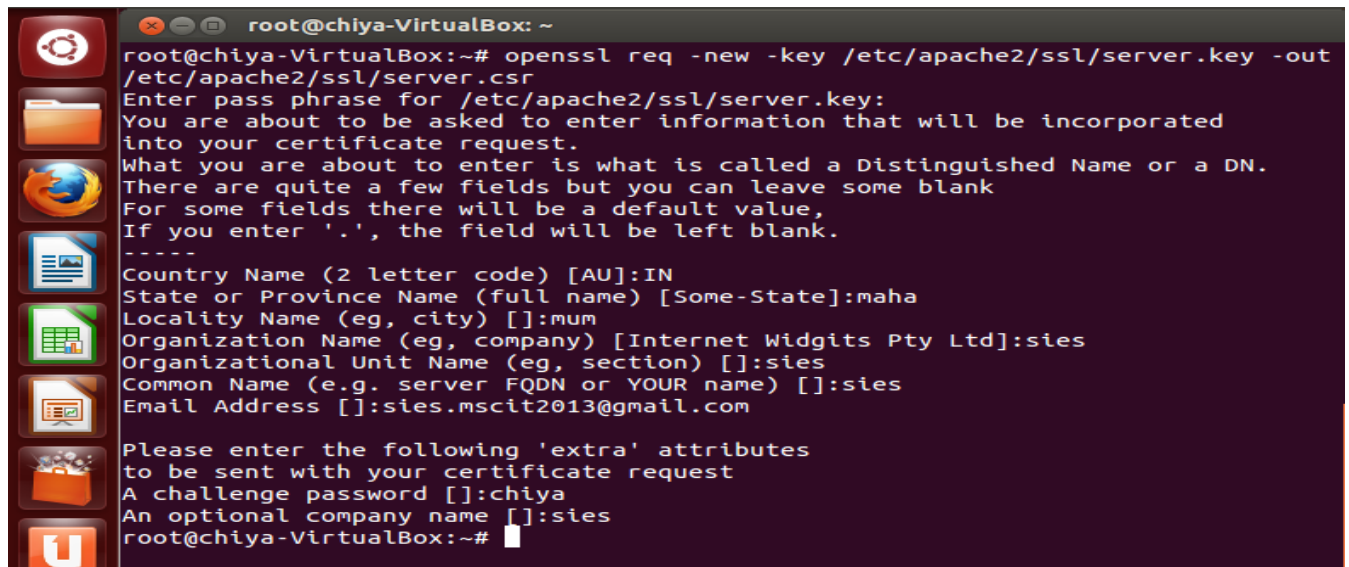
[enter your company name]

[enter your organizational unit or leave it blank]

[enter your common name or fqdn]

[enter your admin email address]

[leave the rest of the attributes blank]



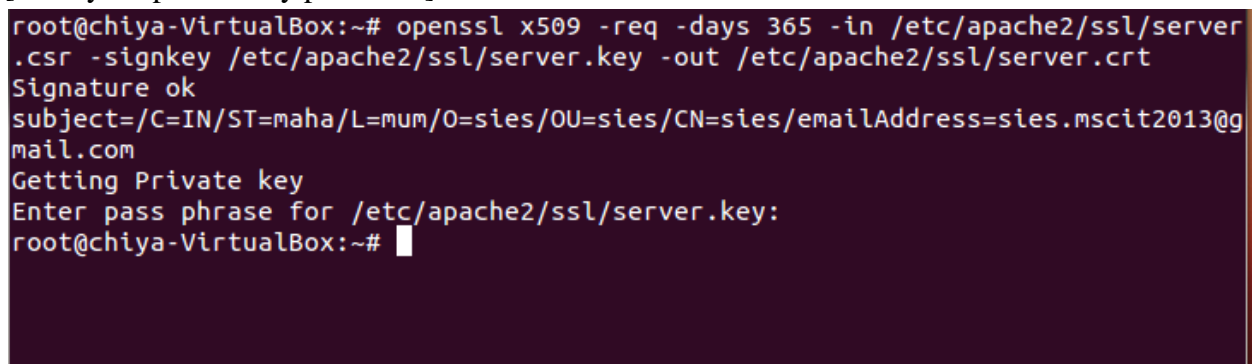
```
root@chiya-VirtualBox: ~
root@chiya-VirtualBox:~# openssl req -new -key /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.csr
Enter pass phrase for /etc/apache2/ssl/server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:maha
Locality Name (eg, city) []:mum
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sies
Organizational Unit Name (eg, section) []:sies
Common Name (e.g. server FQDN or YOUR name) []:sies
Email Address []:sies.mscit2013@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:chiya
An optional company name []:sies
root@chiya-VirtualBox:~#
```

Sign Your Certificate Signing Request

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

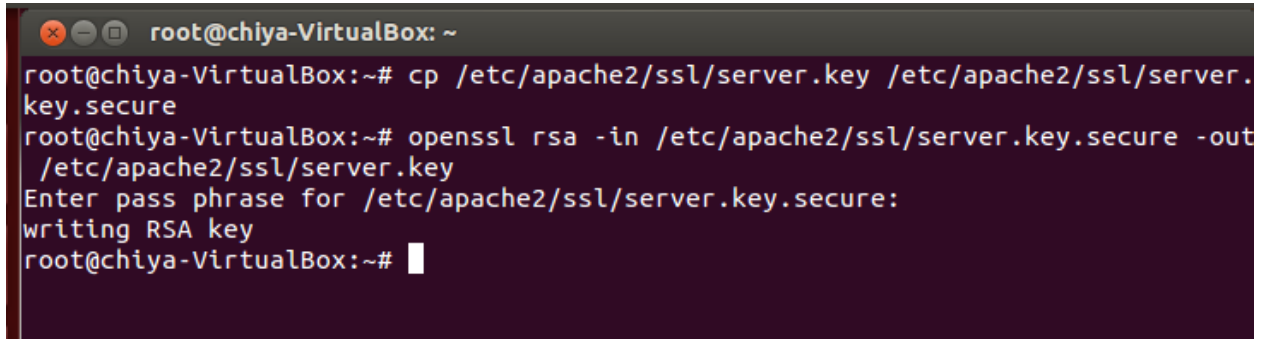
[enter your private key password]



```
root@chiya-VirtualBox:~# openssl x509 -req -days 365 -in /etc/apache2/ssl/server.csr -signkey /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.crt
Signature ok
subject=/C=IN/ST=maha/L=mum/O=sies/OU=sies/CN=sies/emailAddress=sies.mscit2013@gmail.com
Getting Private key
Enter pass phrase for /etc/apache2/ssl/server.key:
root@chiya-VirtualBox:~#
```

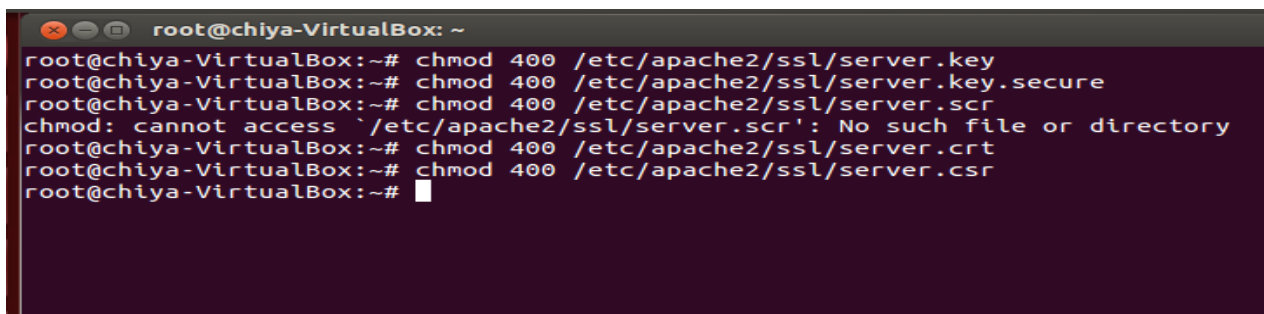
Remove the PassPhrase From Your Private Key

```
cp server.key server.key.secure
openssl rsa -in server.key.secure -out server.key
[enter your private key password]
```



```
root@chiya-VirtualBox: ~
root@chiya-VirtualBox:~# cp /etc/apache2/ssl/server.key /etc/apache2/ssl/server.
key.secure
root@chiya-VirtualBox:~# openssl rsa -in /etc/apache2/ssl/server.key.secure -out
/etc/apache2/ssl/server.key
Enter pass phrase for /etc/apache2/ssl/server.key.secure:
writing RSA key
root@chiya-VirtualBox:~#
```

Set file permissions



```
root@chiya-VirtualBox: ~
root@chiya-VirtualBox:~# chmod 400 /etc/apache2/ssl/server.key
root@chiya-VirtualBox:~# chmod 400 /etc/apache2/ssl/server.key.secure
root@chiya-VirtualBox:~# chmod 400 /etc/apache2/ssl/server.scr
chmod: cannot access `/etc/apache2/ssl/server.scr': No such file or directory
root@chiya-VirtualBox:~# chmod 400 /etc/apache2/ssl/server.crt
root@chiya-VirtualBox:~# chmod 400 /etc/apache2/ssl/server.csr
root@chiya-VirtualBox:~#
```

Configure SSL setting in apache server

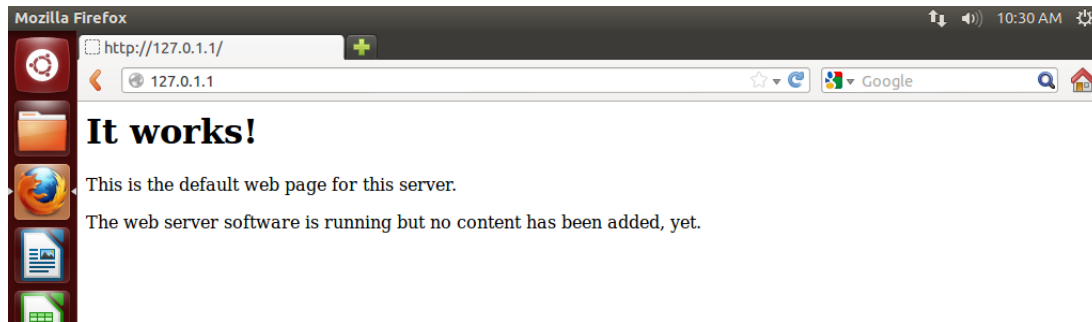
- make sure all cryptography files exists in /etc/apache2/ssl
- create sites-available folder in /etc/apache2
- create default-ssl file in path /etc/apache2/sites-available/default-ssl

```
root@chiya-VirtualBox: /etc/apache2/sites-available
chiya@chiya-VirtualBox:~$ sudo -s
[sudo] password for chiya:
root@chiya-VirtualBox:~# cd /etc/apache2/
root@chiya-VirtualBox:/etc/apache2# dir
apache2.conf  envvars  mods-available  ports.conf  sites-enabled
conf.d        magic    mods-enabled    sites-available  ssl
root@chiya-VirtualBox:/etc/apache2/ssl# cd ssl
root@chiya-VirtualBox:/etc/apache2/ssl# ls
server.crt  server.csr  server.key  server.key.secure
root@chiya-VirtualBox:/etc/apache2/ssl#
root@chiya-VirtualBox:/etc/apache2/ssl# cd /etc/apache2/sites-available/
root@chiya-VirtualBox:/etc/apache2/sites-available# ls
default  default-ssl  default-ssl-
root@chiya-VirtualBox:/etc/apache2/sites-available#
root@chiya-VirtualBox:/etc/apache2/sites-available# gedit /etc/apache2/sites-ava
ilable/default-ssl
```

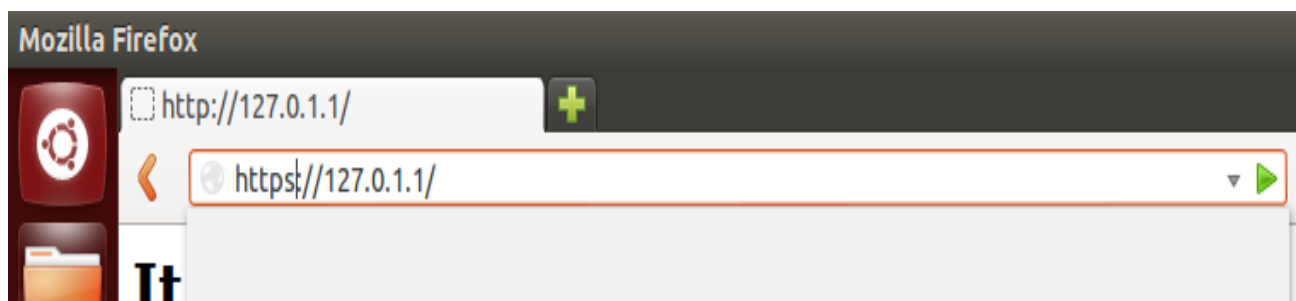
default-ssl confuration file

```
default-ssl (/etc/apache2/sites-available) - gedit
File Edit View Search Tools Documents Help
default-ssl x
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin admin@example.com
    ServerName 127.0.1.1
    ServerAlias 127.0.1.1
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key
    <FilesMatch "\.(cgi|shml|phtml|php)$">
      SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
      SSLOptions +StdEnvVars
    </Directory>
    BrowserMatch "MSIE [2-6]" \
      nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0
    BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
  </VirtualHost>
</IfModule>
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

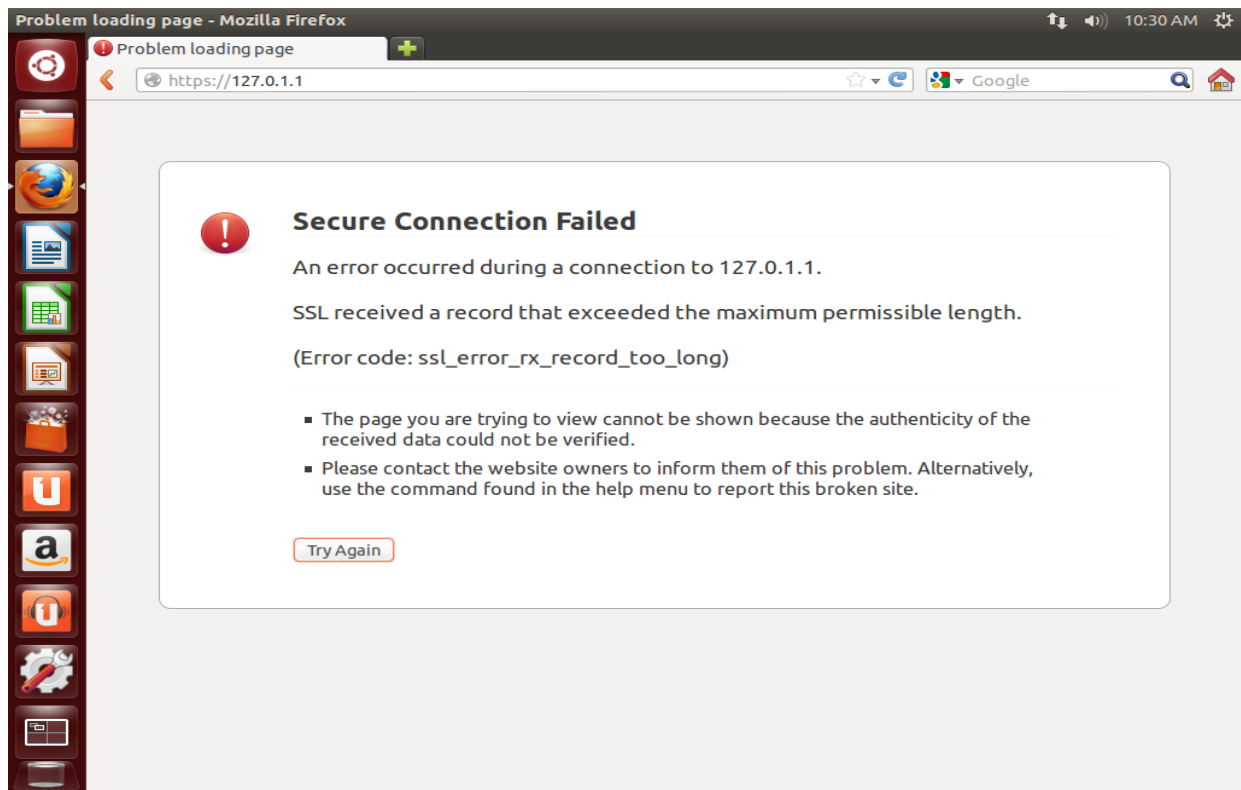
open a website hosted inside apache server



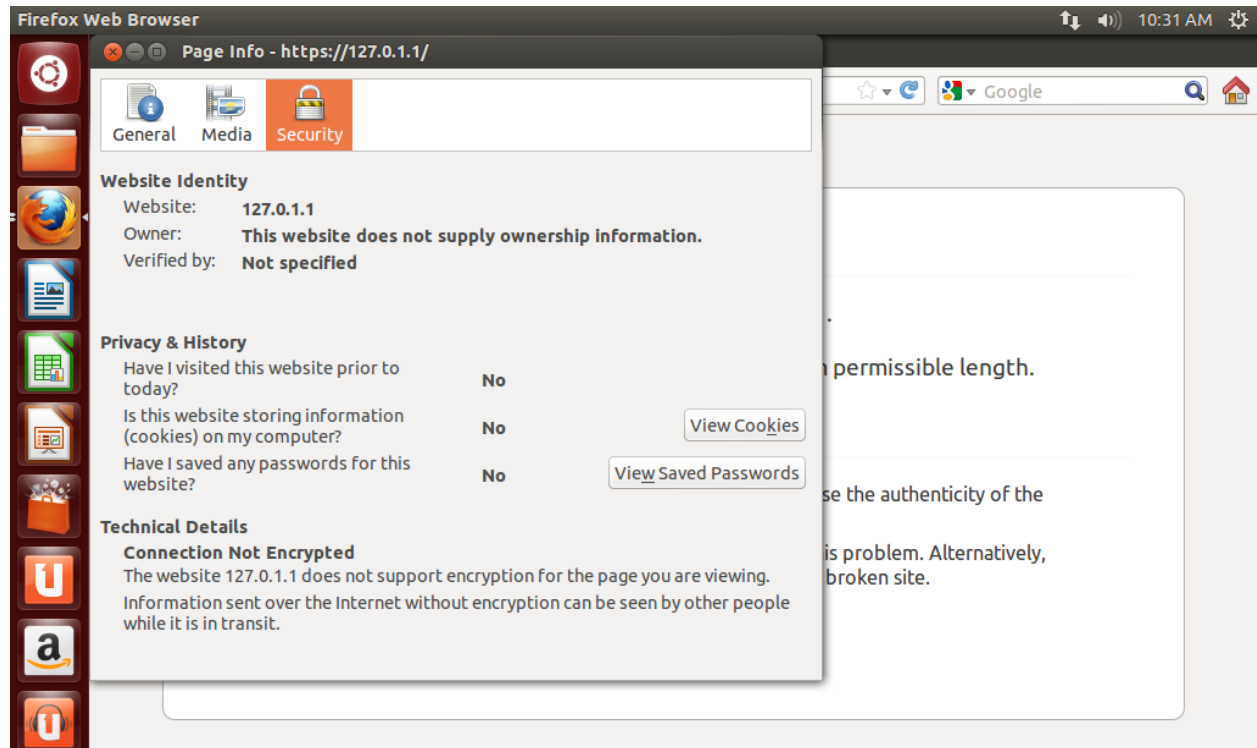
now change the protocol to https in the address bar



Apache server has denied the un-identified https connection



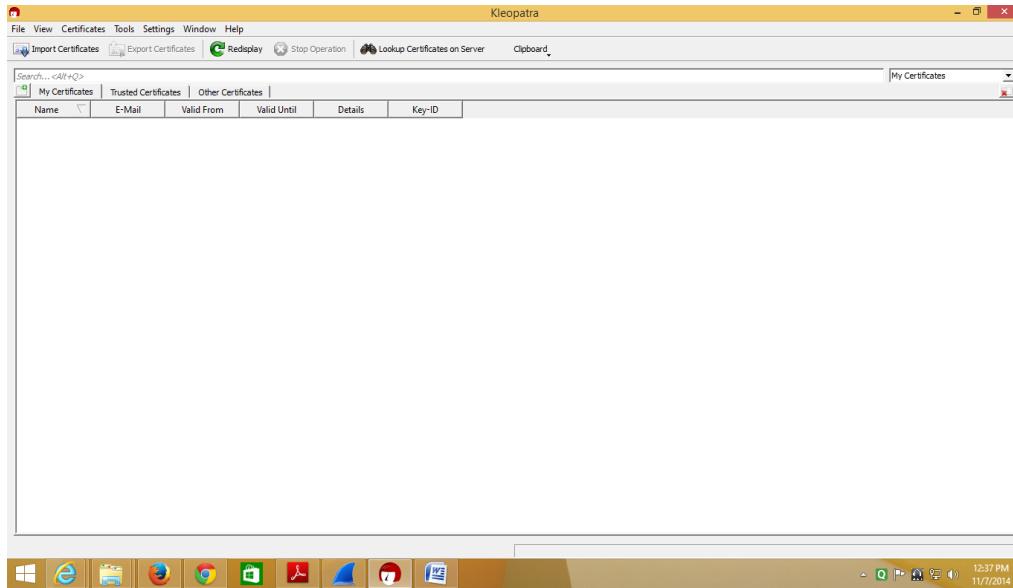
View the connection security details



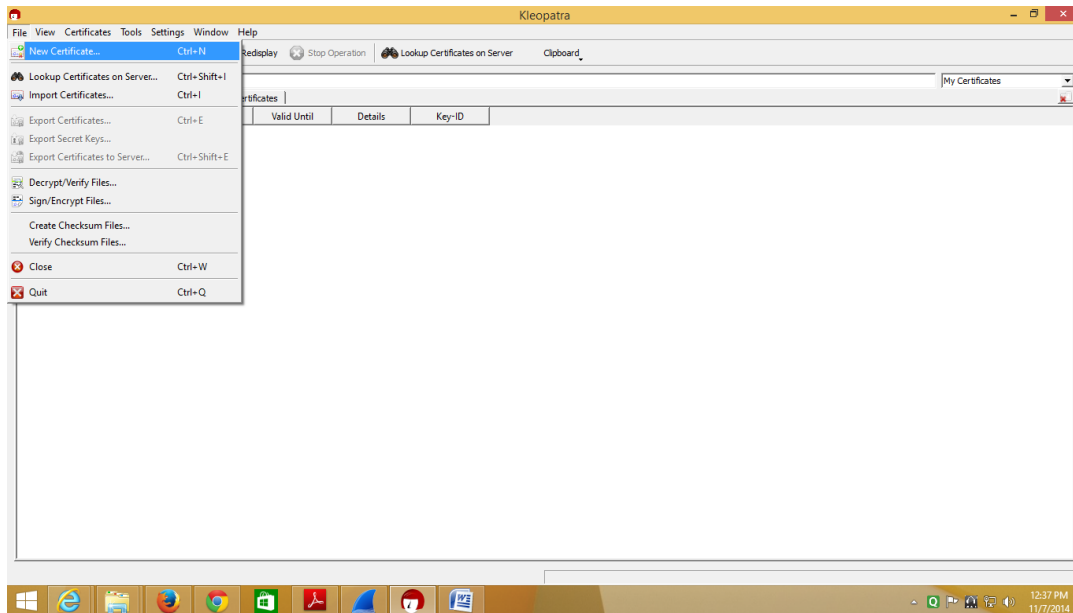
Practical no: 3

Aim : Using GNU PGP

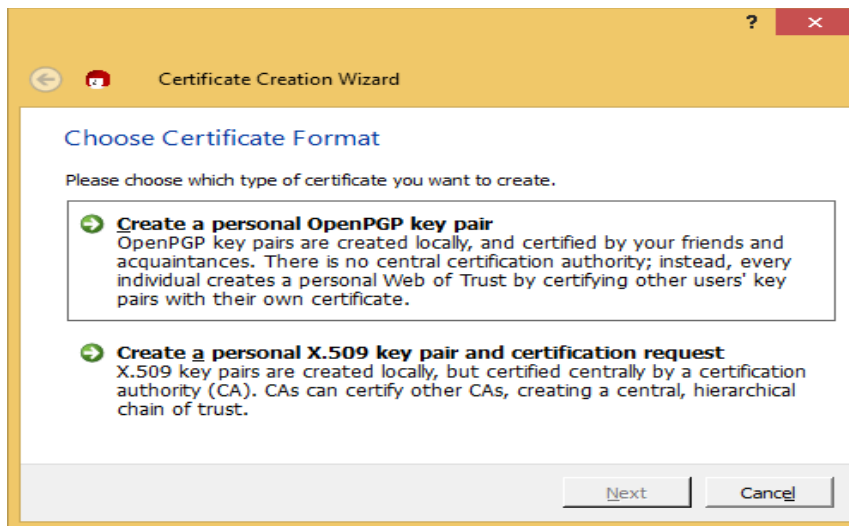
Kleopatra



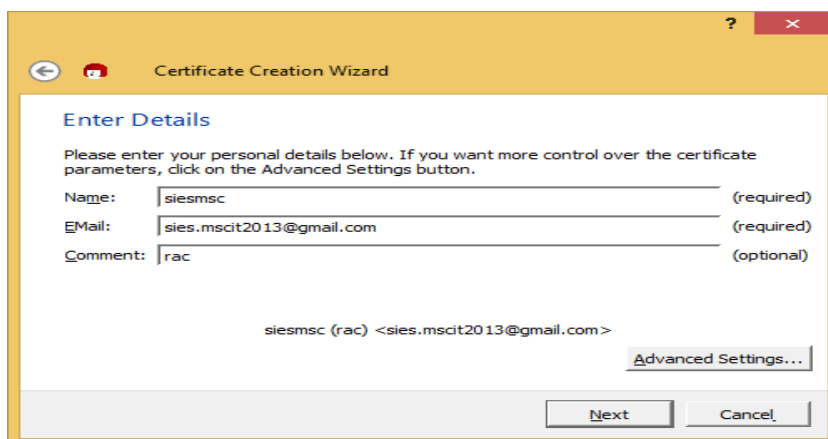
Click on File --> New Certificate or press Ctrl+N



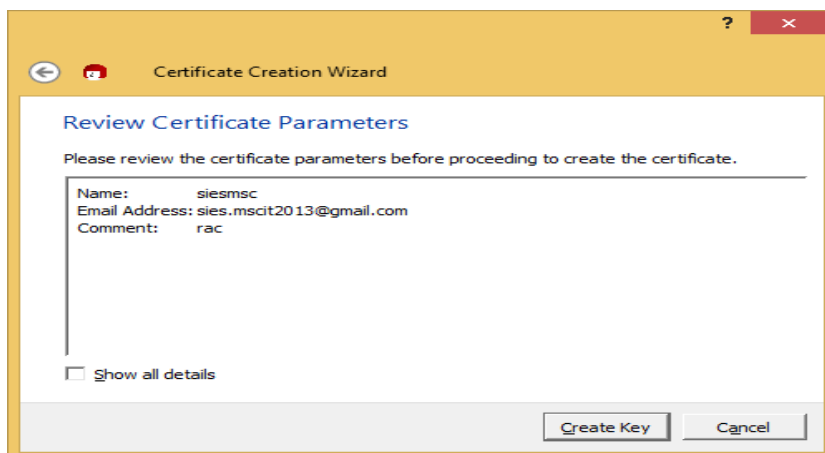
Choose "Create a Personal OpenPGP key Pair" --> Next



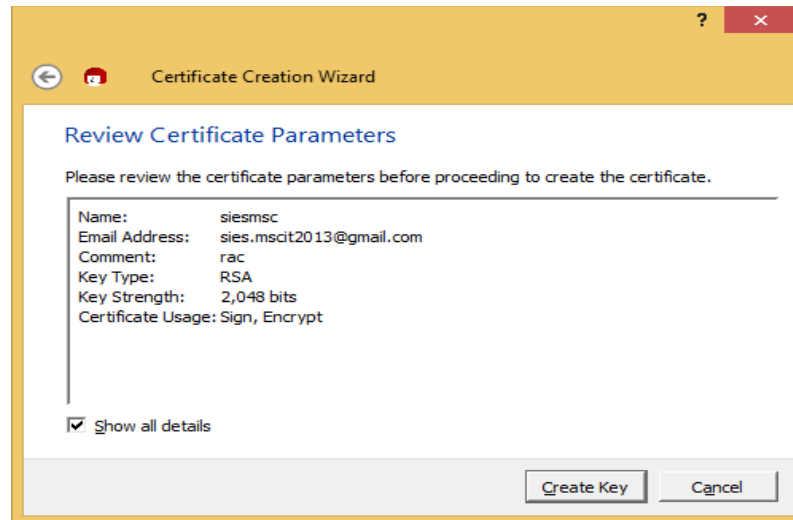
Enter the details Name , Email, Comment --> Next



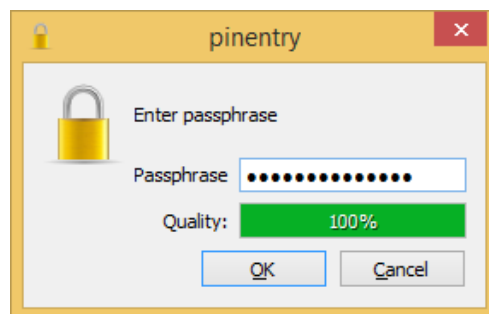
Select Create Key



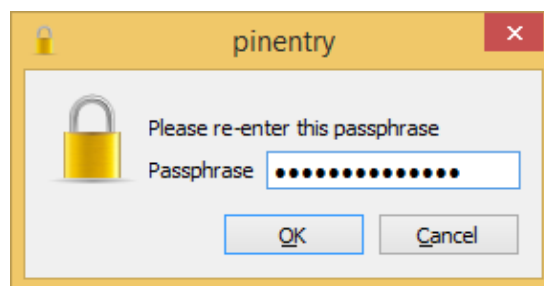
You will see details of your key



Enter Passphrase(password)

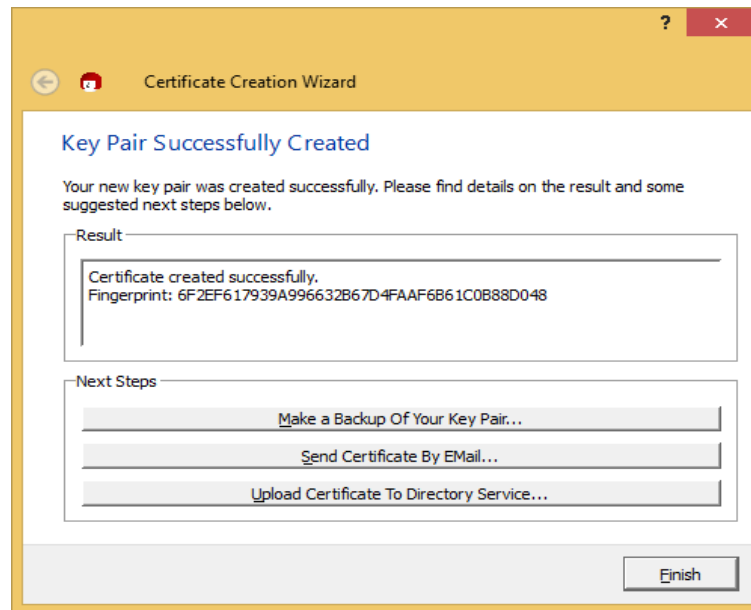


Re-enter the password

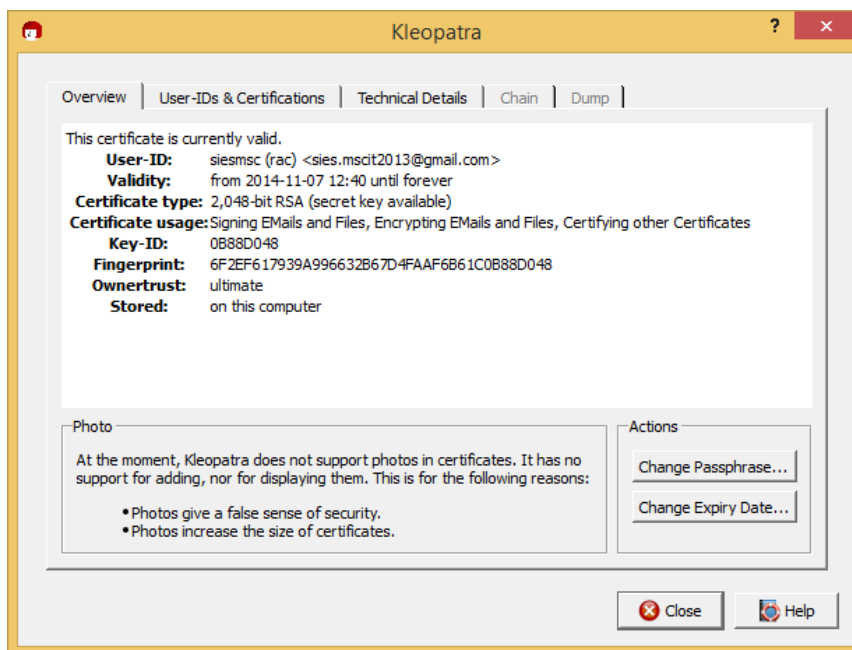


Key Pair Successfully Created

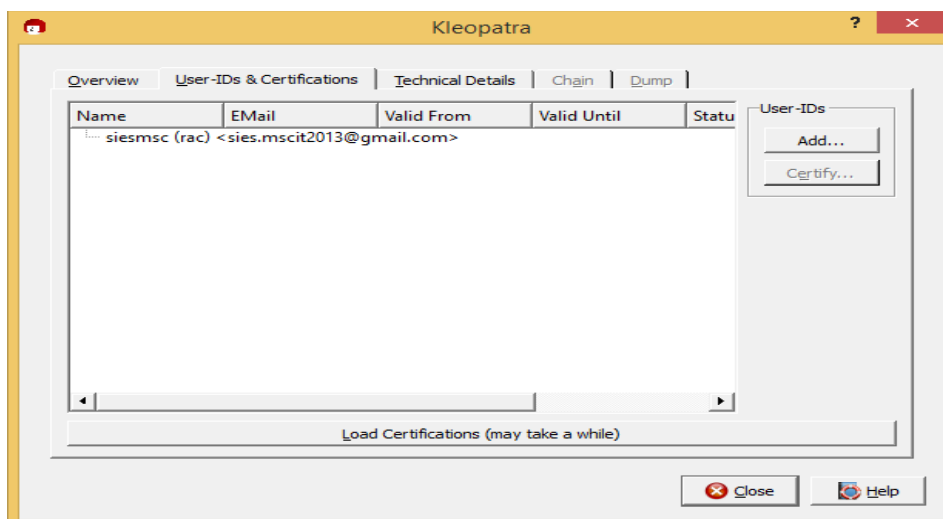
Click Finish



You will see Overview of your Certificate in Overview Tab

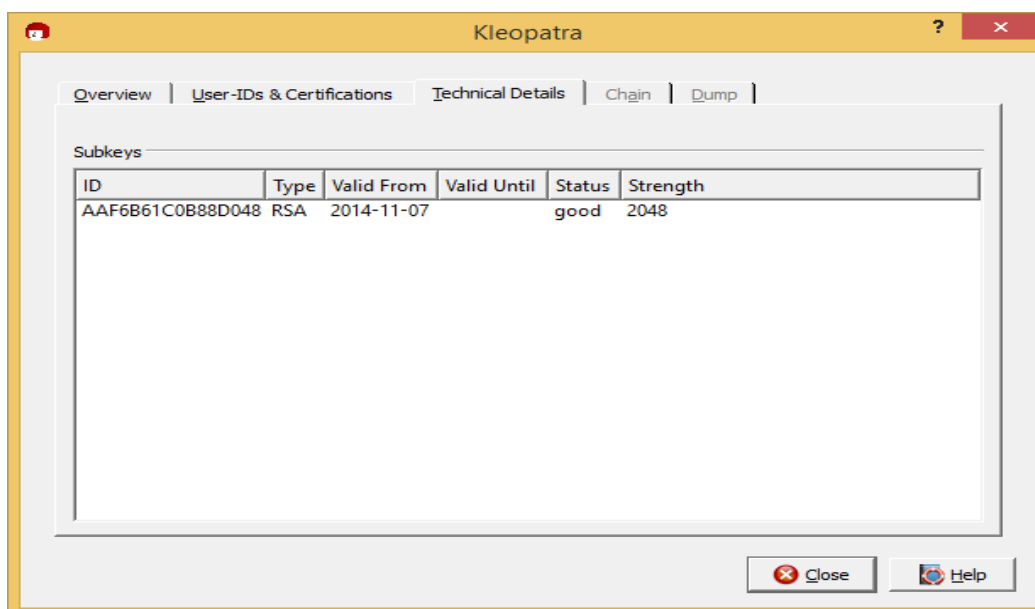


You will see User Id and Certification of your Certificate in User-Ids & Certifications

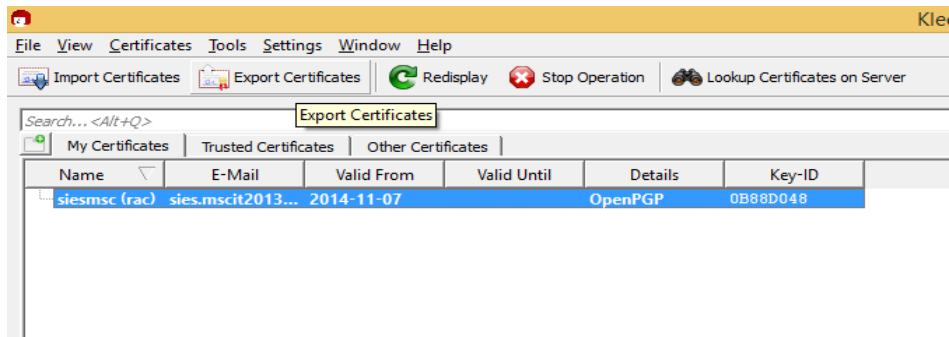


Click on Technical Details to see subkeys Details

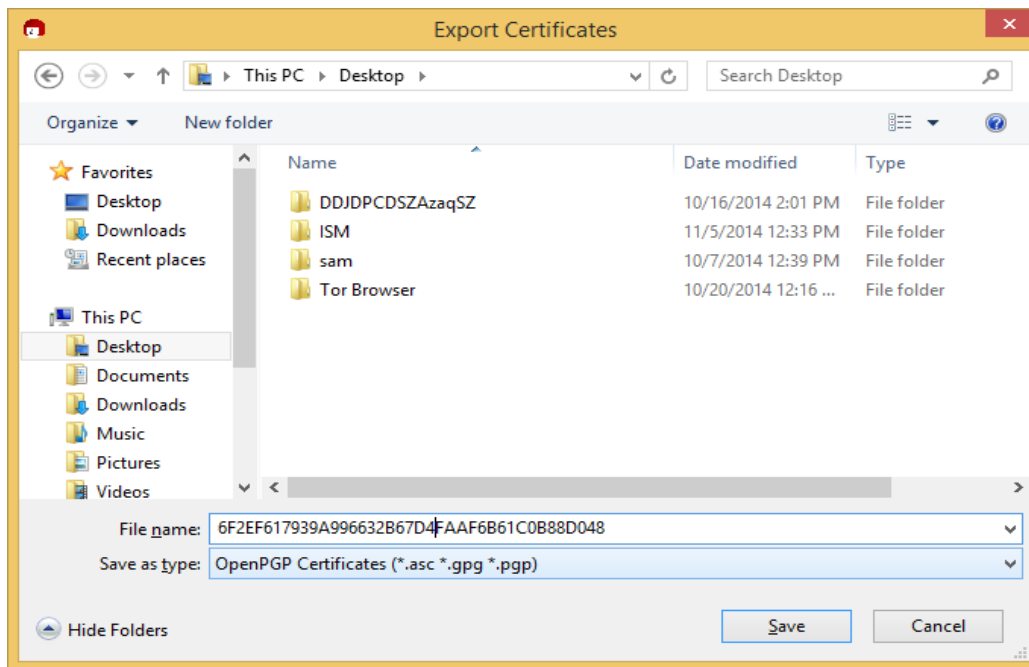
Click on Close



Click on "Export Certificates"



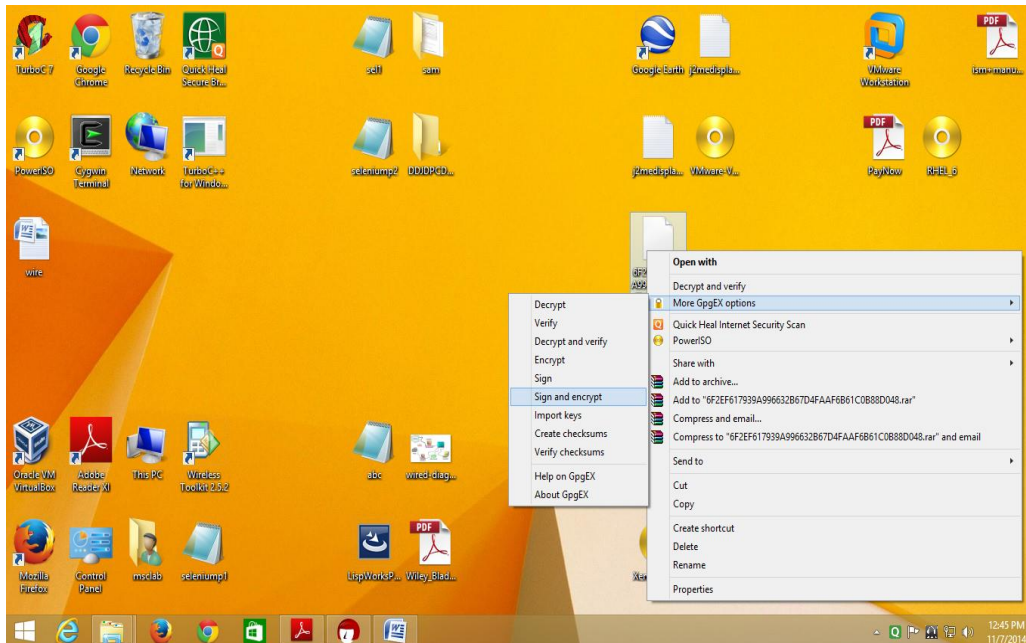
Export the File



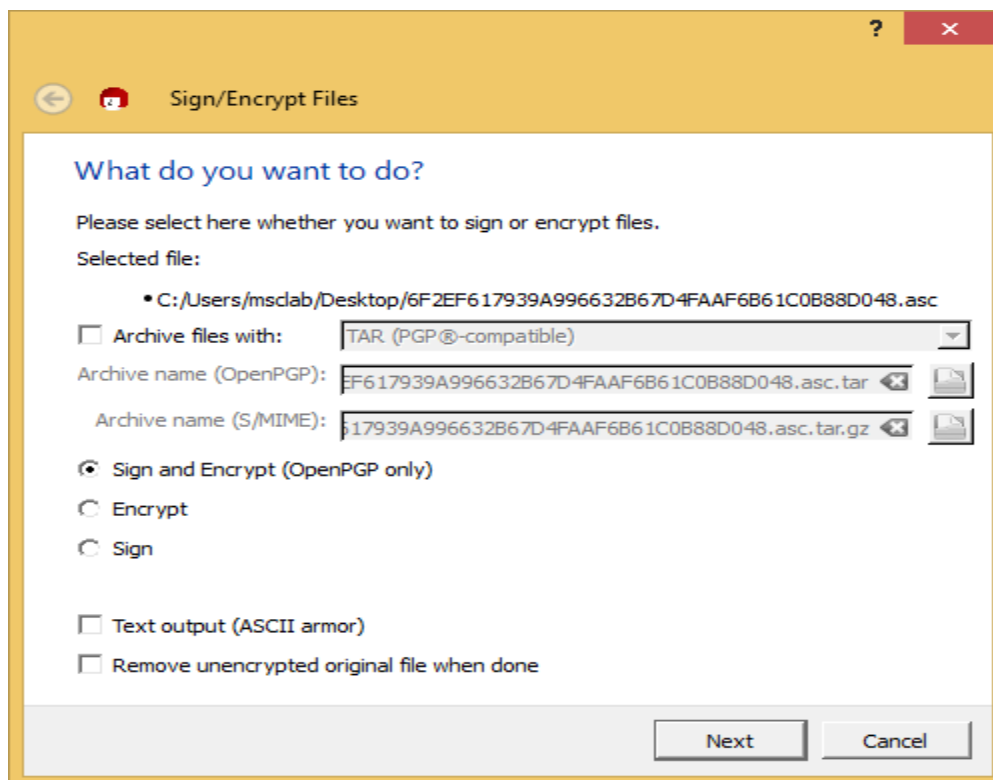
On the Desktop Key Exported

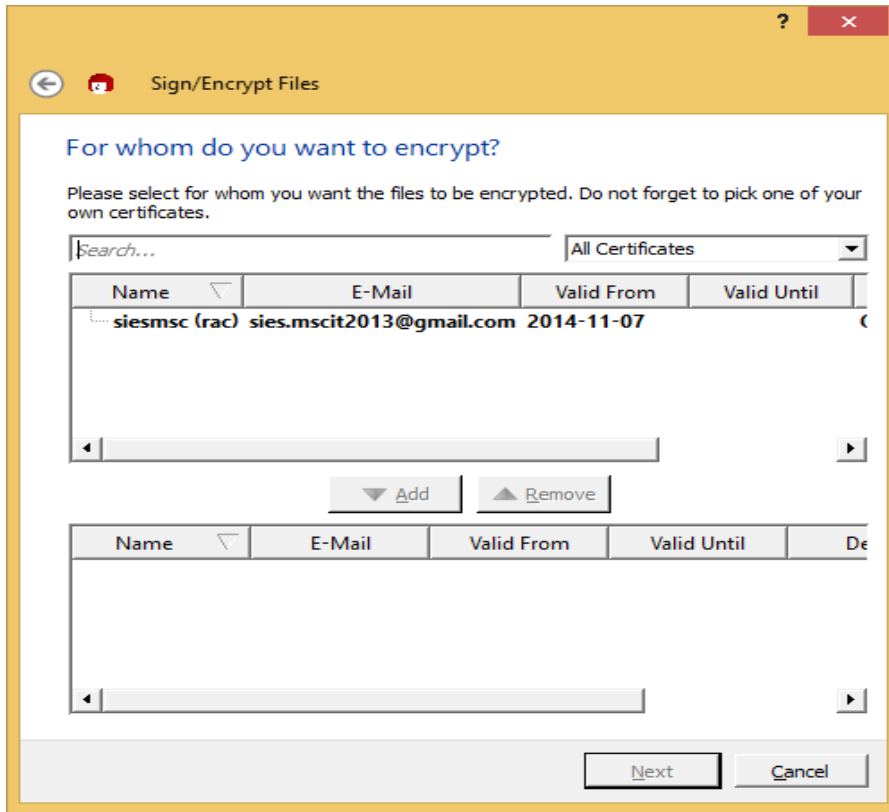


Right Click on Key Go to More GpgEx Options--> Sign and encrypt

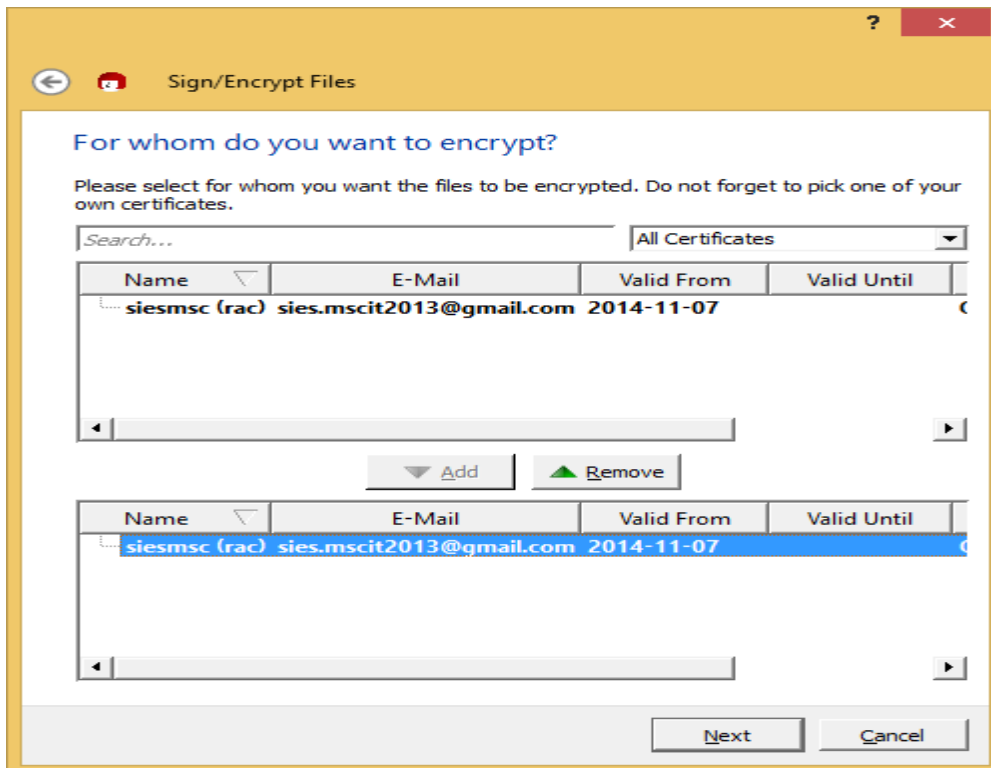


Click Sign & Encrypt(OpenPGP only) radio button --> Next

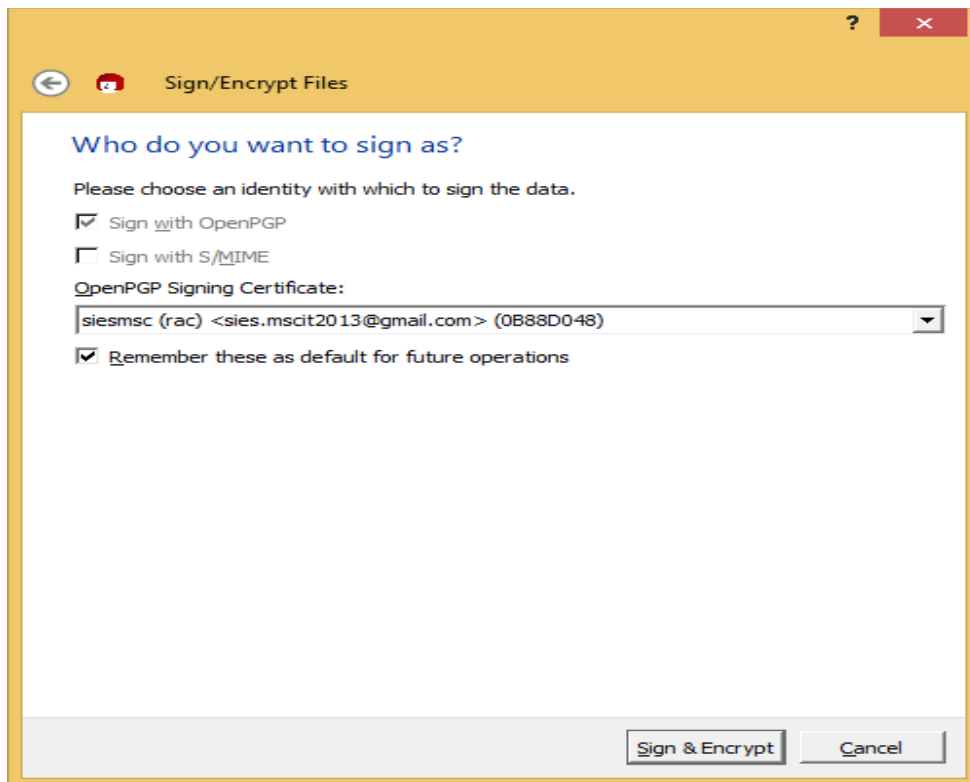




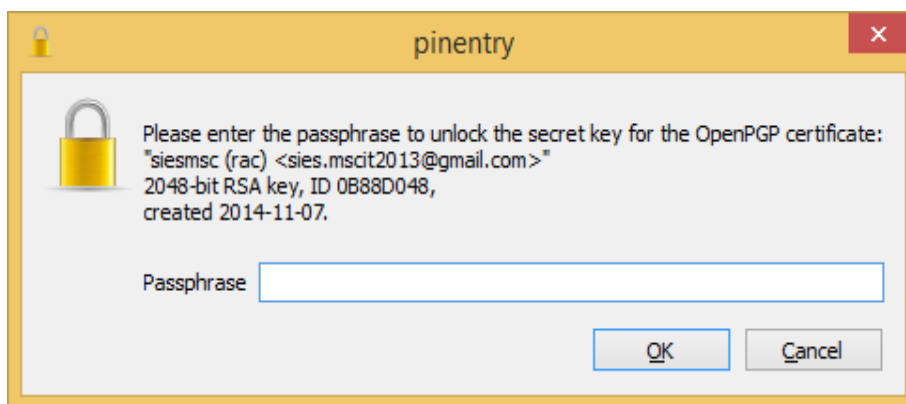
Select file name --> Add --> Next



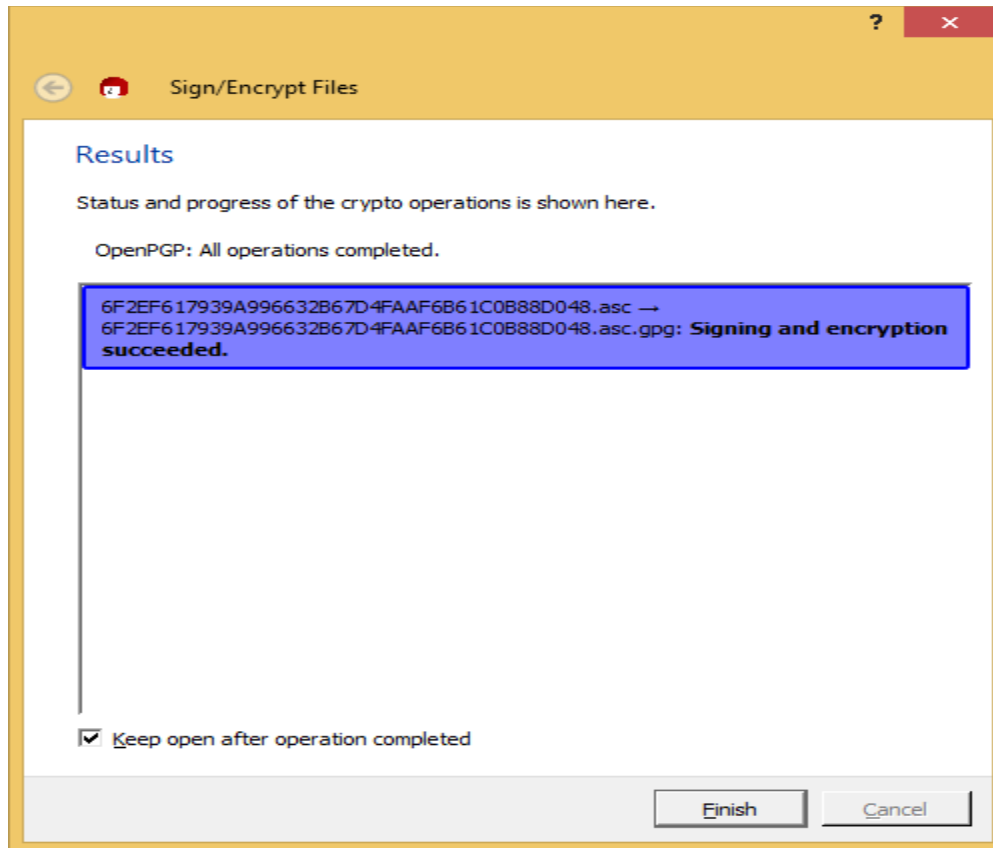
Check "Remember this" --> Sign & Encrypt



Enter Passphrase(Password)

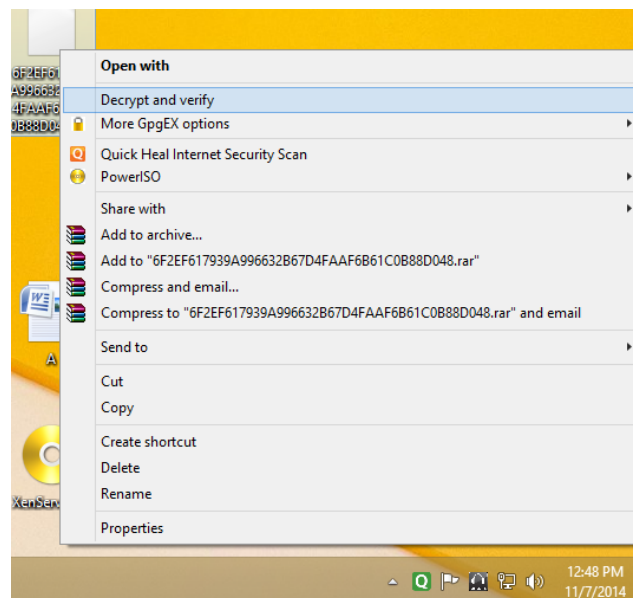


Click Finish

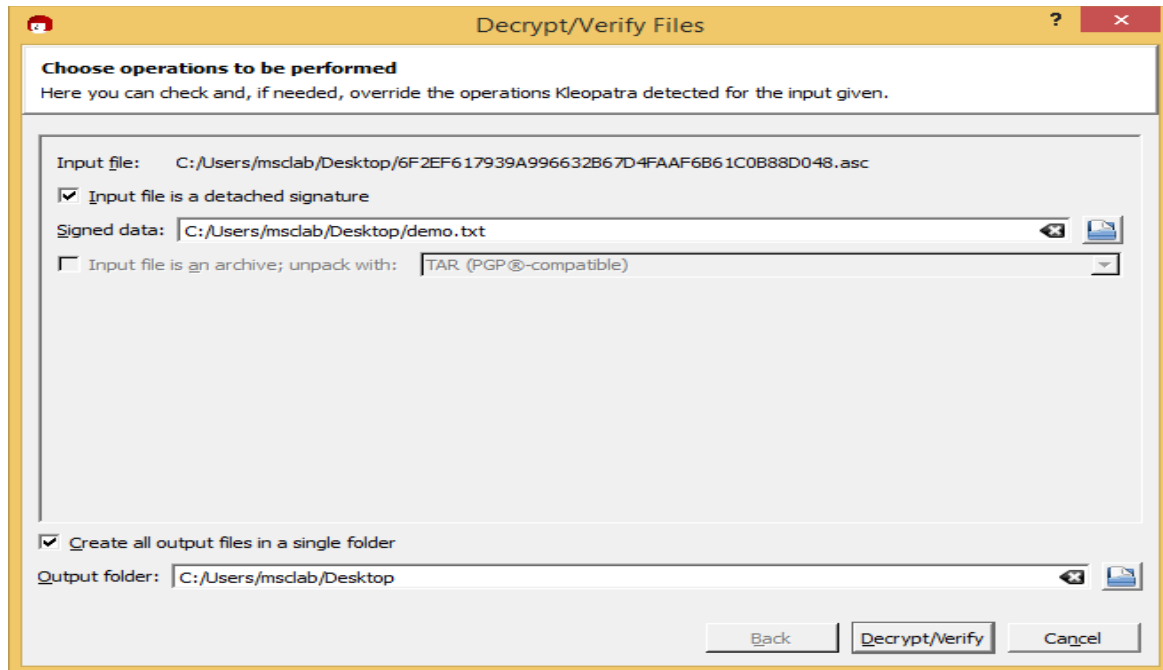


Key will create on Desktop

Right Click on Key-- Decrypt and verify



Select file to decrypt --> Decrypt/verify



Practical no: 4

Aim : Performance evaluation of various cryptographic algorithms

- Install g++ if not already installed
- Install crpto++ if not already installed

Prog.cpp

```
include <iostream>
#include <iomanip>

#include "crypto++/modes.h"
#include "crypto++/aes.h"
#include "crypto++/filters.h"

int main(int argc, char* argv[]) {

    //
    // Key and IV setup
    //
    byte key[ CryptoPP::AES::DEFAULT_KEYLENGTH ], iv[ CryptoPP::AES::BLOCKSIZE ];
    memset( key, 0x00, CryptoPP::AES::DEFAULT_KEYLENGTH );
    memset( iv, 0x00, CryptoPP::AES::BLOCKSIZE );

    //
    // String and Sink setup
    //
    std::string plaintext = "Now is the time for all good men to come to the aide...";
    std::string ciphertext;
    std::string decryptedtext;

    //
    // Dump Plain Text
    //
    std::cout << "Plain Text (" << plaintext.size() << " bytes)" <<std::endl;
    std::cout << plaintext;
    std::cout << std::endl << std::endl;
    //
    // Create Cipher Text
    //
    CryptoPP::AES::Encryption aesEncryption(key,
CryptoPP::AES::DEFAULT_KEYLENGTH);
    CryptoPP::CBC_Mode_ExternalCipher::Encryption cbcEncryption(
aesEncryption, iv );
```

```

    CryptoPP::StreamTransformationFilter          stfEncryptor(cbcEncryption,          new
CryptoPP::StringSink( ciphertext ) );
    stfEncryptor.Put( reinterpret_cast<const unsigned char*>(
plaintext.c_str() ), plaintext.length() + 1 );
    stfEncryptor.MessageEnd();

//
// Dump Cipher Text
//
std::cout << "Cipher Text (" << ciphertext.size() << " bytes)" <<std::endl;

for( int i = 0; i < ciphertext.size(); i++ ) {

    std::cout << "0x" << std::hex << (0xFF & static_cast<byte>(ciphertext[i])) << " ";
}

std::cout << std::endl << std::endl;

//
// Decrypt
//
CryptoPP::AES::Decryption aesDecryption(key,
CryptoPP::AES::DEFAULT_KEYLENGTH);
CryptoPP::CBC_Mode_ExternalCipher::Decryption cbcDecryption(
aesDecryption, iv );

    CryptoPP::StreamTransformationFilter          stfDecryptor(cbcDecryption,          new
CryptoPP::StringSink( decryptedtext ) );
    stfDecryptor.Put( reinterpret_cast<const unsigned char*>(
ciphertext.c_str() ), ciphertext.size() );
    stfDecryptor.MessageEnd();

//
// Dump Decrypted Text
//
std::cout << "Decrypted Text: " << std::endl;
std::cout << decryptedtext;
std::cout << std::endl << std::endl;

return 0;
}

```


To compile use the following command:

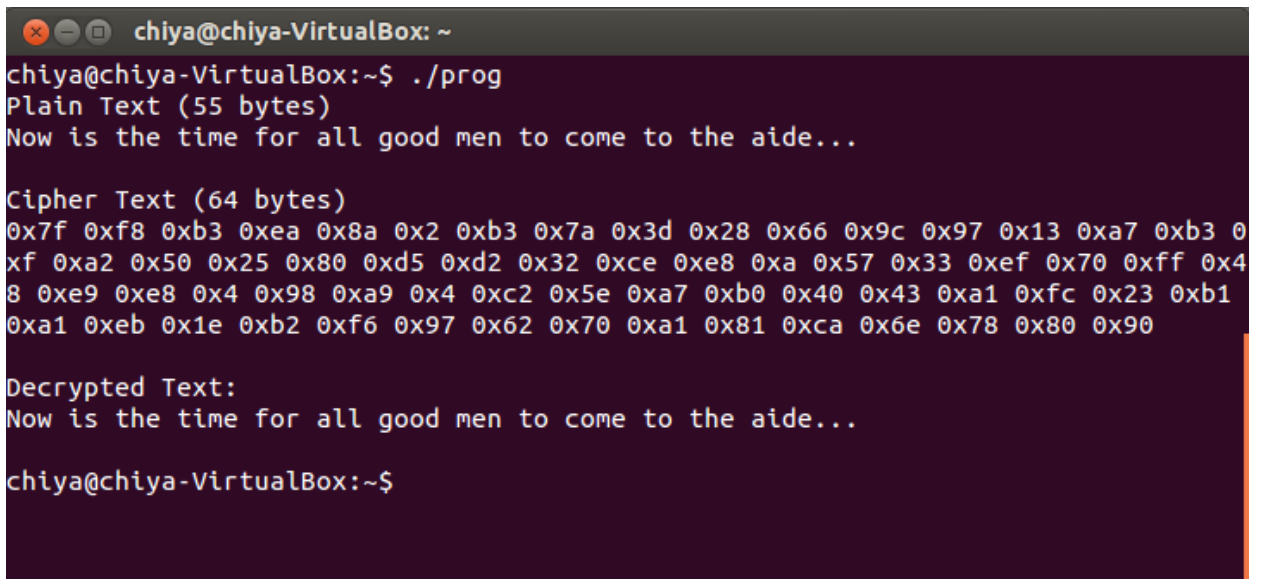
```
g++ -g3 -ggdb -o0 -Wall -Wextra -unused -o AesOutput aesexample.cpp -lcryptopp
```



```
chiya@chiya-VirtualBox: ~
chiya@chiya-VirtualBox:~$ g++ -g3 -ggdb -o0 -Wall -Wextra -unused -o prog prog.cpp -lcryptopp
prog.cpp: In function 'int main(int, char**)':
prog.cpp:48:41: warning: comparison between signed and unsigned integer expressions [-Wsign-compare]
prog.cpp: At global scope:
prog.cpp:8:5: warning: unused parameter 'argc' [-Wunused-parameter]
prog.cpp:8:5: warning: unused parameter 'argv' [-Wunused-parameter]
chiya@chiya-VirtualBox:~$ dir
code.cpp~ Downloads Pictures prog.cpp~ server.key Videos
Desktop examples.desktop prog Public server.key.secure
Documents Music prog.cpp server.crt Templates
chiya@chiya-VirtualBox:~$
```

To execute use the following command

```
./prog
```



```
chiya@chiya-VirtualBox: ~
chiya@chiya-VirtualBox:~$ ./prog
Plain Text (55 bytes)
Now is the time for all good men to come to the aide...

Cipher Text (64 bytes)
0x7f 0xf8 0xb3 0xea 0x8a 0x2 0xb3 0x7a 0x3d 0x28 0x66 0x9c 0x97 0x13 0xa7 0xb3 0
xf 0xa2 0x50 0x25 0x80 0xd5 0xd2 0x32 0xce 0xe8 0xa 0x57 0x33 0xef 0x70 0xff 0x4
8 0xe9 0xe8 0x4 0x98 0xa9 0x4 0xc2 0x5e 0xa7 0xb0 0x40 0x43 0xa1 0xfc 0x23 0xb1
0xa1 0xeb 0x1e 0xb2 0xf6 0x97 0x62 0x70 0xa1 0x81 0xca 0x6e 0x78 0x80 0x90

Decrypted Text:
Now is the time for all good men to come to the aide...

chiya@chiya-VirtualBox:~$
```

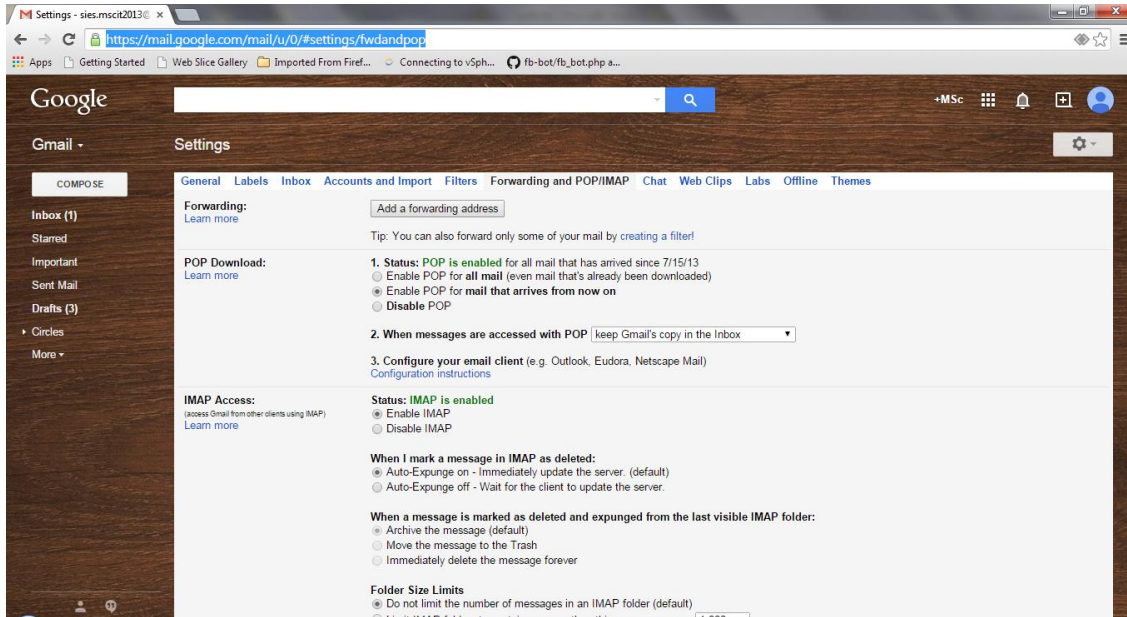
Practical No: 5

Aim : Configuring S/MIME for e-mail communication

Some settings to you gmail account

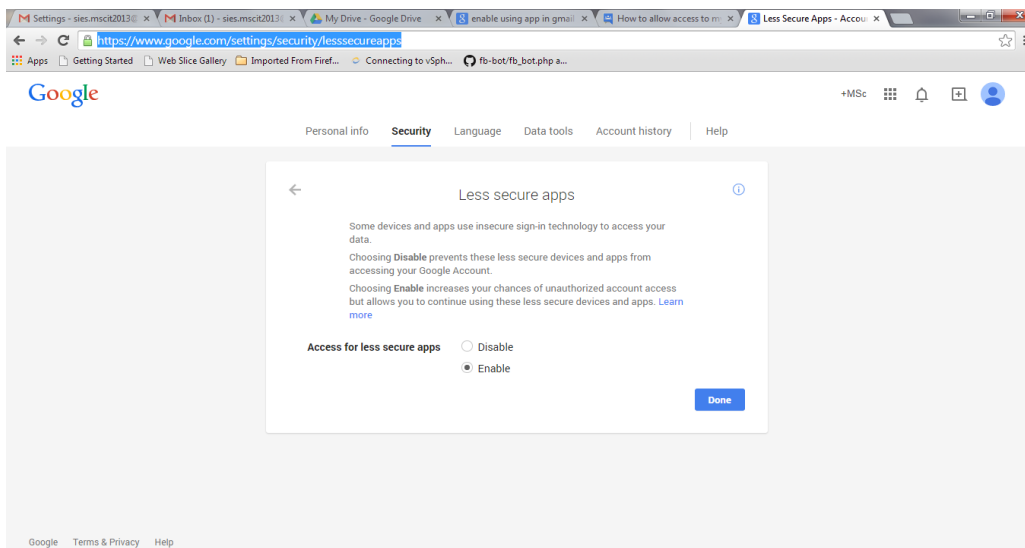
<https://mail.google.com/mail/u/0/#settings/fwdandpop>

➤ Enable pop

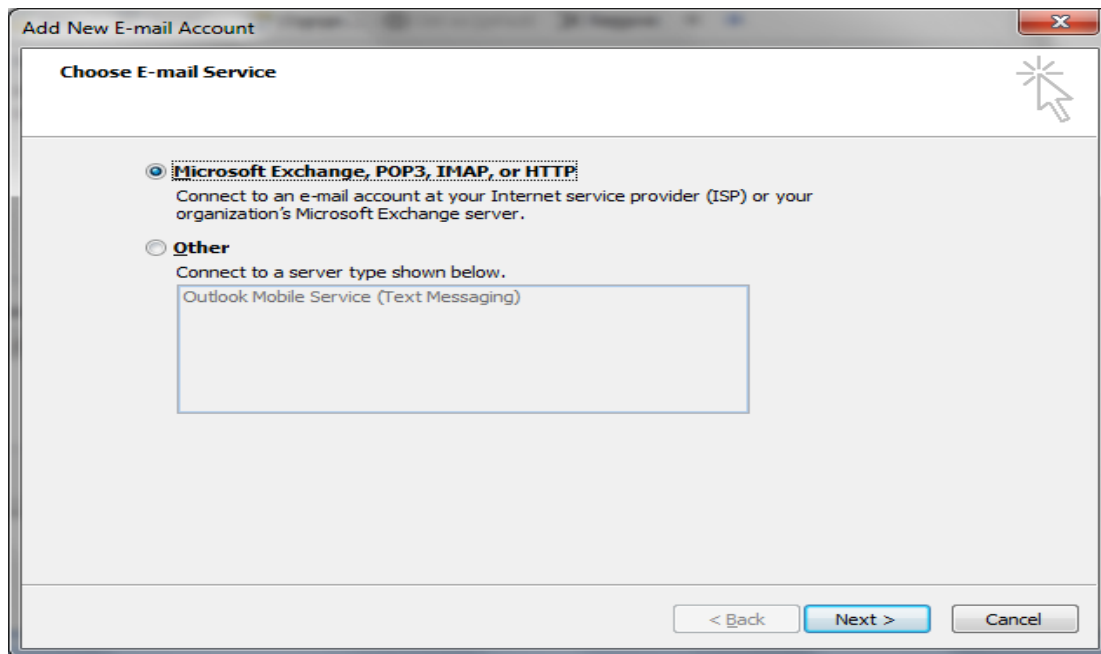


➤ Enable app settings

<https://www.google.com/settings/security/lesssecureapps>



Configure MS outlook by providing the required credentials



The screenshot shows the 'Add New E-mail Account' dialog box with the 'Choose E-mail Service' step. The 'Microsoft Exchange, POP3, IMAP, or HTTP' option is selected. Below it, there is a description: 'Connect to an e-mail account at your Internet service provider (ISP) or your organization's Microsoft Exchange server.' The 'Other' option is also visible, with a description: 'Connect to a server type shown below.' Below the 'Other' description, there is a text box containing 'Outlook Mobile Service (Text Messaging)'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

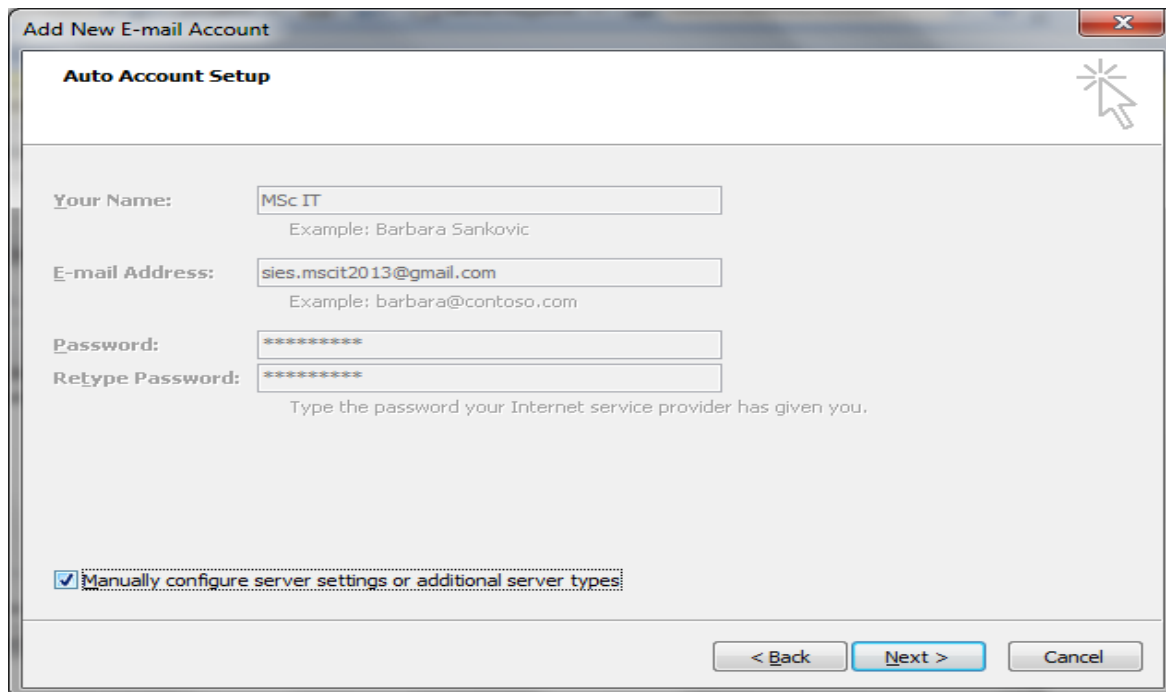
Add New E-mail Account

Choose E-mail Service

Microsoft Exchange, POP3, IMAP, or HTTP
Connect to an e-mail account at your Internet service provider (ISP) or your organization's Microsoft Exchange server.

Other
Connect to a server type shown below.
Outlook Mobile Service (Text Messaging)

< Back Next > Cancel



The screenshot shows the 'Add New E-mail Account' dialog box with the 'Auto Account Setup' step. It contains four input fields: 'Your Name' (with 'MSc IT' entered), 'E-mail Address' (with 'sies.msct2013@gmail.com' entered), 'Password' (with '*****' entered), and 'Retype Password' (with '*****' entered). Below the input fields, there is a checkbox labeled 'Manually configure server settings or additional server types' which is checked. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Add New E-mail Account

Auto Account Setup

Your Name: MSc IT
Example: Barbara Sankovic

E-mail Address: sies.msct2013@gmail.com
Example: barbara@contoso.com

Password: *****

Retype Password: *****
Type the password your Internet service provider has given you.

Manually configure server settings or additional server types

< Back Next > Cancel

Add New E-mail Account

Choose E-mail Service

Internet E-mail
Connect to your POP, IMAP, or HTTP server to send and receive e-mail messages.

Microsoft Exchange
Connect to Microsoft Exchange for access to your e-mail, calendar, contacts, faxes and voice mail.

Other
Connect to a server type shown below.
Outlook Mobile Service (Text Messaging)

< Back Next > Cancel

Add New E-mail Account

Internet E-mail Settings

Each of these settings are required to get your e-mail account working.

User Information

Your Name:

E-mail Address:

Server Information

Account Type:

Incoming mail server:

Outgoing mail server (SMTP):

Logon Information

User Name:

Password:

Remember password

Require logon using Secure Password Authentication (SPA)

Test Account Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

< Back Next > Cancel

More settings

The screenshot shows the 'Internet E-mail Settings' dialog box with the 'General' tab selected. The 'Mail Account' field contains 'sies.msct2013@gmail.com'. The 'Other User Information' section has empty fields for 'Organization' and 'Reply E-mail'. The 'OK' and 'Cancel' buttons are at the bottom.

Internet E-mail Settings

General | Outgoing Server | Connection | Advanced

Mail Account

Type the name by which you want to refer to this account. For example: "Work" or "Microsoft Mail Server"

sies.msct2013@gmail.com

Other User Information

Organization:

Reply E-mail:

OK Cancel

The screenshot shows the 'Internet E-mail Settings' dialog box with the 'Outgoing Server' tab selected. The 'Incoming server (POP3)' is set to 995 with a 'Use Defaults' button. The 'Outgoing server (SMTP)' is set to 465. The 'Use the following type of encrypted connection' dropdown is set to 'SSL'. The 'Server Timeouts' section shows 'Short' and 'Long 1 minute' options. The 'Delivery' section has checkboxes for 'Leave a copy of messages on the server', 'Remove from server after 10 days', and 'Remove from server when deleted from 'Deleted Items''. The 'OK' and 'Cancel' buttons are at the bottom.

Internet E-mail Settings

General | Outgoing Server | Connection | Advanced

Server Port Numbers

Incoming server (POP3): 995 Use Defaults

This server requires an encrypted connection (SSL)

Outgoing server (SMTP): 465

Use the following type of encrypted connection: SSL

Server Timeouts

Short Long 1 minute

Delivery

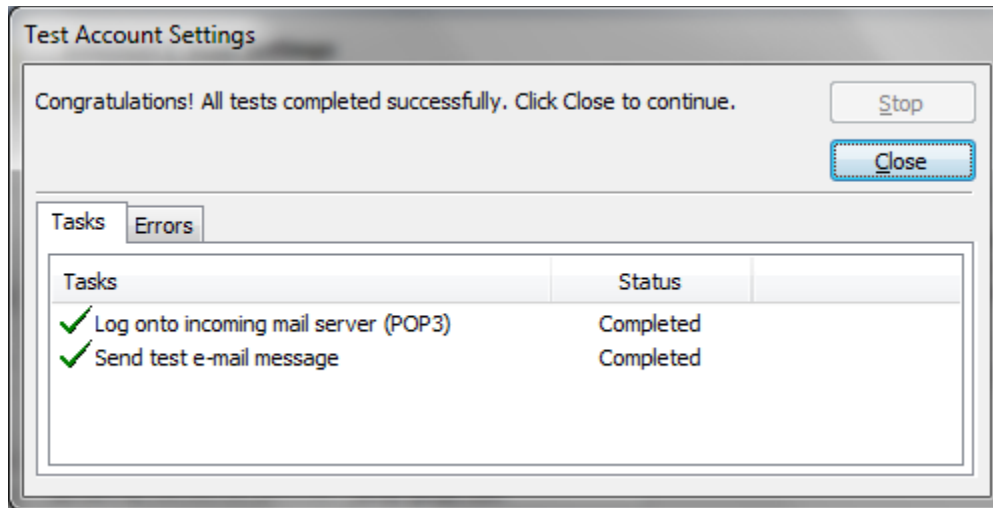
Leave a copy of messages on the server

Remove from server after 10 days

Remove from server when deleted from 'Deleted Items'

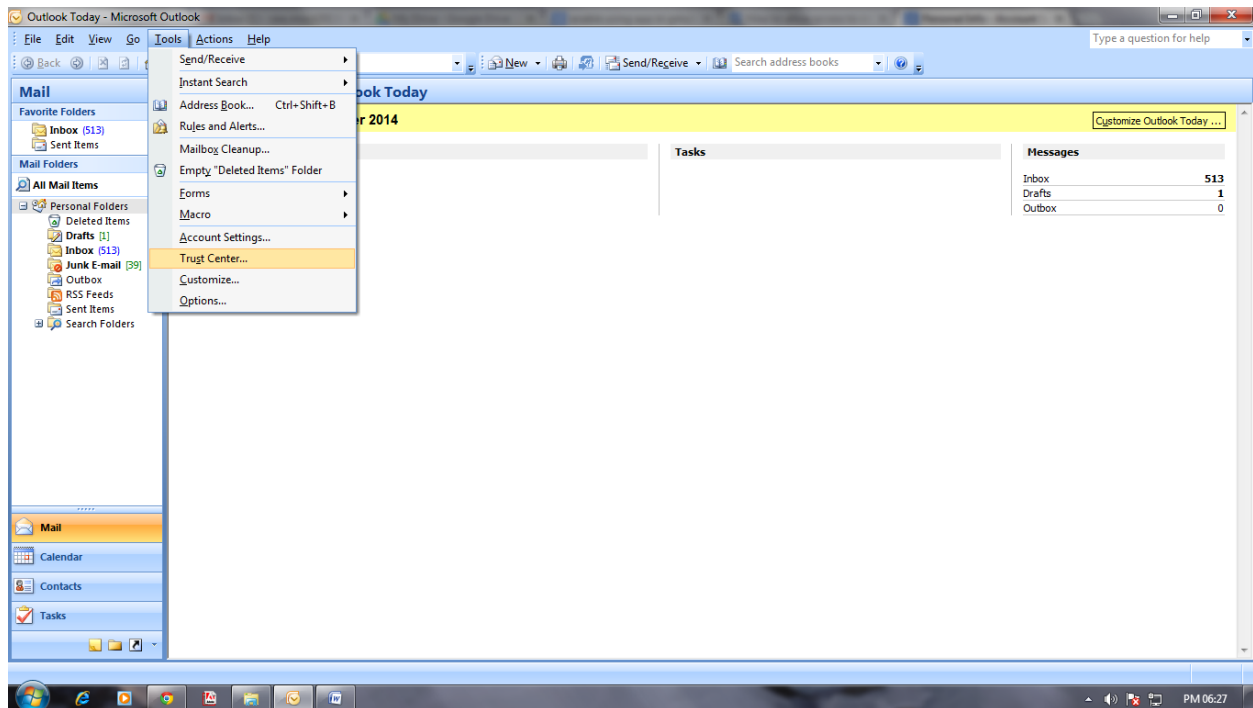
OK Cancel

Test account settings

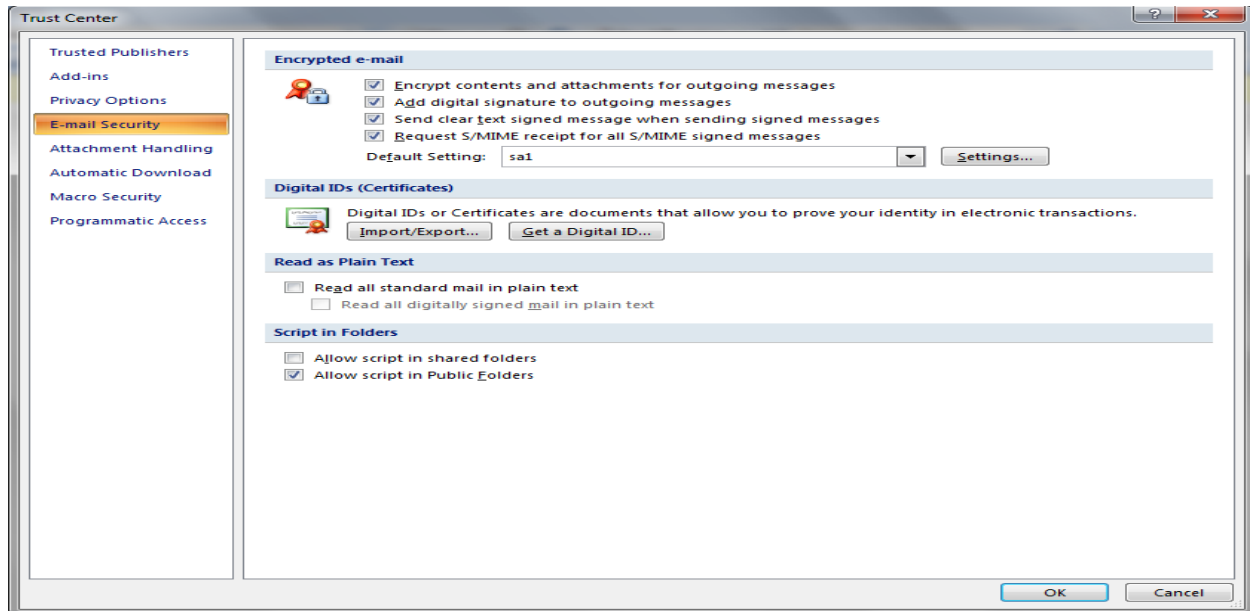


- Click Next
- Click Finish.

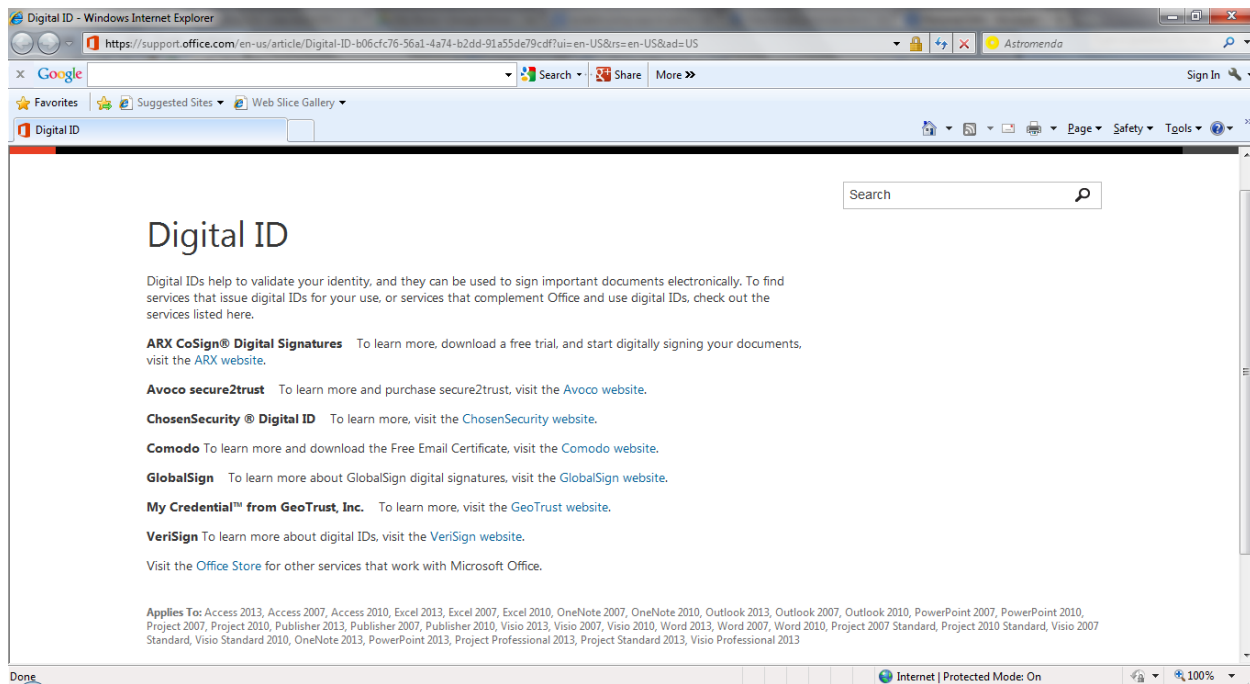
Open Trust Center



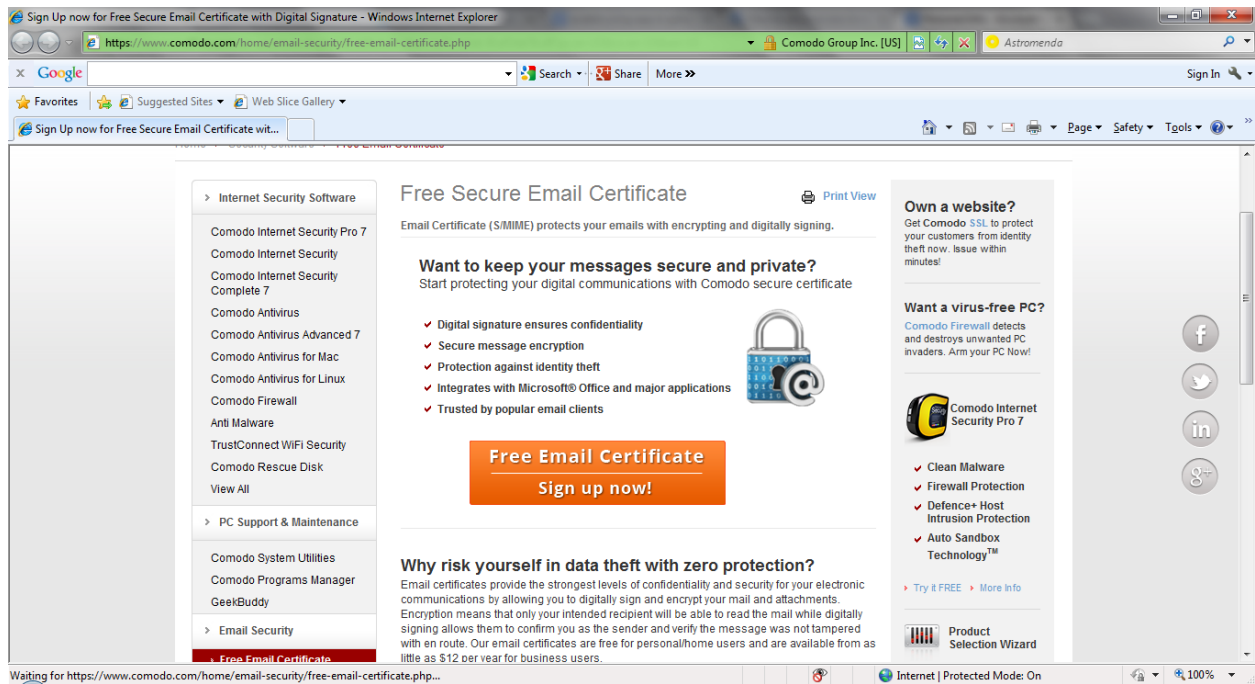
Click on Get a Digital ID.



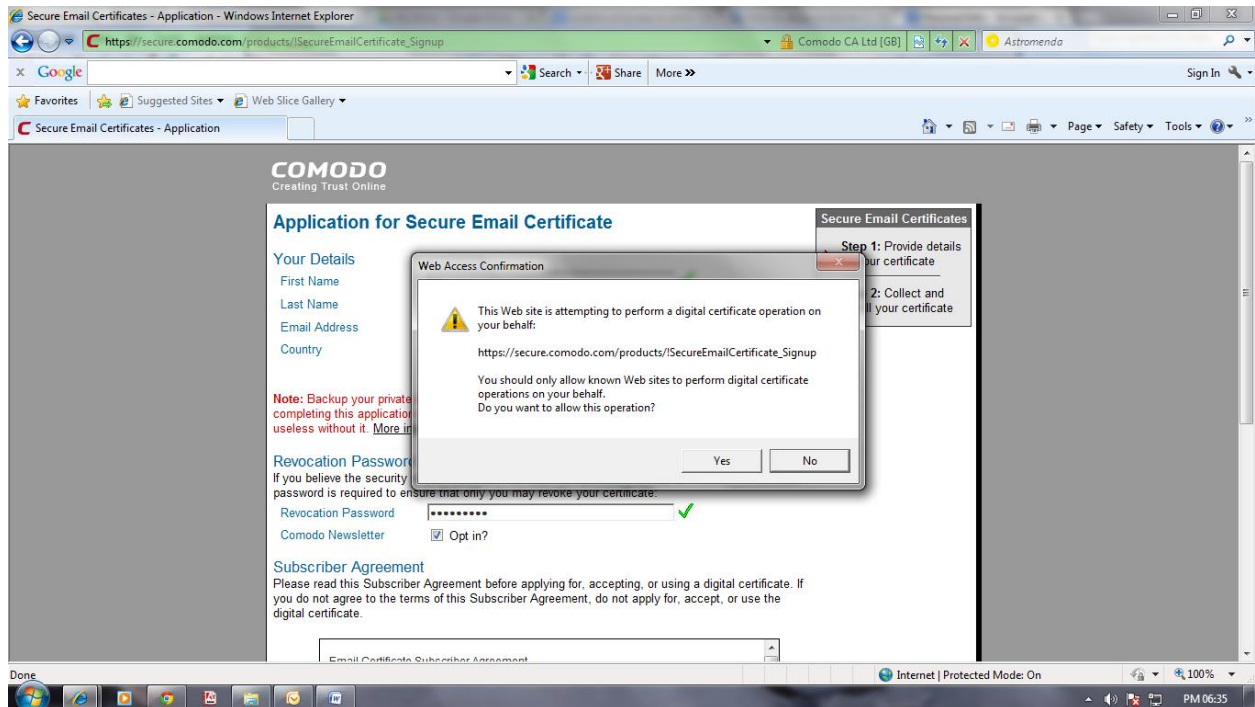
Open Comodo website



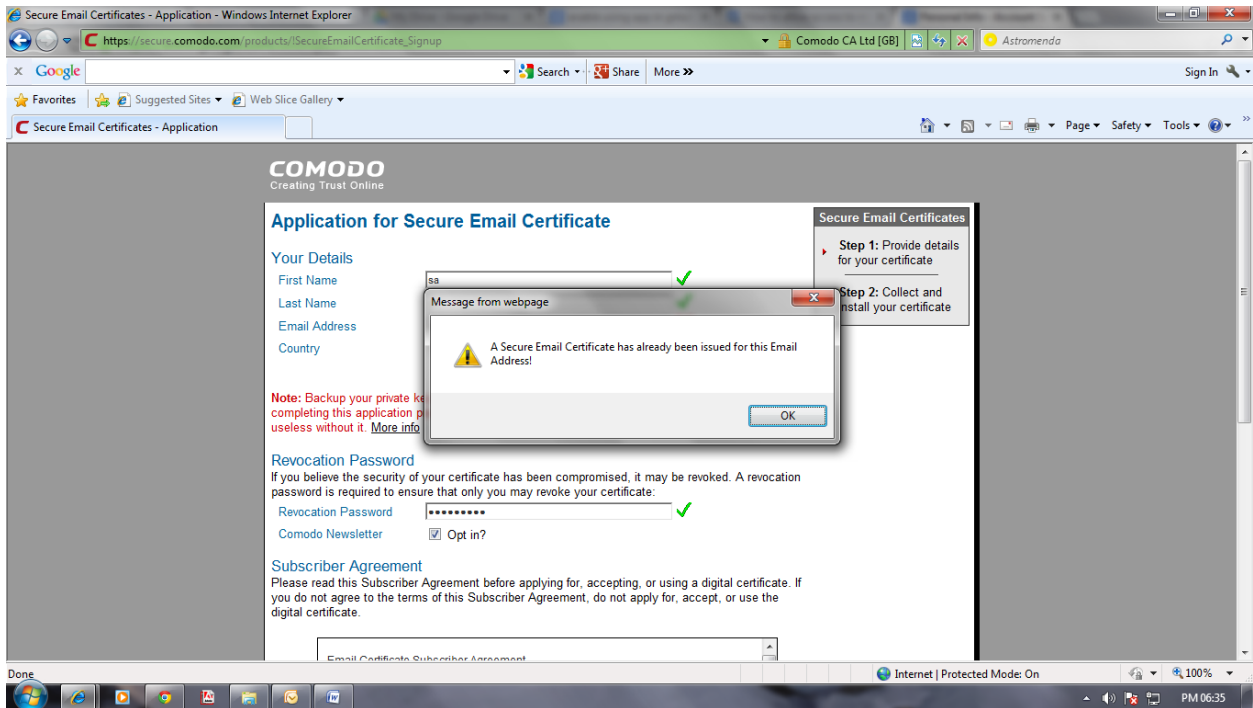
Click on Free Email certificate



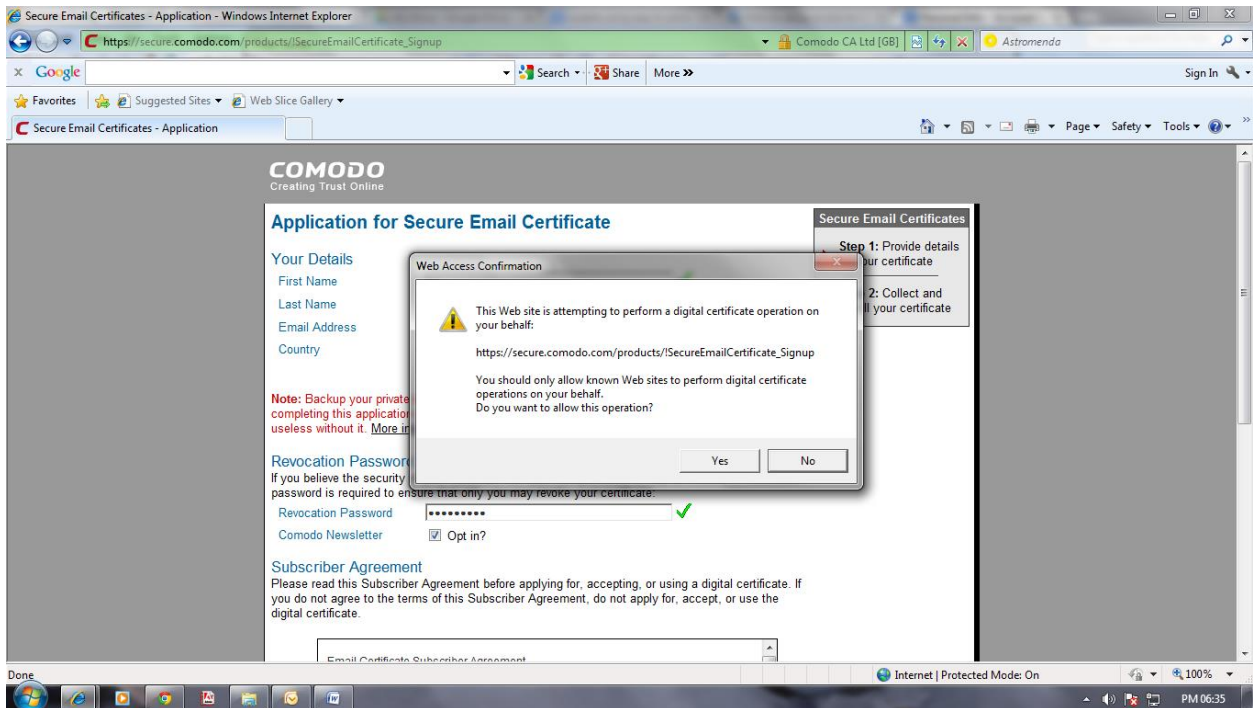
And click "Yes" if Pop up occurs

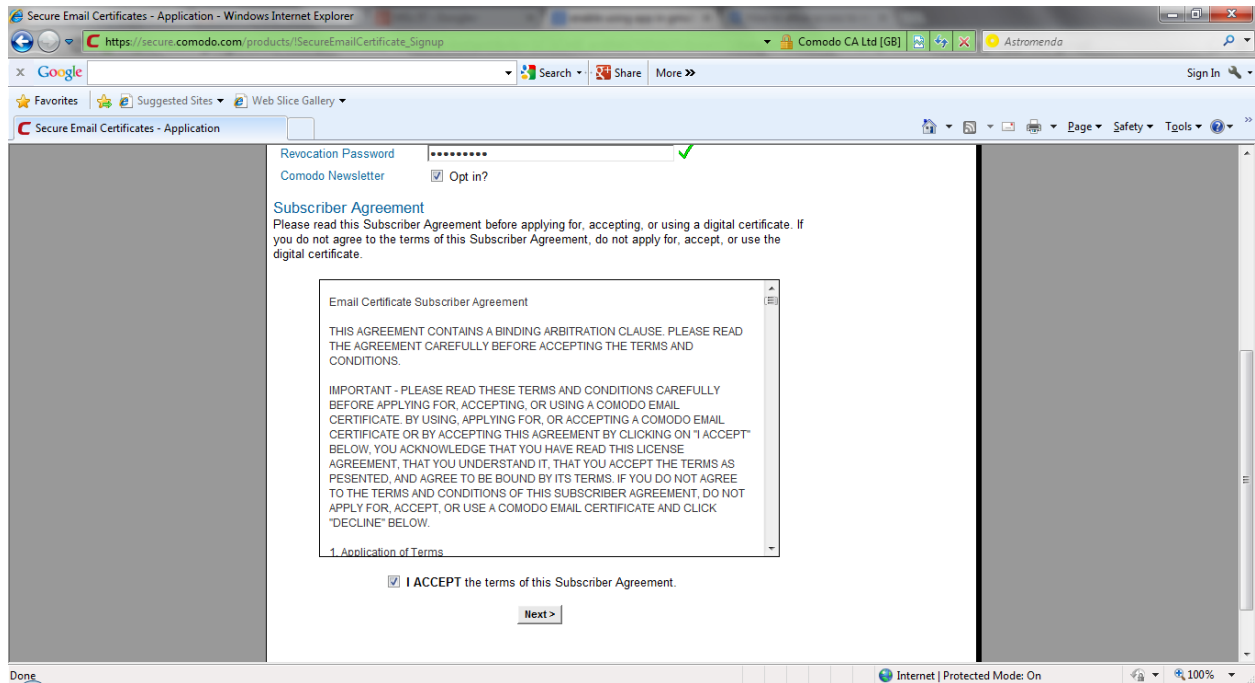


Klik on Ok

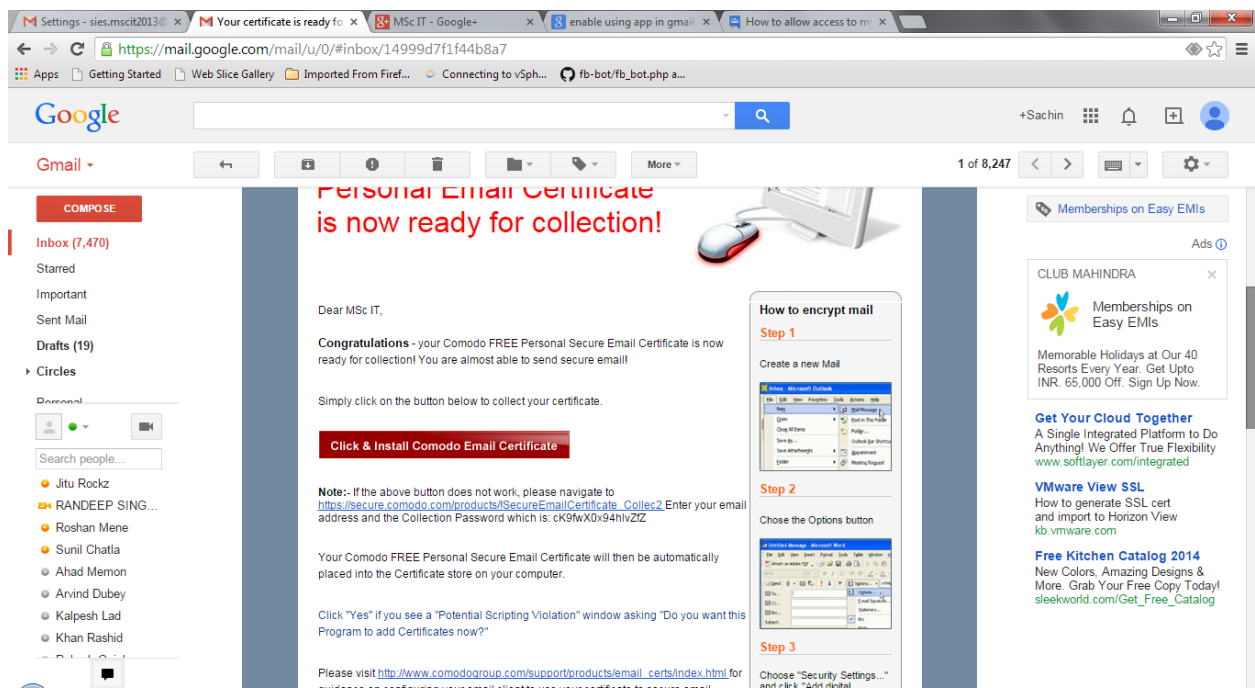


And click "Yes" if Pop up occurs

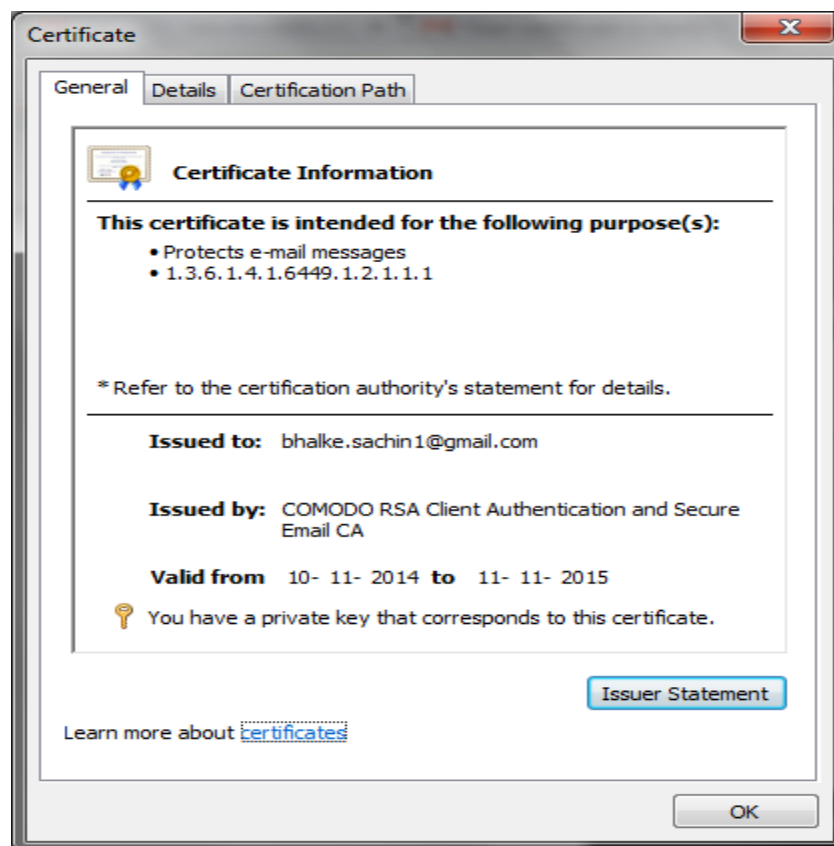
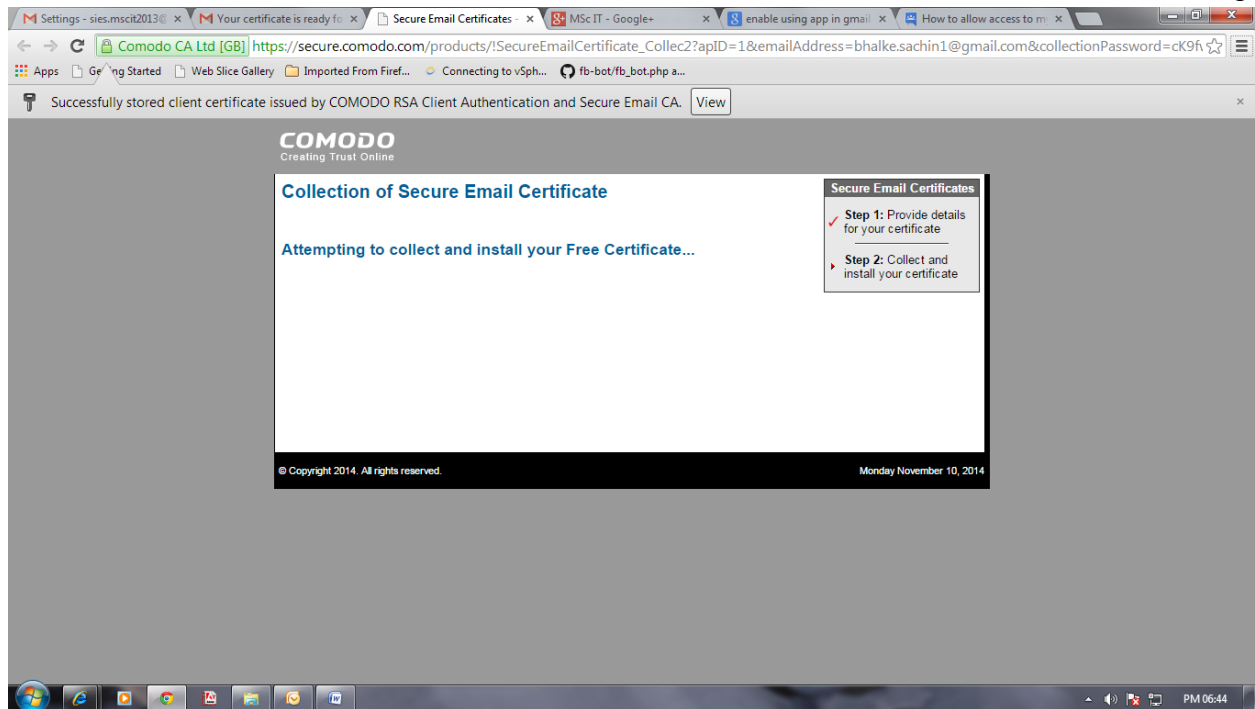




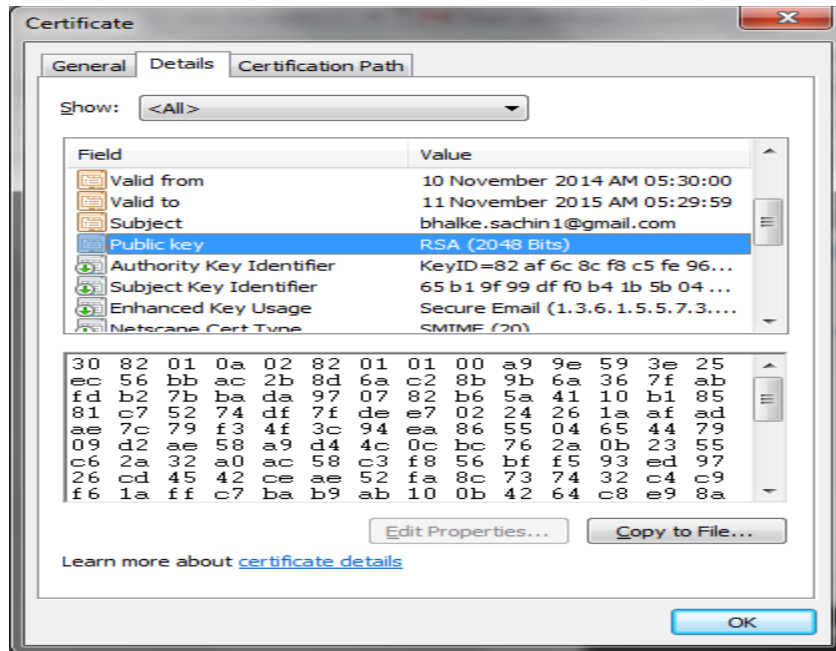
GO to your gmail account and open the then click on Install



Click on “View” on the top



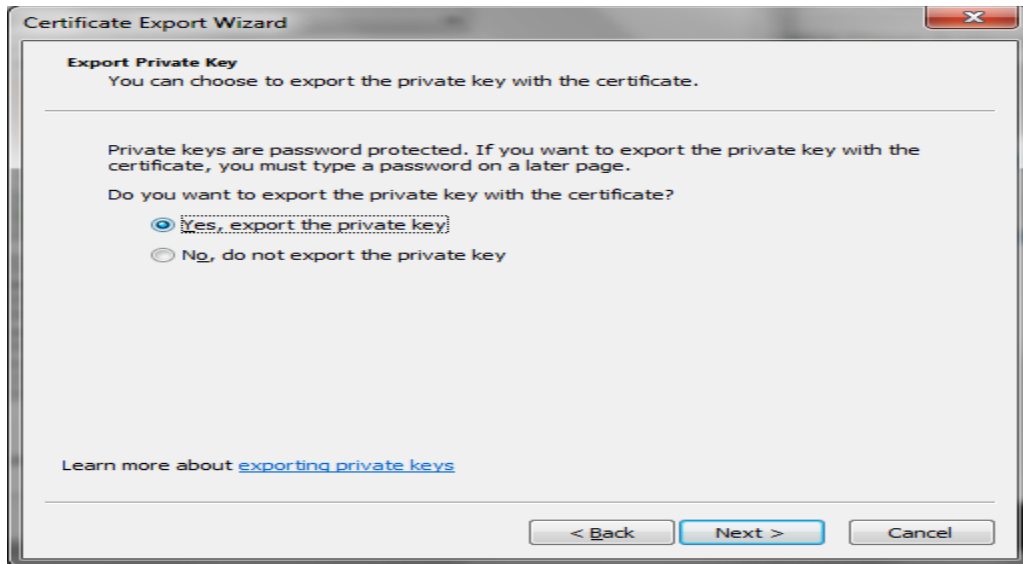
Click on “Detail” . Then Select “Public key” . Then “Copy to file”



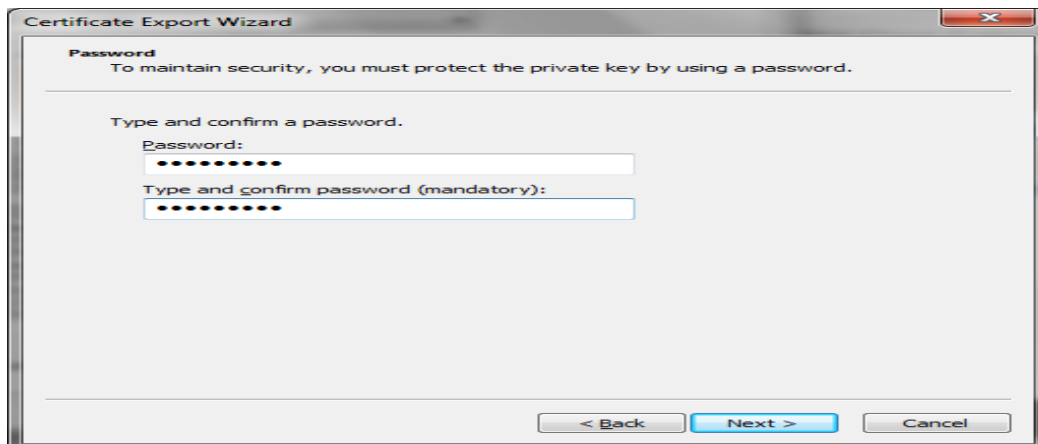
Click next



Click Yes and next



Click Next and Create password

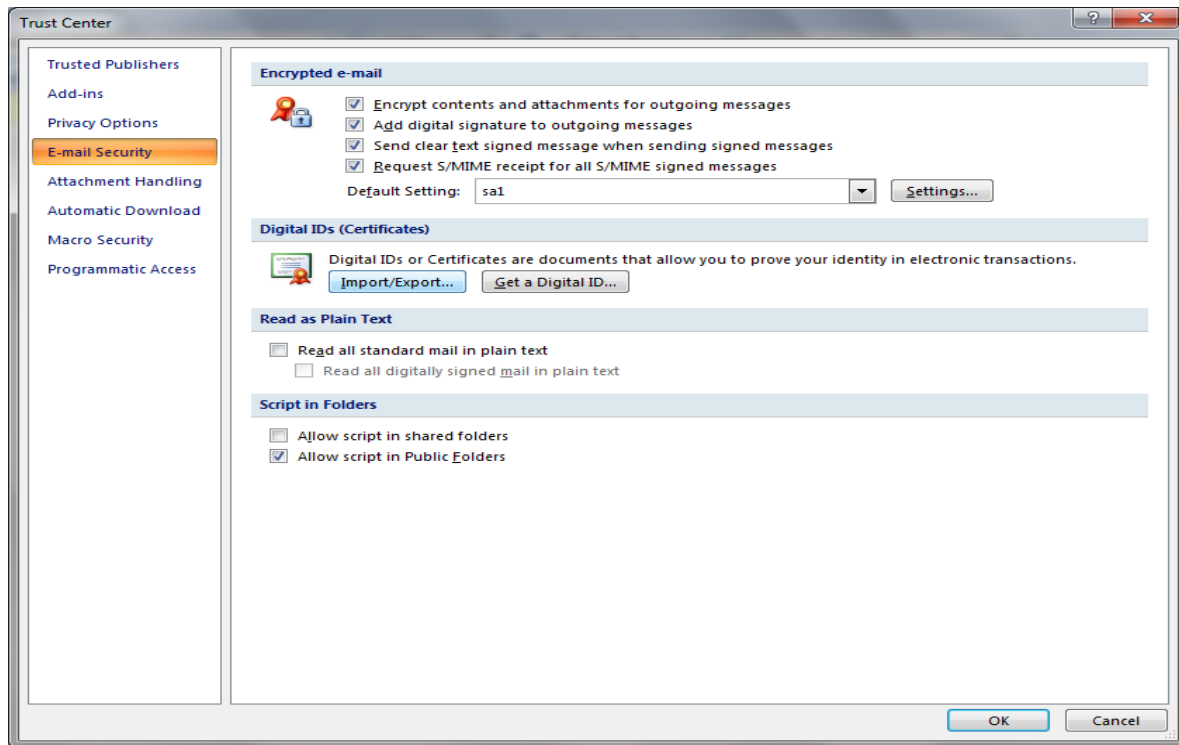


Next → Then Browse data to store → Finish

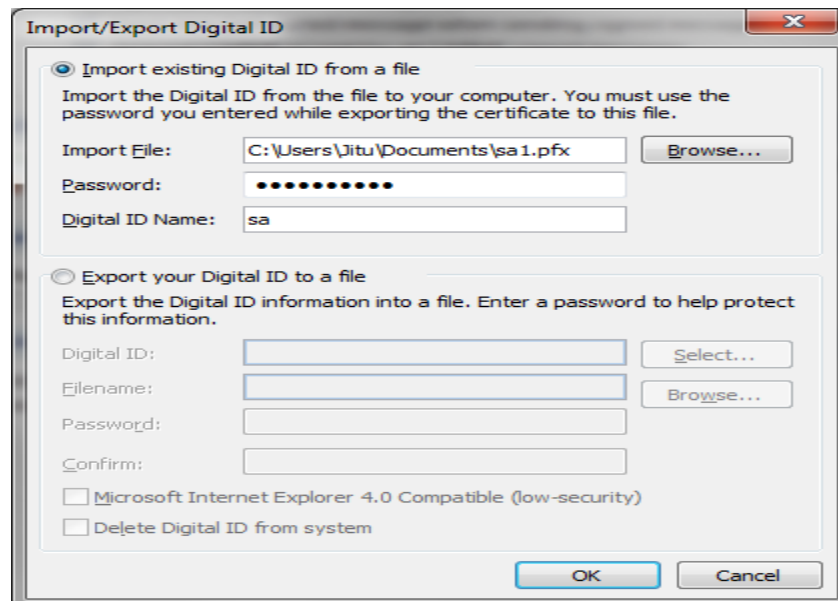
→ Repeat above same step using different gmail account(Receiver)

Now configure that Certificate to your outlook account

Go to Tools → Trust center → Email Security → click on Import /export

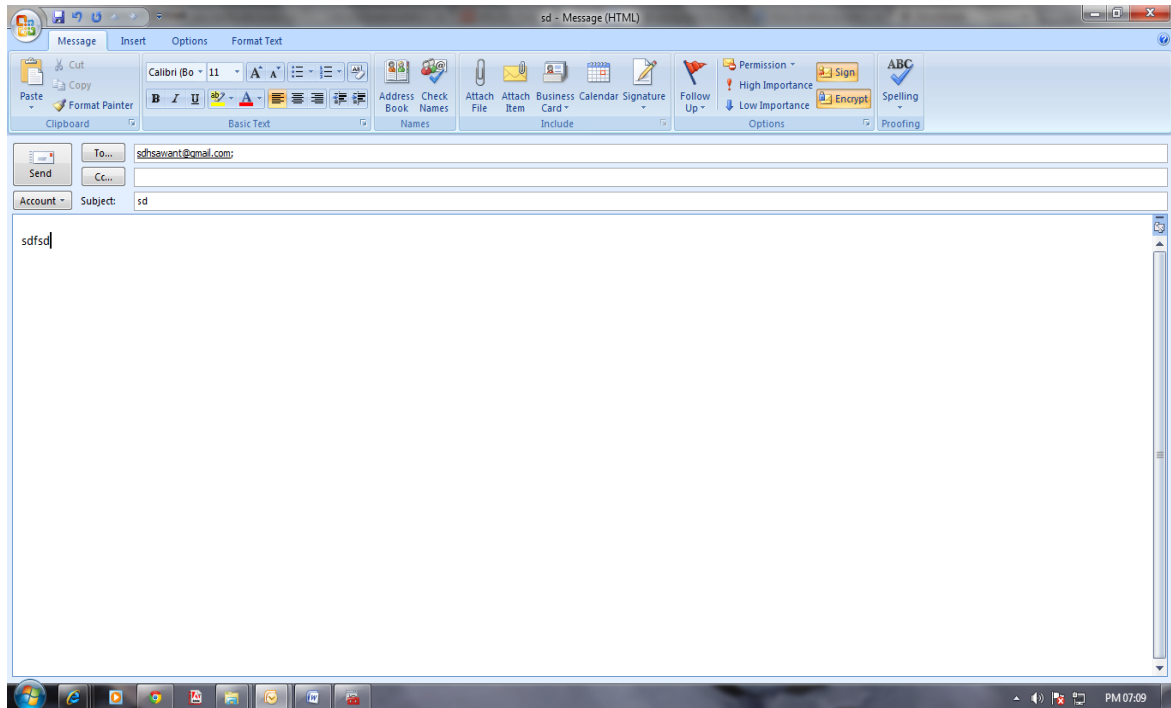


Browse your Digital Certificate here

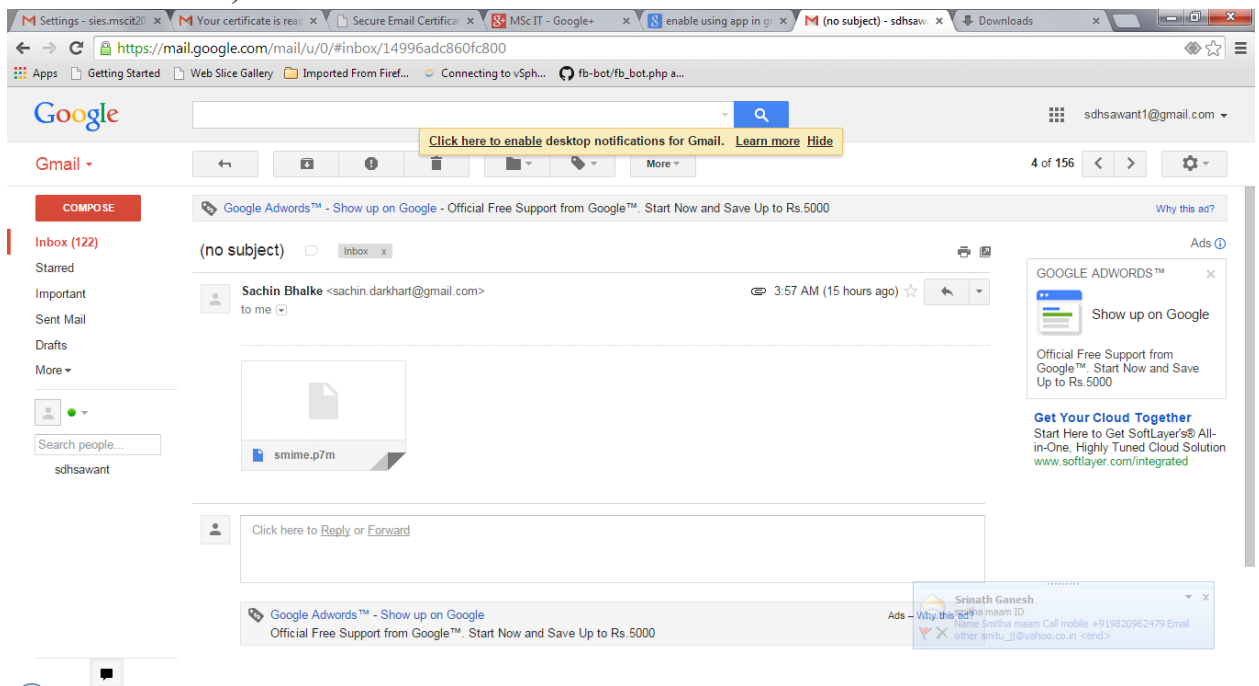


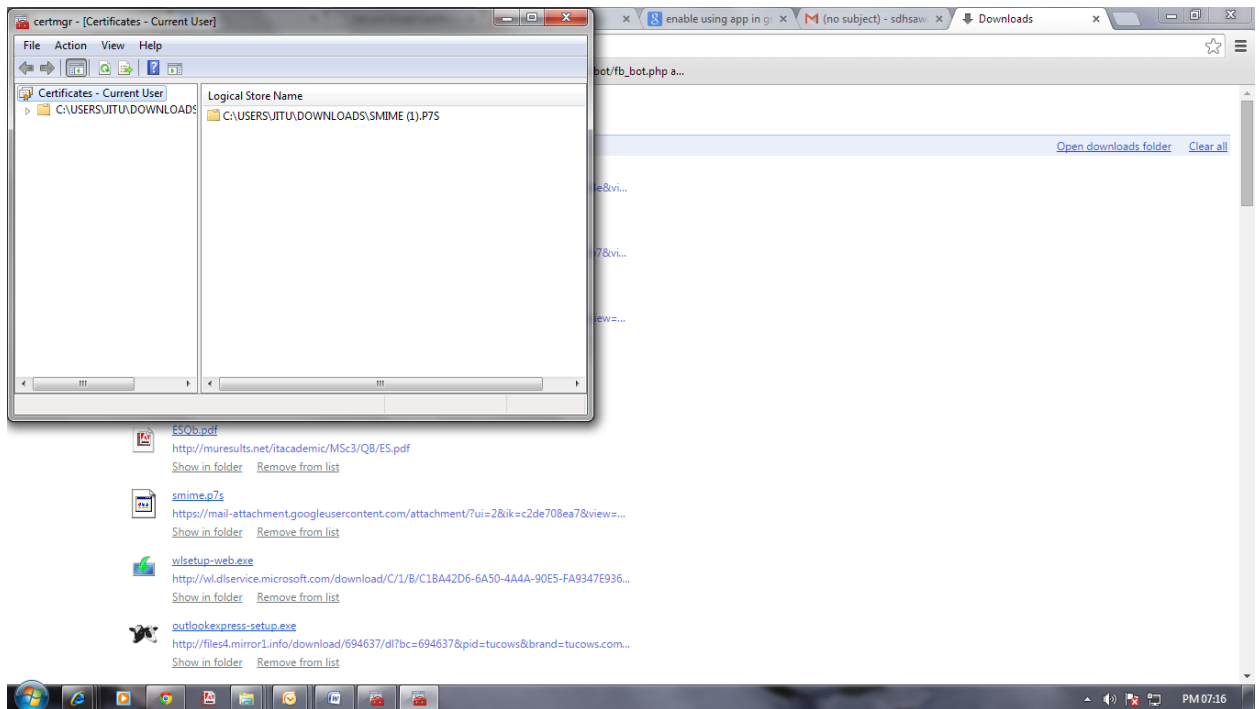
→click “OK”

- Create new message
- And send to Reciever

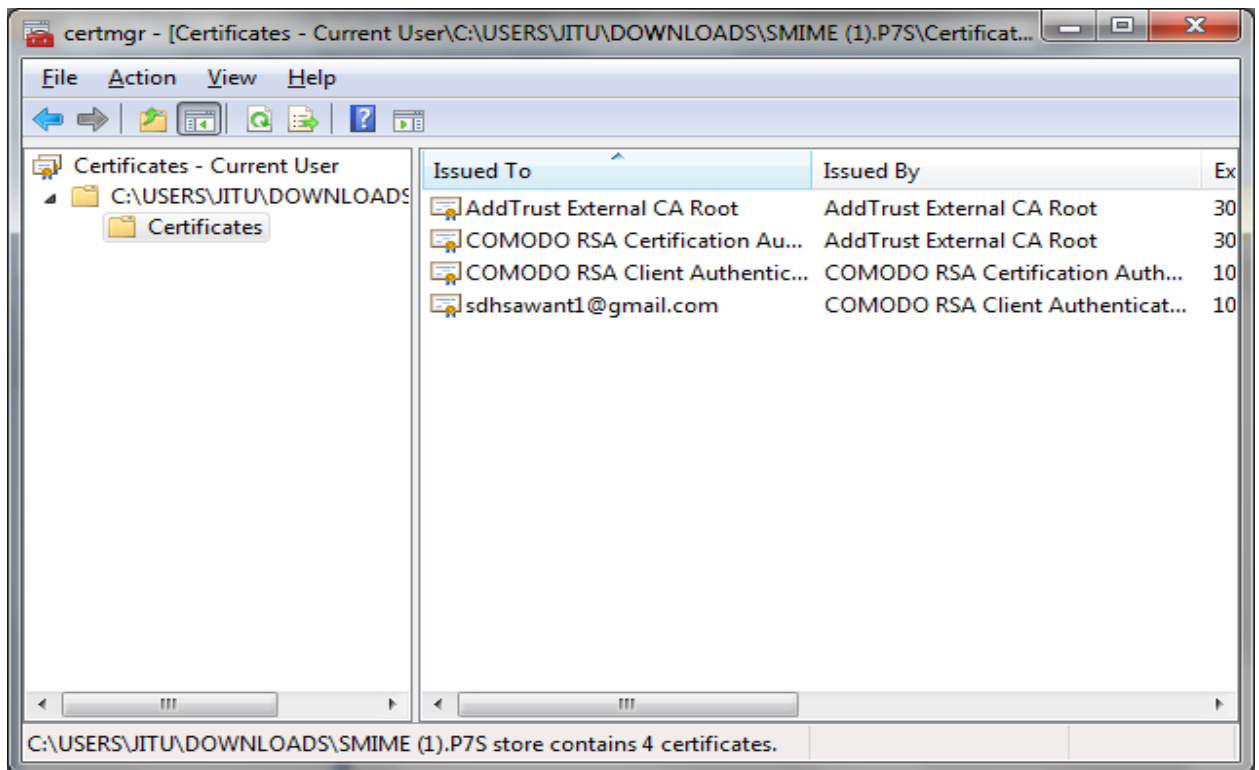


Download the attached file(Public key)→open if not directly open(open with “Crypto Shell Extensions”)

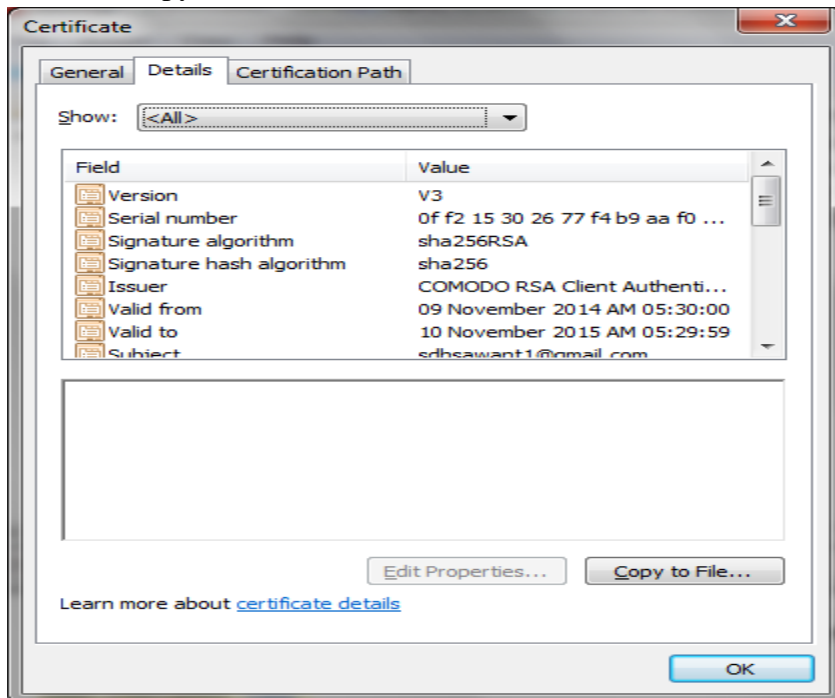




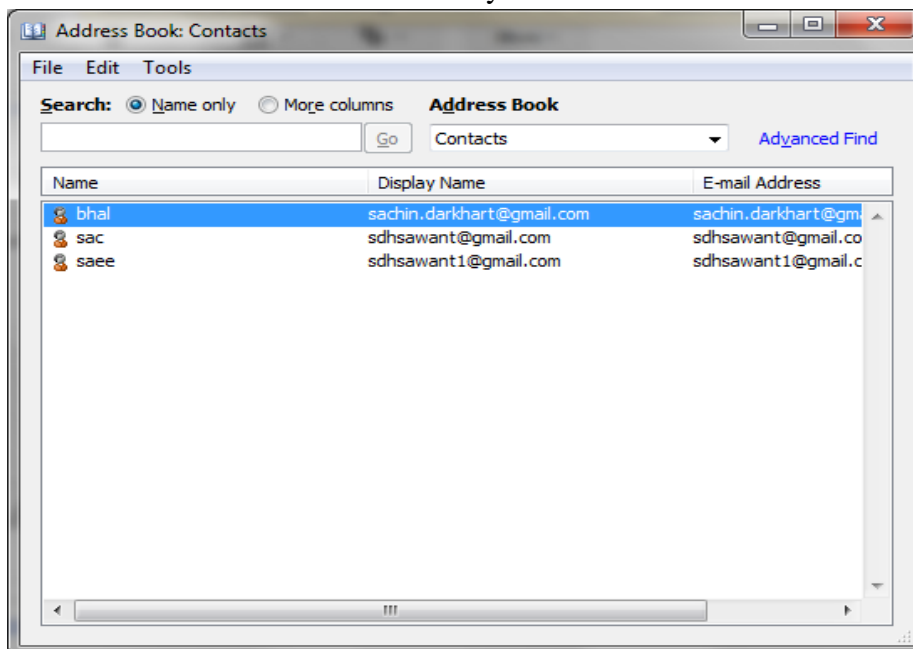
Click on Certificates



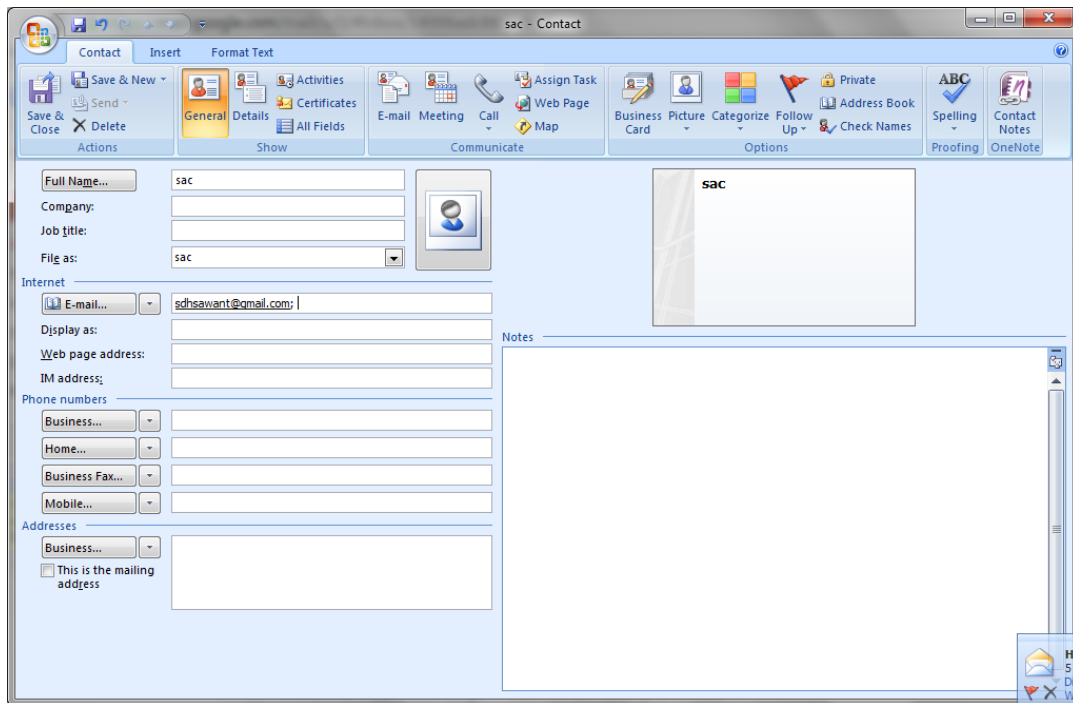
Double click on the "Receivers Public key"(Issued To →email address)
Details→Copy to files→Save



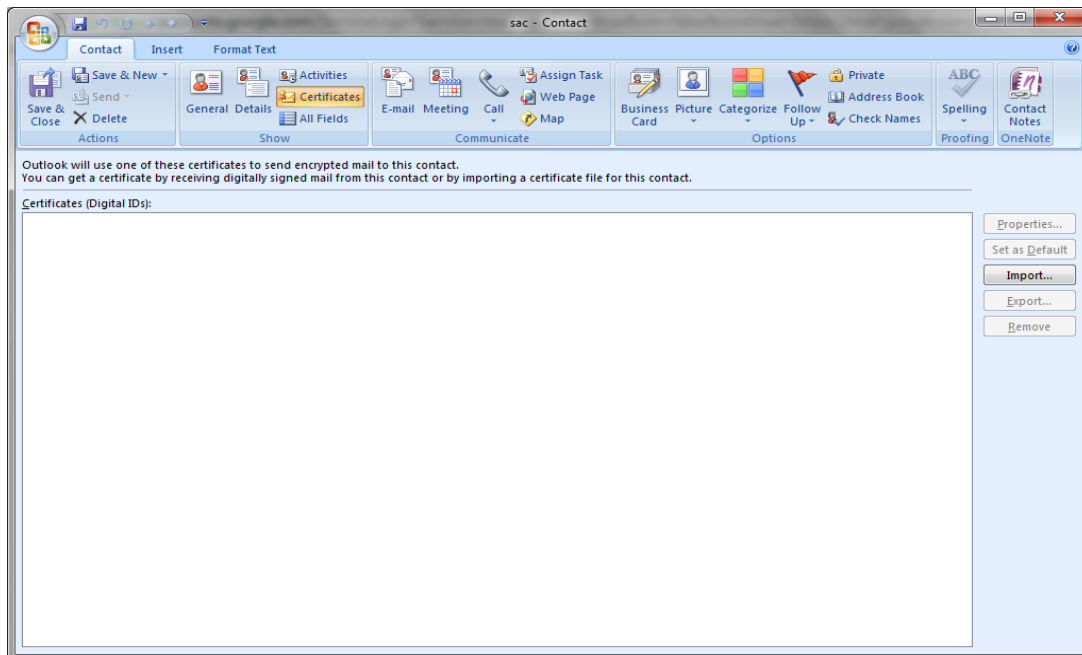
Now Address book→File→New Entry→

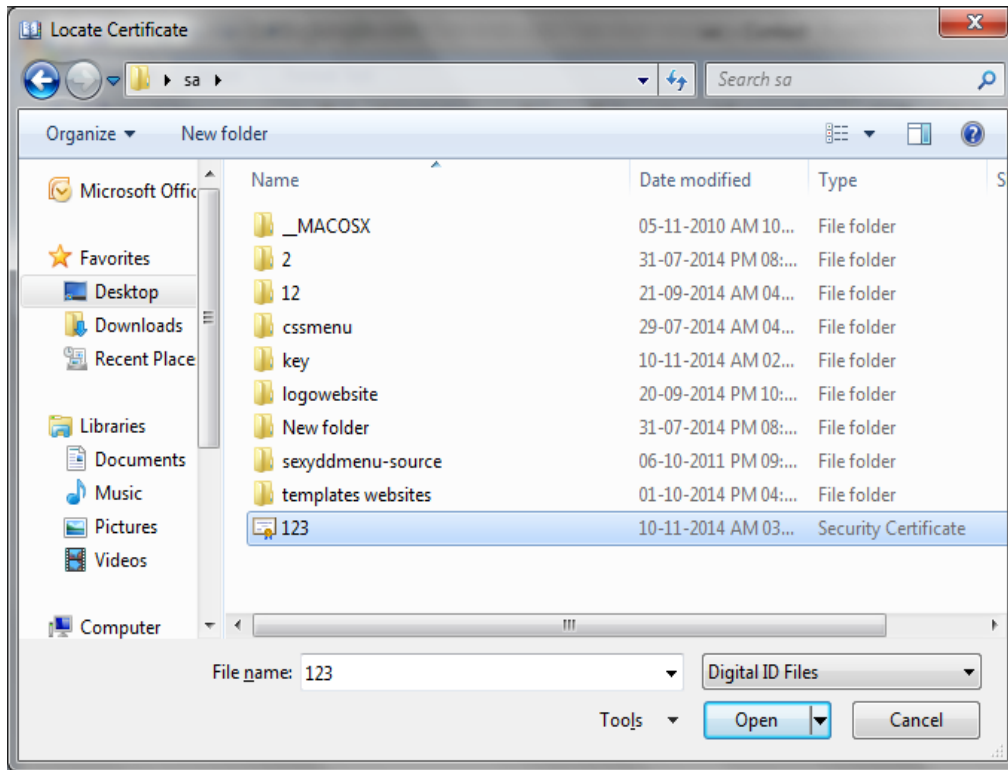


Enter name and Email Address(receivers)



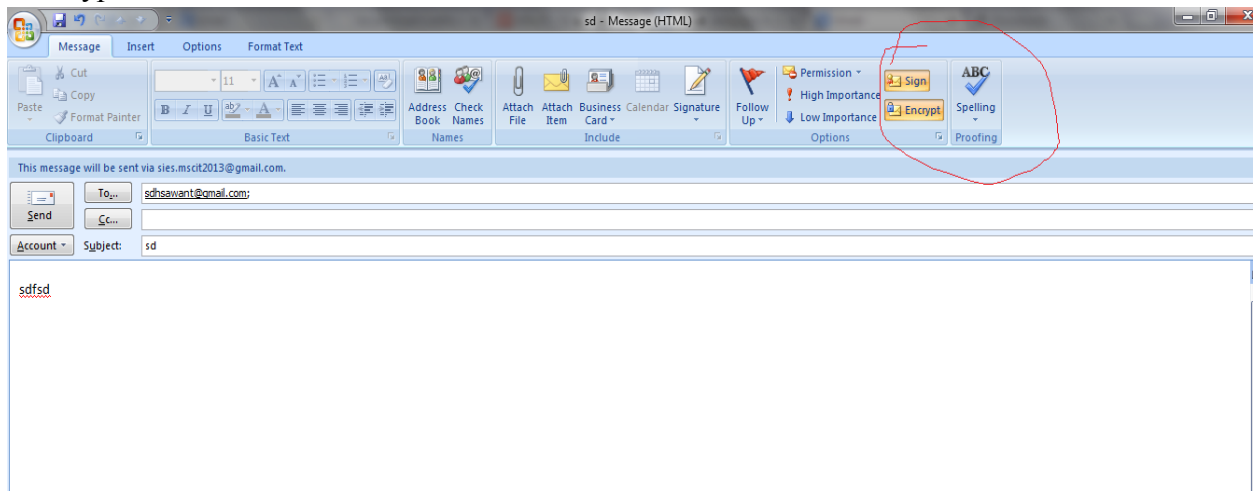
Click on Certificate→Import Certificate(Recievers Public key)





Click "Ok"

Then Create New message →select "To"→ Select contact name→Enable on" Sign " and "Encrypt"→send



Practical No: 6

Aim : Understanding buffer overflow & format string attacks

- make sure u have gedit or equivalent text editor
- Use gedit file.c to create the code file

Source code

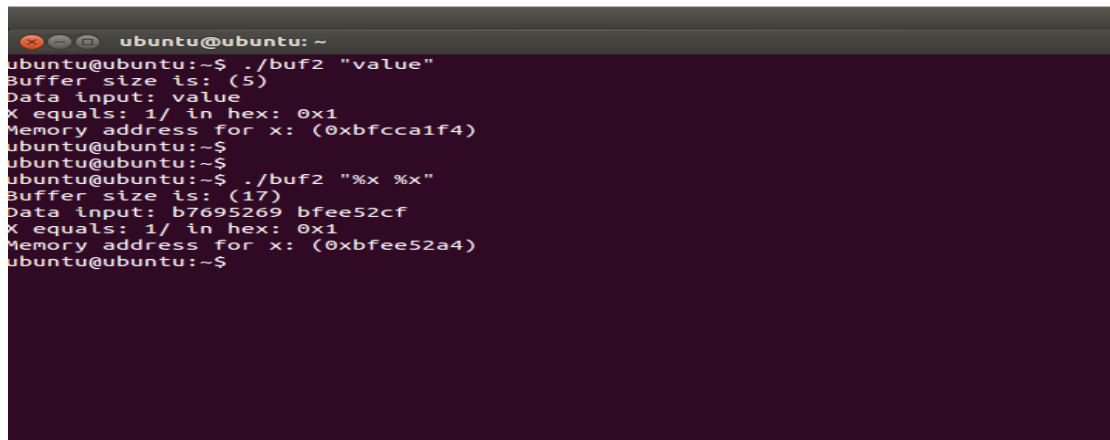
```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

int main (int argc, char **argv)
{
    char buf [100]
    int x = 1
    snprintf ( buf, sizeof buf, argv [1] ) ;
    buf [ sizeof buf -1 ] = 0
    printf ( "Buffer size is: (%d) \nData input: %s \n" , strlen (buf) , buf ) ;
    printf ( "X equals: %d/ in hex: %#x\nMemory address for x: (%p) \n" , x, x,&x) ;
    return 0 ;
}
```

Compile using the following command

```
gcc fileName.c -o fileName
```

This is format string vulnerability. If the format string parameter “%x %x” is inserted in the input string, when the format function parses the argument, the output will display the name Bob, but instead of showing the %x string, the application will show the contents of a memory address.



```
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ ./buf2 "value"
Buffer size is: (5)
Data input: value
X equals: 1/ in hex: 0x1
Memory address for x: (0xbfcca1f4)
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ ./buf2 "%x %x"
Buffer size is: (17)
Data input: b7695269 bfee52cf
X equals: 1/ in hex: 0x1
Memory address for x: (0xbfee52a4)
ubuntu@ubuntu:~$
```

Source code

```
#include <stdio.h>
#include <string.h>

int main(void)
{
    char buff[15];
    int pass = 0;
    printf("\n Enter the password : \n");
    gets(buff);
    if(strcmp(buff, "thegeekstuff"))
    {
        printf ("\n Wrong Password \n");
    }
    else
    {
        printf ("\n Correct Password \n");
        pass = 1;
    }
    if(pass)
    {
        /* Now Give root or admin rights to user*/
        printf ("\n Root privileges given to the user \n");
    }

    return 0;
}
```

Compile using the following command

```
gcc fileName.c -o fileName
```

There is a logic behind the output above. What attacker did was, he/she supplied an input of length greater than what buffer can hold and at a particular length of input the buffer overflow so took place that it overwrote the memory of integer 'pass'. So despite of a wrong password, the value of 'pass' became non zero and hence root privileges were granted to an attacker.

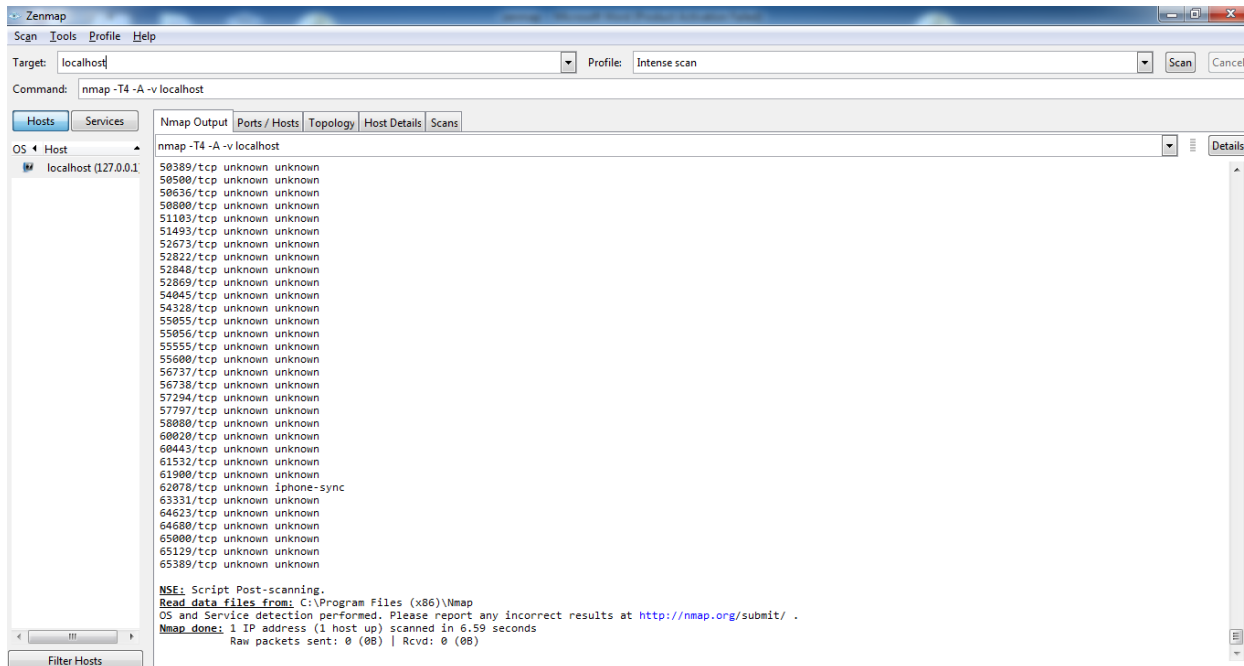
Practical No: 7

Aim : Using Nmap/Zenmap

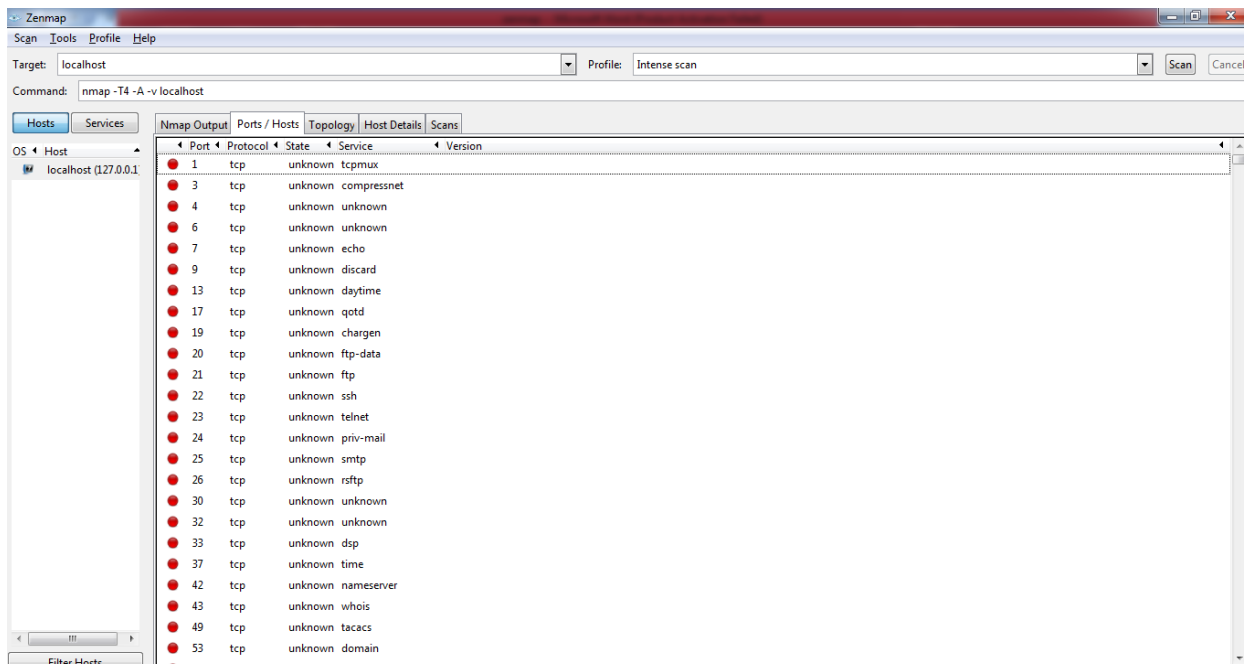
Open Nmap

Target --> "localhost"

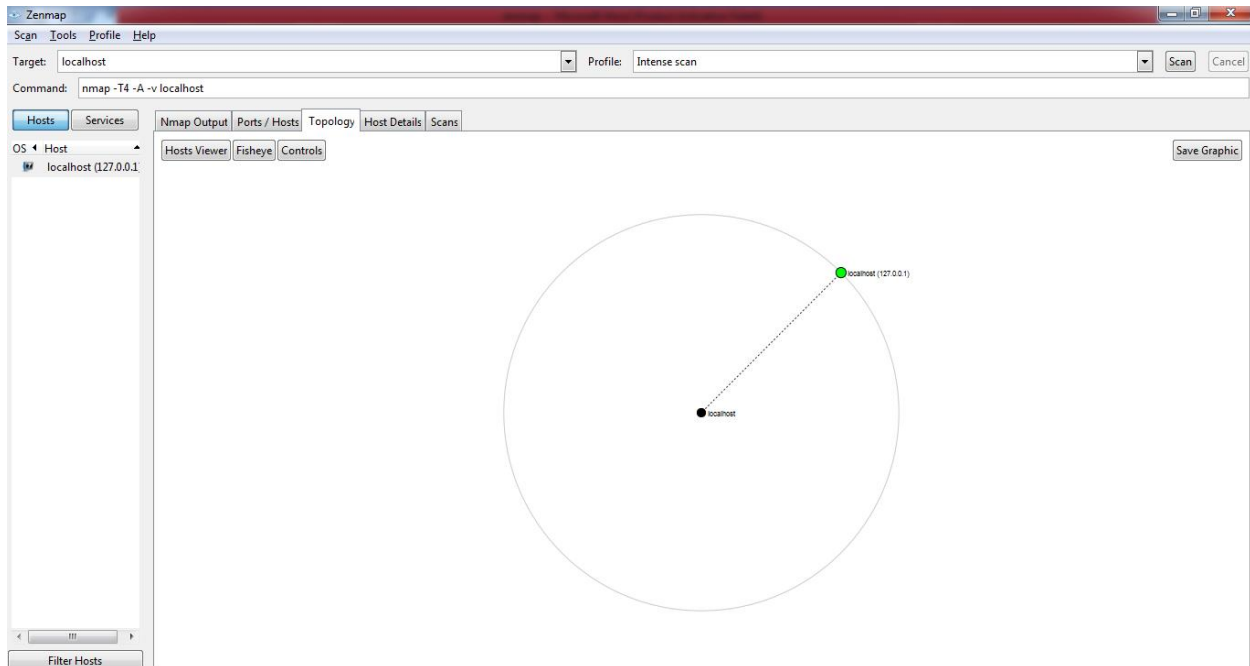
Select "Scan" --> Select Profile "Intense Scan"



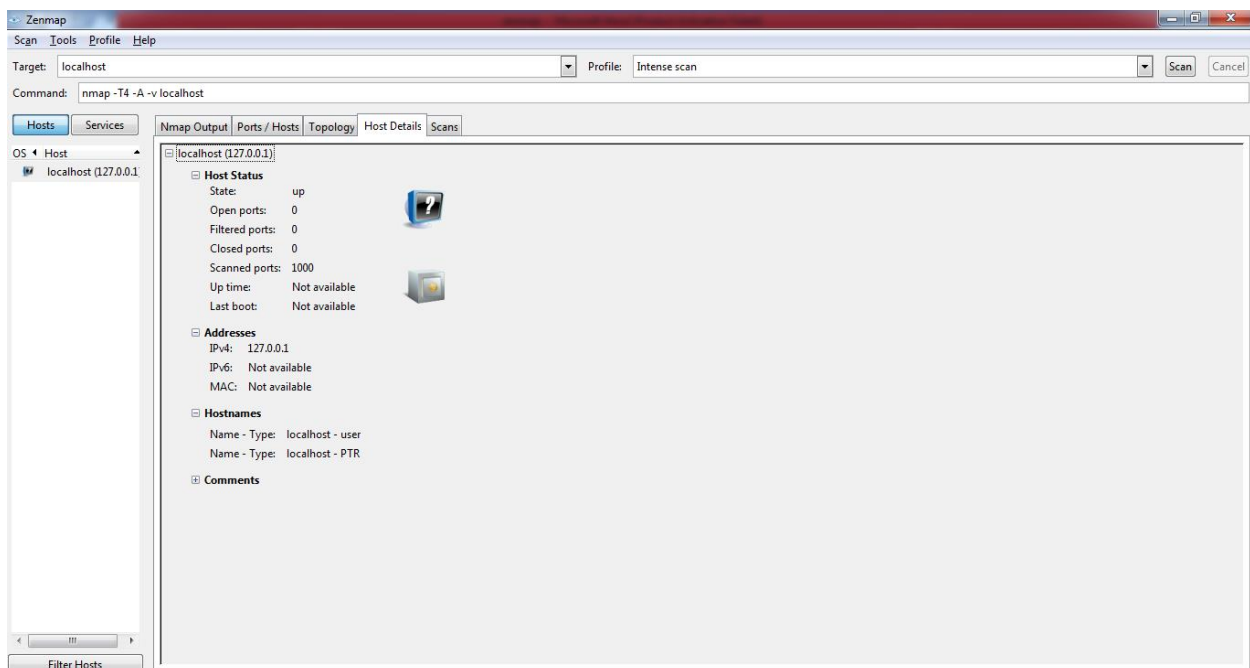
Select Host Tab



Open Topology Tab



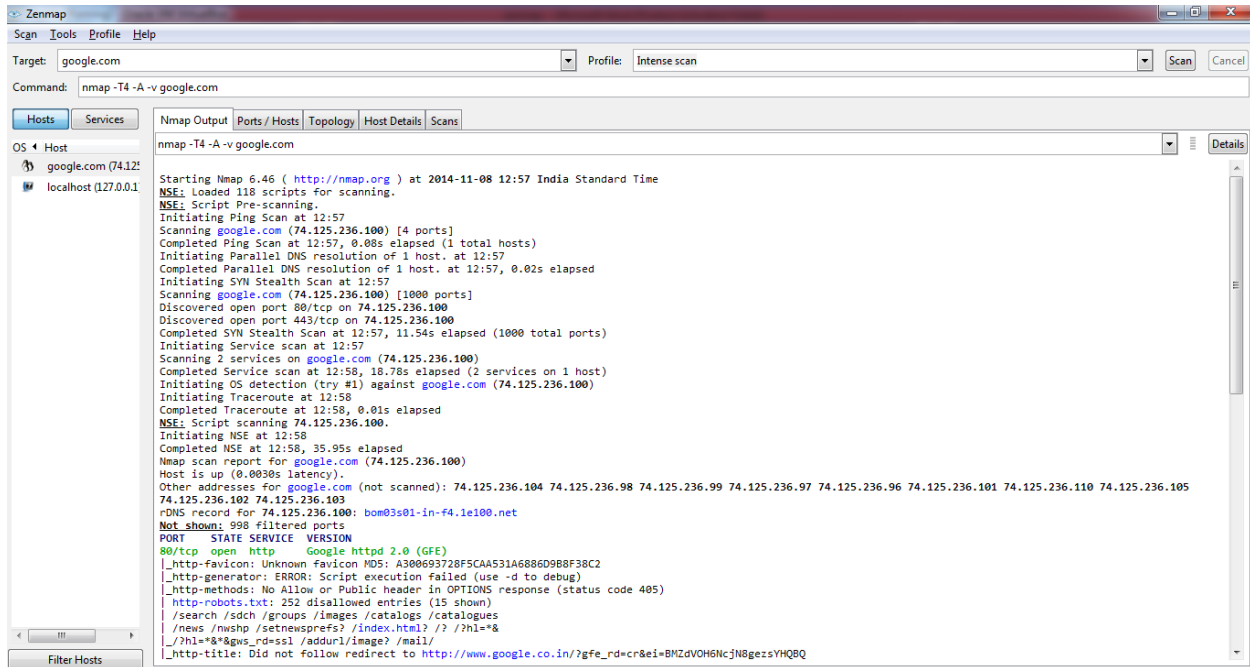
Open Host Details



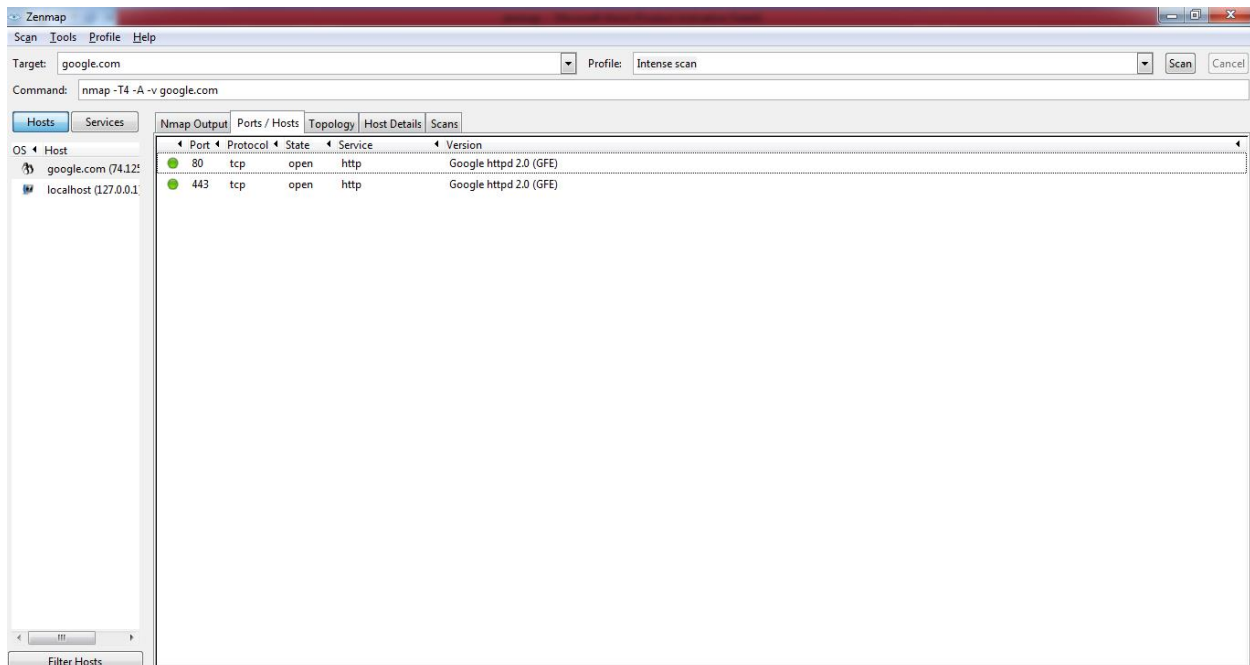
Target --> "google.com"

Select "Scan" --> Select Profile "Intense Scan"

Select Host Tab --> Nmap Output



Go to Ports/Hosts tab

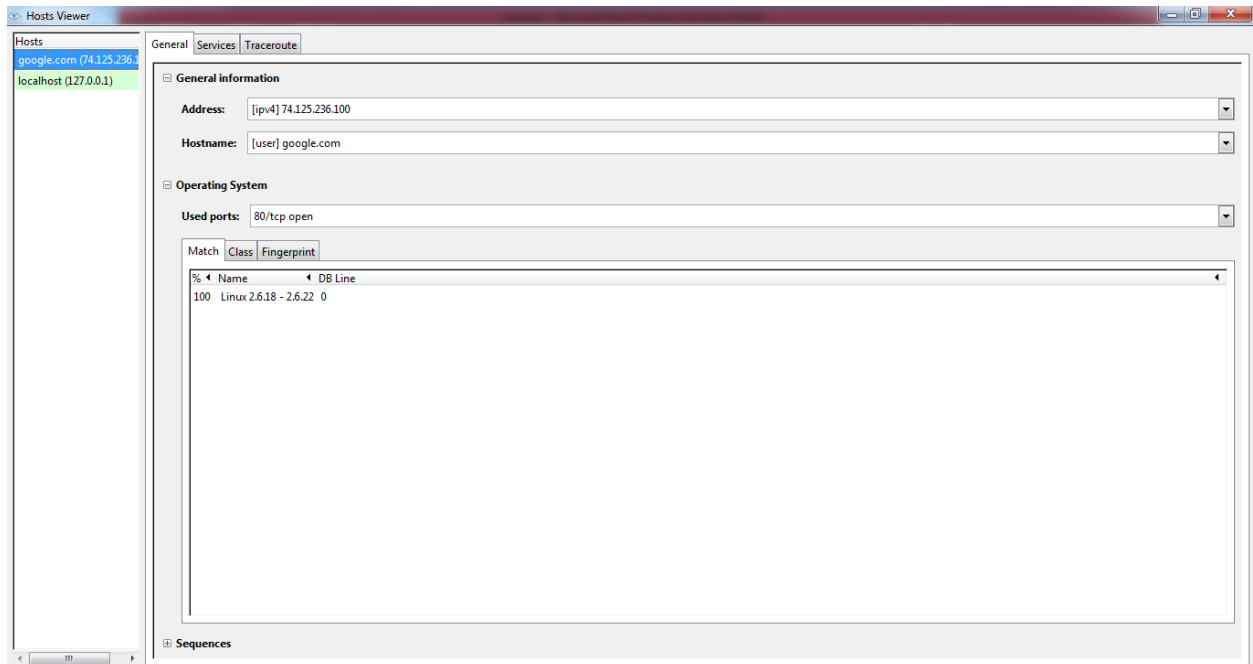


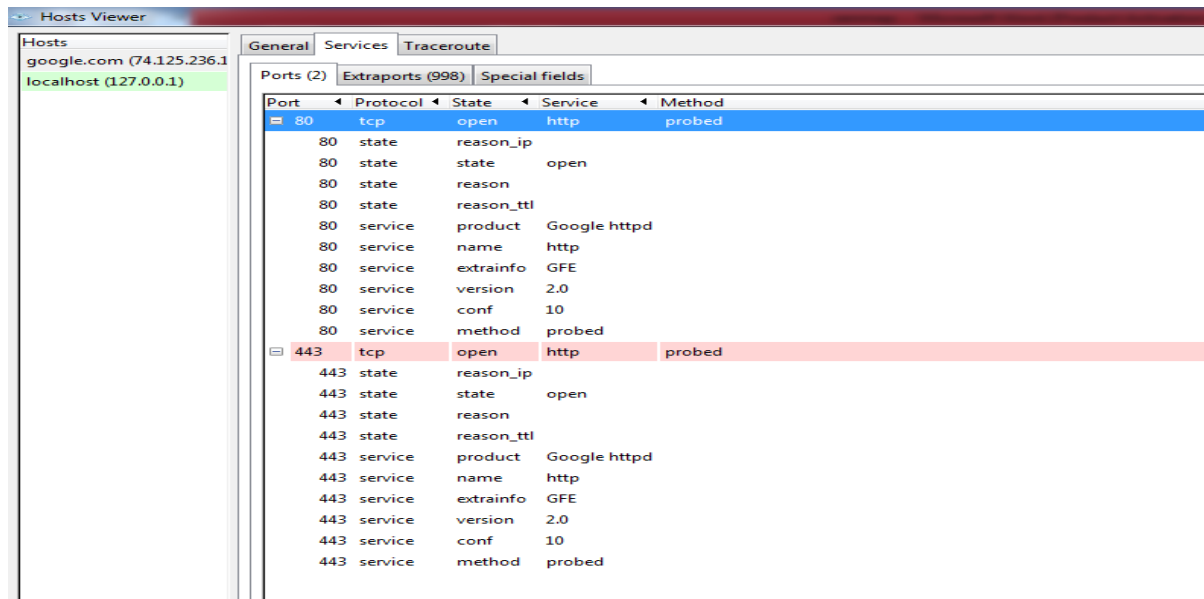
Go to Host Viewer

Go

to

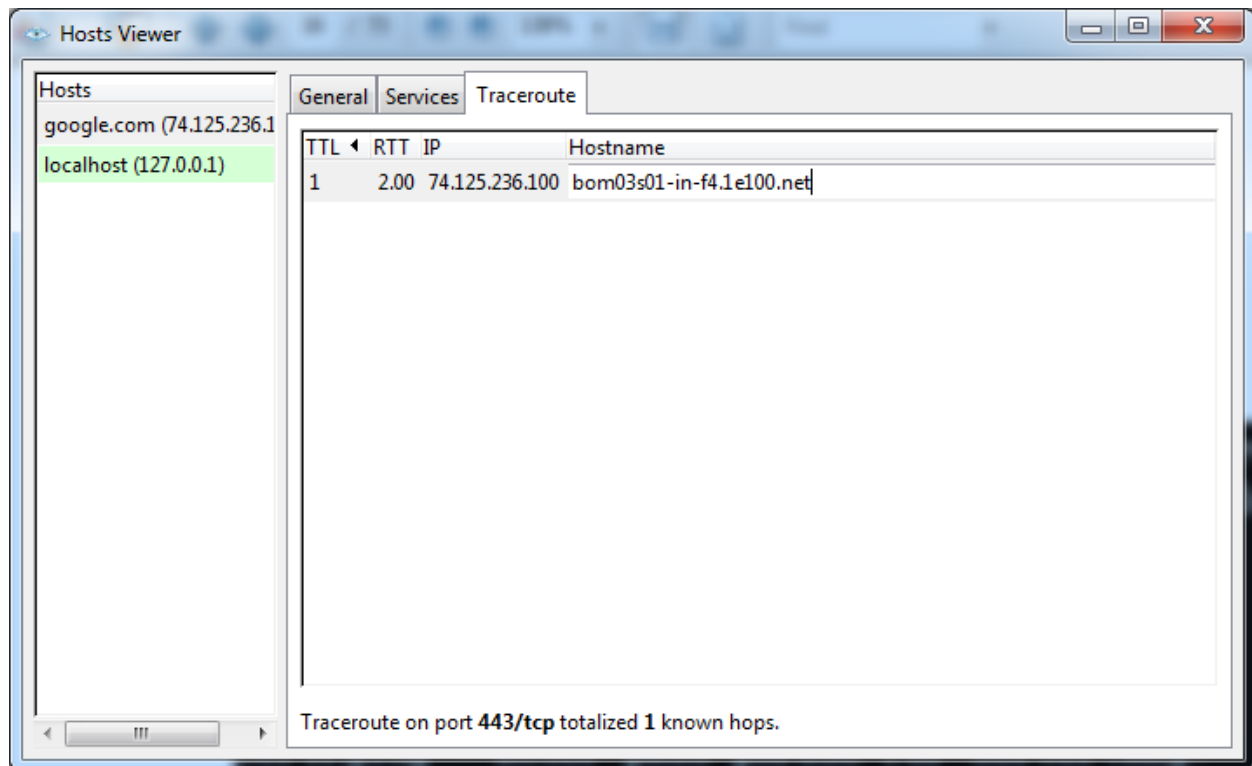
General



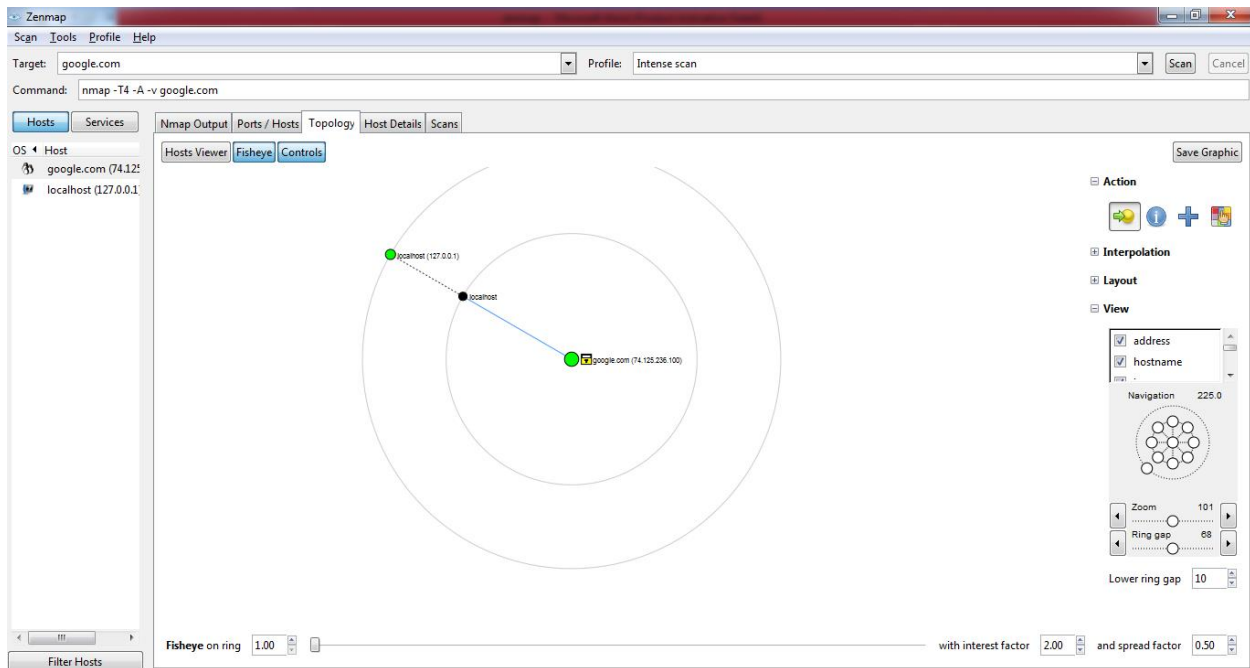


Go to Service

Go To Traceroute



Go to Zenmap --> Select "Hosts"



Select Host Details

Target: google.com Profile: Intense scan Command: nmap -T4 -A -v google.com

Hosts Services

OS Host

- google.com (74.125.236.100)
- localhost (127.0.0.1)

Host Details for google.com (74.125.236.100)

- Host Status**
 - State: up
 - Open ports: 2
 - Filtered ports: 998
 - Closed ports: 0
 - Scanned ports: 1000
 - Up time: Not available
 - Last boot: Not available
- Addresses**
 - IPv4: 74.125.236.100
 - IPv6: Not available
 - MAC: Not available
- Hostnames**
 - Name - Type: google.com - user
 - Name - Type: bom03s01-in-f4.1e100.net - PTR
- Operating System**
 - Name: Linux 2.6.18 - 2.6.22
 - Accuracy: 100%
- Ports used**
- OS Classes**

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Linux	Linux	2.6.X	100%
- TCP Sequence**

Target "scanme.nmap.org" --> Profile Intense Scan

Target: scanme.nmap.org Profile: Intense scan Command: nmap -T4 -A -v scanme.nmap.org

Hosts Services

OS Host

- google.com (74.125.236.100)
- localhost (127.0.0.1)
- scanme.nmap.org

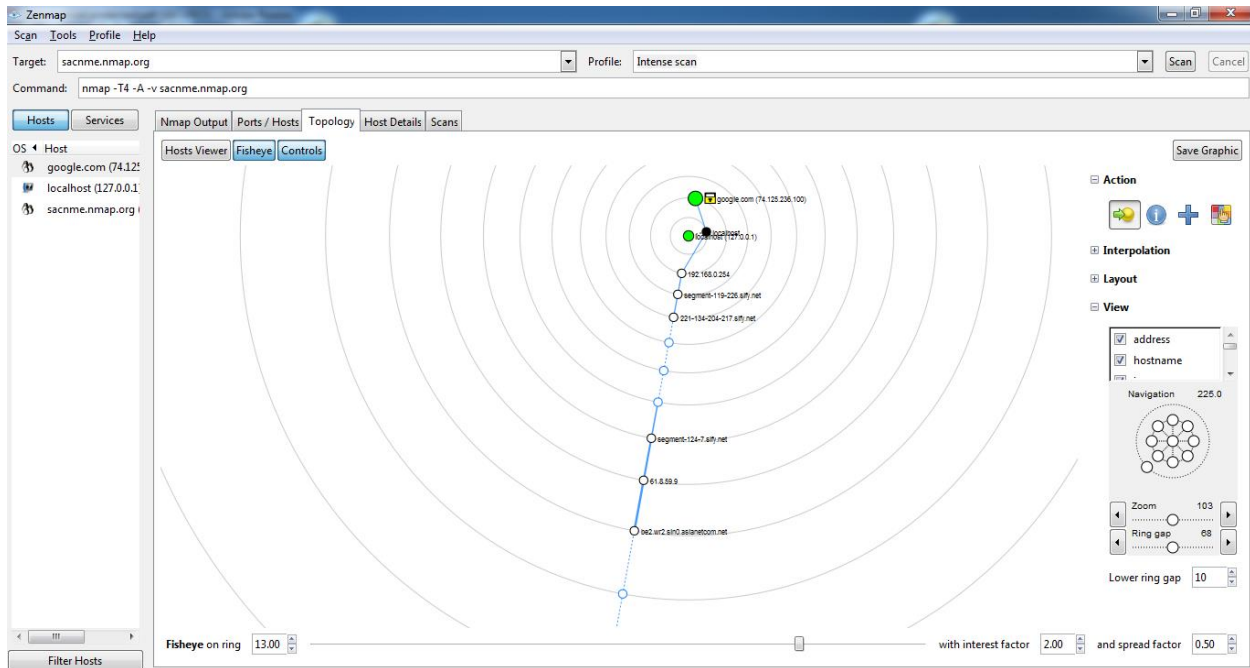
Host Details for scanme.nmap.org

```
nmap -T4 -A -v scanme.nmap.org
|_ Consider submitting a service fingerprint.
|_ Run with --script-args http-server-header.skip
|_ http-title: / - Revision 33798: /
|_ ssl-date: 2014-11-08T07:34:46+00:00; -17s from local time.
31337/tcp closed Elite
Device type: general purpose|storage-misc|firewall|broadband router
Running (JUST GUESSING): Linux 2.6.X|3.X (93%), Netgear RAIDiator 4.X (87%), Zhone embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.18 cpe:/o:linux:linux_kernel:3 cpe:/o:netgear:raidiator:4 cpe:/h:zhone:6211-13
Aggressive OS guesses: Linux 2.6.18 (93%), Linux 2.6.18 - 2.6.22 (90%), Linux 2.6.15 - 2.6.26 (likely embedded) (87%), Linux 3.2 - 3.6 (87%), Linux 3.5 (87%),
Netgear ReadyNAS Duo NAS device (RAIDiator 4.1.4) (87%), Linux 2.6.32 - 2.6.39 (86%), Linux 3.2.0 (85%), Vyatta router (Linux 2.6.26) (85%), Linux 2.6.28 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.041 days (since Sat Nov 08 12:09:28 2014)
Network Distance: 15 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 113/tcp)
HOP RTT ADDRESS
1 1.00 ms 192.168.0.254
2 17.00 ms segment-119-226.sify.net (119.226.13.193)
3 17.00 ms 221-134-204-217.sify.net (221.134.204.217)
4 ... 6
7 35.00 ms segment-124-7.sify.net (124.7.237.85)
8 77.00 ms 61.8.59.9
9 100.00 ms be2.wr2.sin0.asianetcom.net (61.14.157.185)
10 ... 11
12 289.00 ms 10ge0-1.core1.sjc2.he.net (216.218.192.233)
13 289.00 ms 10ge3-2.core3.fmt2.he.net (184.105.222.13)
14 275.00 ms router3-fat.linode.com (65.49.10.218)
15 282.00 ms nmap.org (173.255.243.189)

NSE: Script Post-scanning.
Initiating NSE at 13:08
Completed NSE at 13:08, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 365.00 seconds
Raw packets sent: 3138 (142.562KB) | Rcvd: 102 (5.674KB)
```

Select Host --> Select Topology



Practical No: 8

Aim : Socket Programming

Socket program Client class

```
import java.io.DataInputStream;
import java.io.DataOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;

public class GreetingClient {
    public static void main(String[] args) {
        String serverName = args[0];
        int port = Integer.parseInt(args[1]);
        try
        {
            System.out.println("Connecting to " + serverName + " on port "
                + port);
            Socket client = new Socket(serverName, port);
            System.out.println("Just connected to "
                + client.getRemoteSocketAddress());
            OutputStream outToServer = client.getOutputStream();
            DataOutputStream out = new DataOutputStream(outToServer);
            out.writeUTF("Hello from " + client.getLocalSocketAddress());
            InputStream inFromServer = client.getInputStream();
            DataInputStream in = new DataInputStream(inFromServer);
            System.out.println("Server says " + in.readUTF());
            client.close();
        }
        catch (IOException e)
        {
            e.printStackTrace();
        }
    }
}
```

Socket program Server class

```
import java.io.DataInputStream;
import java.io.DataOutputStream;
import java.io.IOException;
import java.net.ServerSocket;
import java.net.Socket;
import java.net.SocketTimeoutException;
```

```

public class GreetingServer extends Thread {
    private final ServerSocket serverSocket;

    public GreetingServer(int port) throws IOException {
        serverSocket = new ServerSocket(port);
        serverSocket.setSoTimeout(10000);
    }

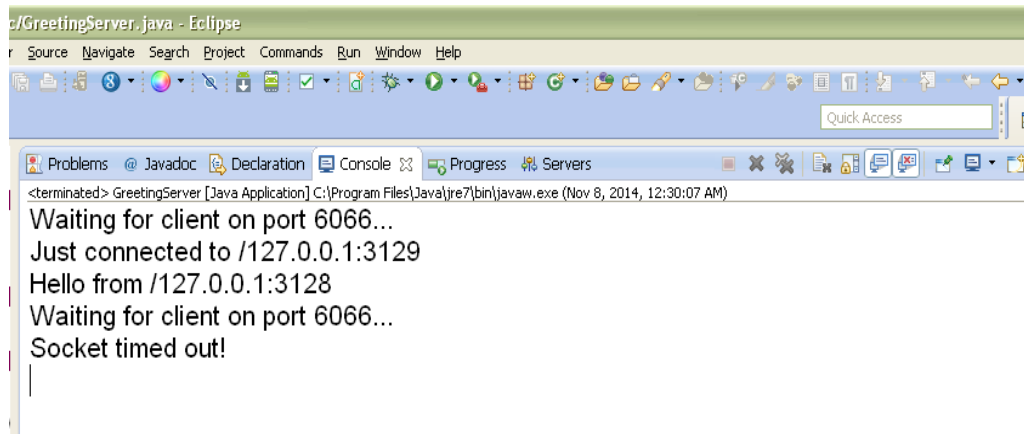
    @Override
    public void run() {
        while (true) {
            try {
                System.out.println("Waiting for client on port "
                    + serverSocket.getLocalPort() + "...");
                Socket server = serverSocket.accept();
                System.out.println("Just connected to "
                    + server.getRemoteSocketAddress());
                DataInputStream in = new DataInputStream(
                    server.getInputStream());
                System.out.println(in.readUTF());
                DataOutputStream out = new DataOutputStream(
                    server.getOutputStream());
                out.writeUTF("Thank you for connecting to "
                    + server.getLocalSocketAddress() + "\nGoodbye!");
                server.close();
            } catch (SocketTimeoutException s) {
                System.out.println("Socket timed out!");
                break;
            } catch (IOException e) {
                e.printStackTrace();
                break;
            }
        }
    }

    public static void main(String[] args) {
        int port = Integer.parseInt(args[0]);
        try {
            Thread t = new GreetingServer(port);
            t.start();
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}

```

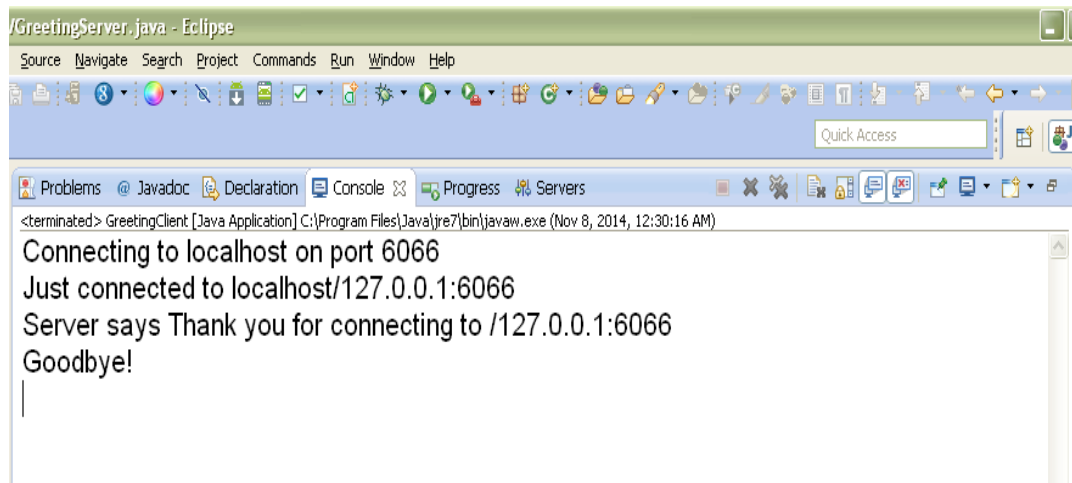

Run at command prompt

Java GreetingServer 6066



```
c:/GreetingServer.java - Eclipse
r Source Navigate Search Project Commands Run Window Help
Problems Javadoc Declaration Console Progress Servers
<terminated> GreetingServer [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Nov 8, 2014, 12:30:07 AM)
Waiting for client on port 6066...
Just connected to /127.0.0.1:3129
Hello from /127.0.0.1:3128
Waiting for client on port 6066...
Socket timed out!
```

Java GreetingClient localhost 6066



```
/GreetingServer.java - Eclipse
Source Navigate Search Project Commands Run Window Help
Problems Javadoc Declaration Console Progress Servers
<terminated> GreetingClient [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Nov 8, 2014, 12:30:16 AM)
Connecting to localhost on port 6066
Just connected to localhost/127.0.0.1:6066
Server says Thank you for connecting to /127.0.0.1:6066
Goodbye!
```