

DEPARTMENT OF INFORMATION TECHNOLOGY
COMPUTER COMMUNICATION AND NETWORKING LAB
LAB3: 08/08/2019

NOTE:

1. Record your observations in your observation book

Part A: Email System.

Objective: To observe the working of SMTP (communication between SMTP client and server) using command line.

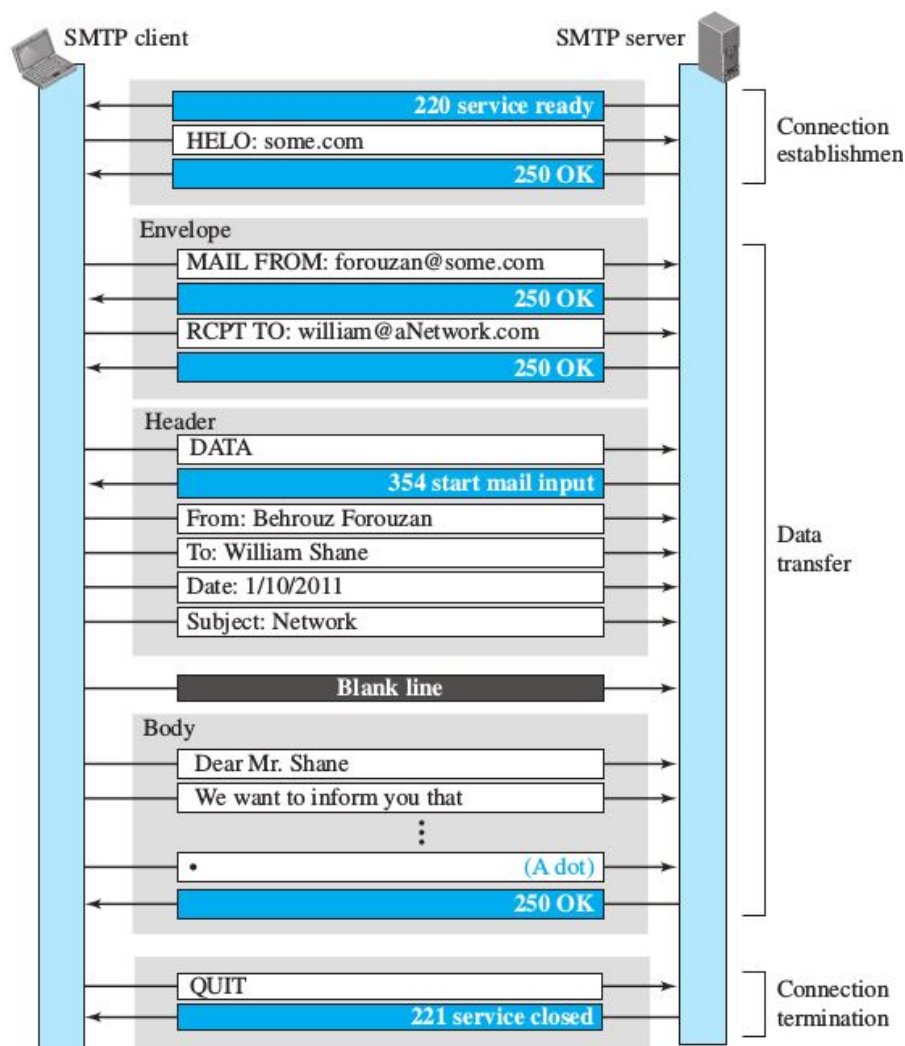


Fig 1. SMTP Client Server Communication

TASK 1: Open terminal. Copy and paste the following command.

You need to login using your credentials to gmail. But login username and password must be encoded. So use base64 converter to get the hash of the username password string.
Copy the following command:

```
echo -en '\000username@gmail.com\000gmailpassword' | base64
```

Replace username with your gmail username and replace gmailpassword with the actual password.

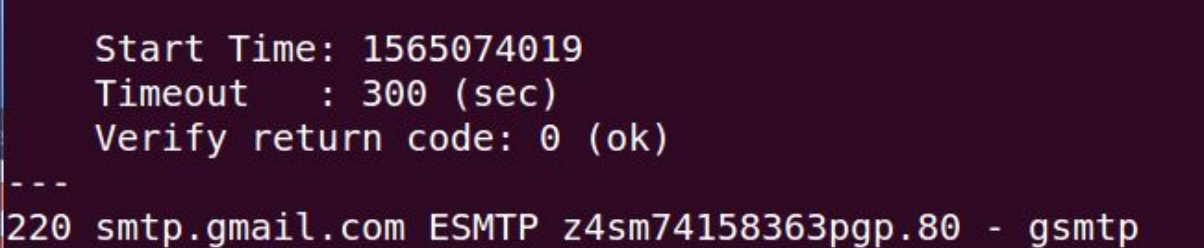
An encoded string will be generated. Just copy this string to a notepad or any other place.
This will be used soon.

Now we are ready to communicate with gmail server.

Copy and paste the following command: openssl is an alternate to TELNET. It is built with Secure Socket Layer(SSL)/ Transport Layer Security(TLS) security.

```
openssl s_client -connect smtp.gmail.com:465 -crlf
```

Port 465 is for smtps : SMTP Secure - SSL encryption is started automatically before any SMTP level communication



```
Start Time: 1565074019
Timeout    : 300 (sec)
Verify return code: 0 (ok)
---
220 smtp.gmail.com ESMTP z4sm74158363pgp.80 - gsmt
```

Note down:

1. Command and the Reply what you get from the server.
2. Try to match it with the dialog flow shown in Figure 1.

Type :

```
HELO www.gmail.com
```

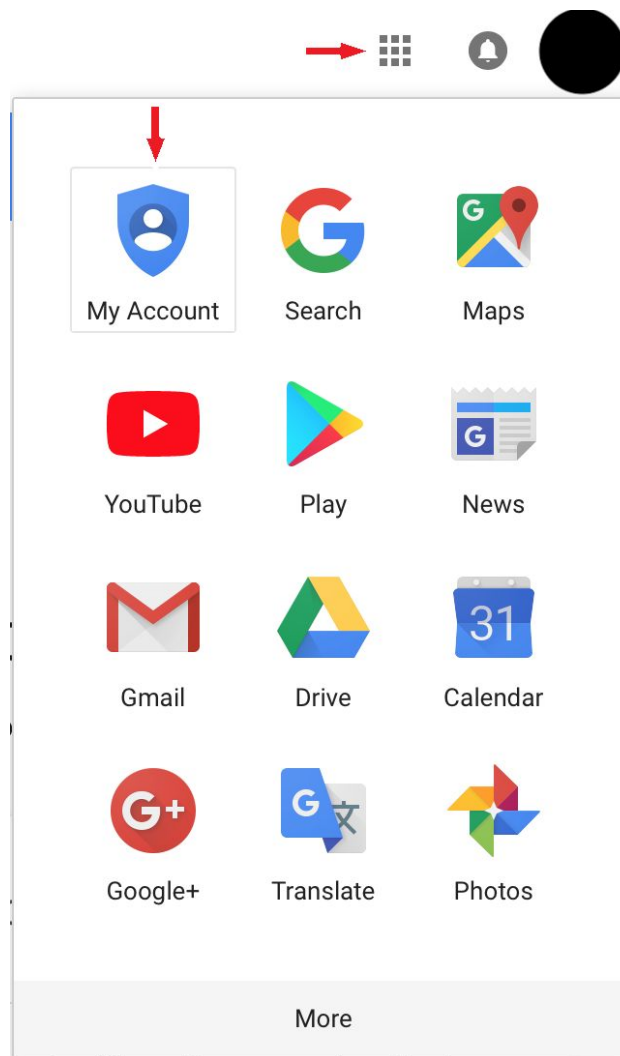
Now Type the command **AUTH PLAIN**

You will get 334 as a reply from server.

Now paste the encoded username password

Server will respond with 235 Accepted.

If you cannot connect to server: Please go to gmail account settings:



Important note: Choose Security option and scroll down to see “Less Secure App Access” option. Turn this option ON. (NOT RECOMMENDED. PLEASE REVERT THIS ONCE YOU FINISH YOUR EXPERIMENT)

OR is you have set “2-step verification ON”. Please turn it OFF. Remember you will have to redo the 2-step verification settings again. Then turn on “Less Secure App Access”.

Now continue logging in from command line. (You may have to start from the beginning).

If server sends 235 accepted after the encrypted username password is entered, we can go ahead for creating a mail. Mail has Envelope, Message Header and Message Body sections.

So first create Envelope by typing :

MAIL FROM: <your gmail id>

After server responds, type:

rcpt to: <recipient's mail id>

Note that **rcpt to** is in lower case. [capital R is a command to server for renegotiation]

After server responds, you will now create Message Header. You will indicate this to server by sending a command:

DATA

Notice the server response.

Now make the header with following details:

FROM:

TO:

DATE:

SUBJECT:

[-----BLank Line-----]

Create Message Body : Type your message

. **[A dot indicates end of message body]**

Notice server response

Now we are done with mail creation, we may close the connection by typing:

QUIT

Note the server response.

PART B: Domain Name System

TASK 2: Querying DNS

Using dig command.

DIG - Domain Information Groper is a tool that is used for querying DNS servers for various DNS records. There are many types of records:

Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

Step 1: Type **dig www.google.com**

Note down the DNS message content.

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29574
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                180     IN      A      172.217.31.206

;; Query time: 3 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Aug 06 21:29:27 IST 2019
;; MSG SIZE rcvd: 55
```

ANSWER Section has Domain, TTL, Class, Record Type, Value

Step 2: Type **dig www.google.com +trace**

Observe the DNS lookup path: First the root name servers for '.' are looked up, followed by the name servers for the .com domain, and then finally the name servers for google.com are returned, followed by the DNS records for it.

Note down how many root servers, TLD servers and authoritative name servers appear in the output.

Also try other websites.

Step 3: Type **dig google.com ANY**

We can use the 'ANY' option to query all DNS record types pertaining to a particular domain.

Note down what different records are returned.

An MX record or mail exchange record maps a domain name to a list of mail exchange servers for that domain.

Type : **dig www.google.com +noall +answer**

This is show only answer section in the DNS message.