

CA169: Week 11

Email - SMTP, POP, IMAP

EMAIL

- One of the killer apps on the Internet – 1965
- Must be connected to the Internet
- Sending and receiving are different
 - SMTP and POP
- Simple Mail Transfer Protocol for outgoing
- Post Office Protocol for retrieving incoming mail
- IMAP is another for retrieving email, some retrieve through file system shared with email server, some proprietary protocols available.

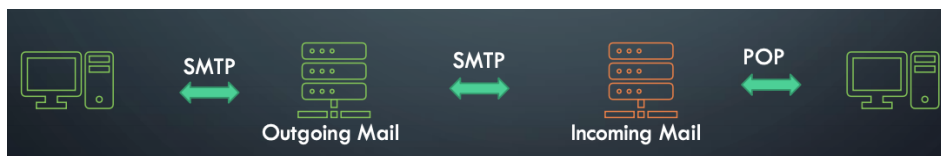
EMAIL & MAIL SERVERS

- Email is managed by mailservers
- You have two
- Incoming mail
- Outgoing mail



SENDING MAIL (SMTP)

- Sending mail is handled by mailservers
- Your local mail server (gmail) takes responsibility to deliver the mail
- It is sent to the recipients incoming mail server

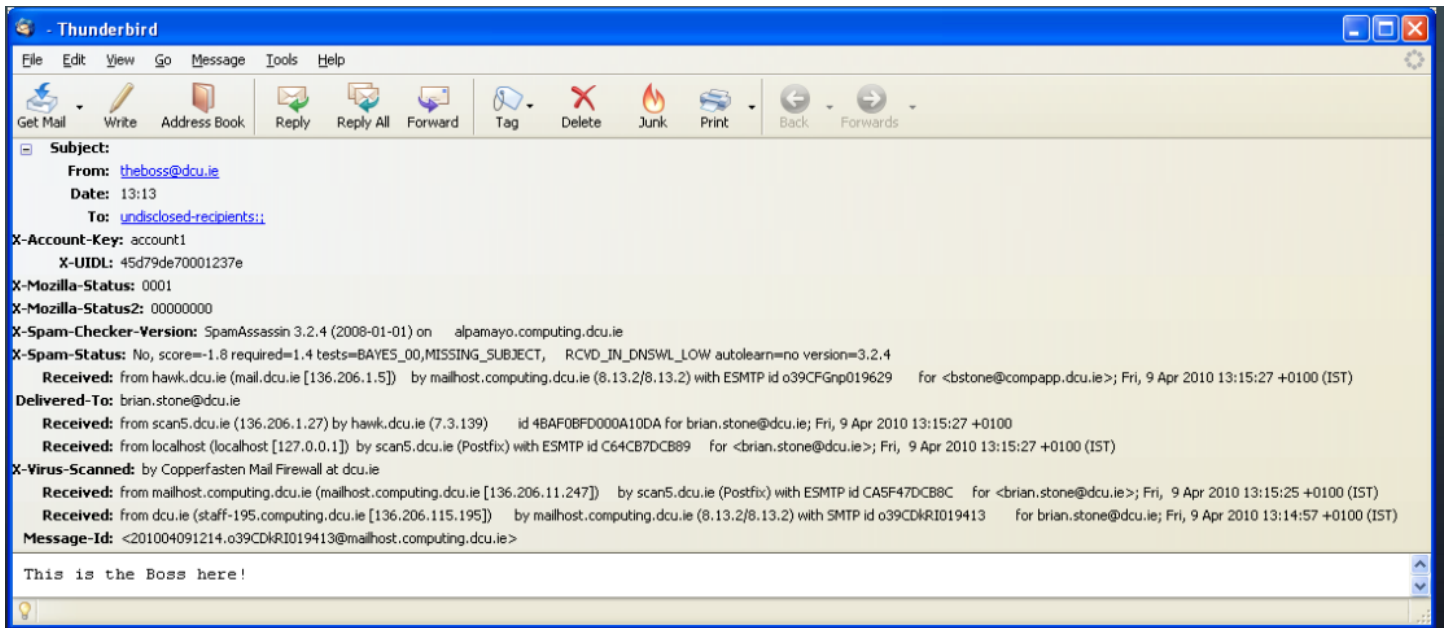
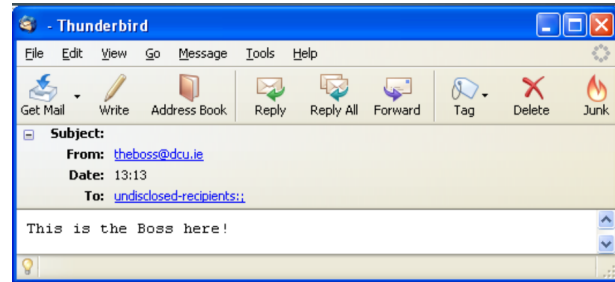


OLD EXAMPLE (PRE-GMAIL)

- telnet mailhost.computing.dcu.ie 25
- Opens an insecure shell to the mailhost on port 25
- When you make the connection on port 25 (the mail port), the mailserver says what it is and awaits commands.

```
Command Prompt
220 mailhost.computing.dcu.ie ESMTP Sendmail 8.13.2/8.13.2; Fri, 9 Apr 2010 13:46 +0100 (IST)
500 5.5.1 Command unrecognized: ""
help
214-2.0.0 This is sendmail version 8.13.2
214-2.0.0 Topics:
214-2.0.0      HELO      EHLO      MAIL      RCPT      DATA
214-2.0.0      RSET      NOOP      QUIT      HELP      URFY
214-2.0.0      EXPN      UVERB     ETRN      DSN        AUTH
214-2.0.0      STARTTLS
214-2.0.0 For more info use "HELP <topic>".
214-2.0.0 To report bugs in the implementation send email to
214-2.0.0      sendmail-bugs@sendmail.org.
214-2.0.0 For local information send email to Postmaster at your site.
214 2.0.0 End of HELP info
helo dcu.ie
250 mailhost.computing.dcu.ie Hello staff-195.computing.dcu.ie [136.206.115.19]
, pleased to meet you
mail from
501 5.5.2 Syntax error in parameters scanning "from"
mail from: theboss@dcu.ie
250 2.1.0 theboss@dcu.ie... Sender ok
rcpt to: brian.stone@dcu.ie
250 2.1.5 brian.stone@dcu.ie... Recipient ok
data
354 Enter mail, end with "." on a line by itself
This is the Boss here!
250 2.0.0 o39CDkRI019413 Message accepted for delivery
quit
221 2.0.0 mailhost.computing.dcu.ie closing connection

Connection to host lost.
C:\>
```

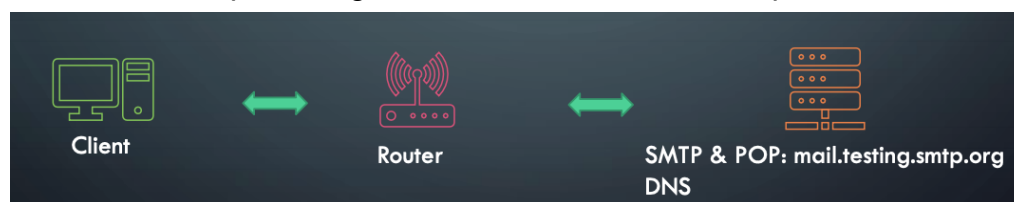


USING EMAIL

- Using an email client to send\receive email
 - Specify your email address
 - A password for the account
 - Name of outgoing mailservr
 - Name of incoming mail server
- User must present a password to retrieve email
- Mail may be sent without a password

SAMPLE CONFIGURATION

- Here is the sample configuration used for the email capture files



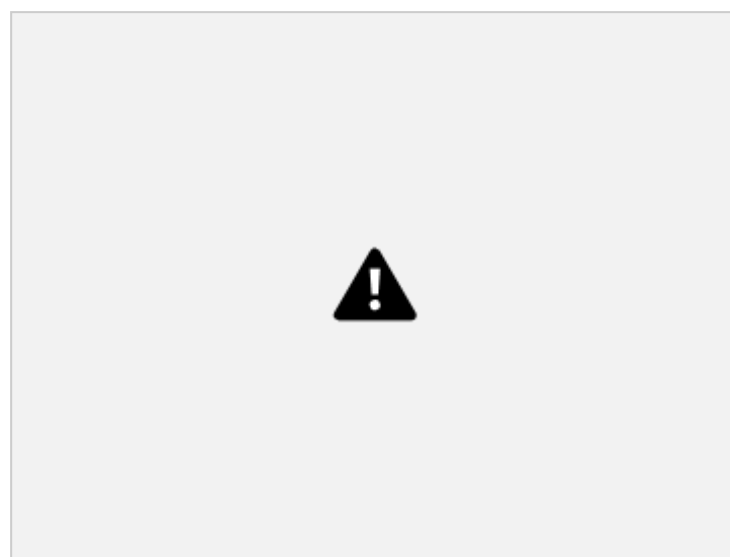
CONFIG NOTES

- The server runs DNS, SMTP and POP3 on the Linux OS
- The client also runs Linux on a laptop
 - The gmail package is running
- The dummy domain for this is testsmtp.org
- Two mail accounts setup on the mail servers
 - sendmemail@testingsmtp.org
 - netwatcher@testingsmtp.org
- Outgoing mail is directed to
 - mail.testingsmtp.org
- Incoming is directed to
 - pop3.testingsmtp.org
- Many servers may be configured on a single physical machine, in this case 192.168.32.206
- SMTP listens on port 25
- POP3 listens on port 110
- The machine also runs a DNS so the host name testingsmtp.org can be translated into the IP address of the server

The image shows a Wireshark packet capture window titled 'plain_smtp.cap - Wireshark'. The packet list pane shows 23 packets. The selected packet is packet 1, a DNS Standard query AAAA mail.testingsmtp.org. The packet details pane shows the following information:

- Frame 1 (80 bytes on wire, 80 bytes captured)
- Ethernet II, Src: 08:00:5b:ca:3b:bc (08:00:5b:ca:3b:bc), Dst: 08:00:5b:ca:3b:bc (08:00:5b:ca:3b:bc)
- Internet Protocol, Src: 192.168.32.208 (192.168.32.208), Dst: 192.168.32.206 (192.168.32.206)
- User Datagram Protocol, Src Port: 32898 (32898), Dst Port: 53 (53)
- Domain Name System (query)

The packet bytes pane shows the raw data of the DNS query.



OUTGOING MAIL

- Look at the Wireshark capture file
- plain.smtp.cap
- netwatch@testingsmtp.org sends an email from the laptop
- Things start off with several DNS requests (P1,P3,P5) and ask for the address of the outgoing mail server
 - mail.testingsmtp.org
- P1,P3 are AAAA requests for compatibility with IP V6, not really interested in that
 - P5 is a DNS A record, responded to by server with IP 192.168.32.206
 - P7 is a PTR request to translate 192.168.32.206 back to a machine name (to be sure)
 - Server responds with name mail.testingsmtp.org
- P9 a TCP connection is initialised to port 25 on 192.168.32.206 (email well known port)
- P12 from server is a greeting
 - 220 Welcome! Please send your message! ESMTP
 - Ready and speaks Extended SMTP
- P16 client responds
 - EHLO laptop.testingsmtp.org (EHLO is extended HELO)
 - Thus laptop is identified
- P14,P15 issues DNS requests to validate ID of client
- SMTP servers today are configured to identify the email clients and to allow only those on their LAN to send outgoing email
- This prevents them from being used to send lots of spam or to hide the true source of the email (address spoofing)
- As before with HTTP, you can follow the entire TCP trace by going to the Analyse menu and choosing Follow TCP Stream from the menu

SMTP TRANSFERS

- Commands
- MAIL FROM specifies email address of sender
- RCPT TO specifies address of recipient, may be many
- DATA the body of the email itself, terminated by a single dot "." on a line by itself (CRLF.CRLF) (carriage return line feed)

DATA SECTION

- Headers
 - subject, from, to, content-type etc. and the message itself
 - Used for display purposes when viewed by recipients
- After the data section, another email could start off again, so emails may be batched together when sending over the SMTP connection
- Terminates with a RSET and QUIT

The image shows a Wireshark capture of an SMTP session. The packet list on the left shows various DNS queries and responses, followed by a TCP connection establishment (SYN, ACK) and SMTP commands (EHLO, MAIL FROM, RCPT TO, DATA). The packet details pane on the right shows the structure of the SMTP message, including the envelope and the message body. The packet bytes pane at the bottom shows the raw data of the captured packets.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.32.208	192.168.32.206	DNS	Standard query AAAA pop3.testingsmtp.org
2	0.000955	192.168.32.206	192.168.32.208	DNS	Standard query response
3	0.003264	192.168.32.208	192.168.32.206	DNS	Standard query AAAA pop3.testingsmtp.org
4	0.003897	192.168.32.206	192.168.32.208	DNS	Standard query response
5	0.003949	192.168.32.208	192.168.32.206	DNS	Standard query A pop3.testingsmtp.org
6	0.004141	192.168.32.206	192.168.32.208	DNS	Standard query response A 192.168.32.100
7	0.004553	192.168.32.208	192.168.32.206	DNS	Standard query PTR 100.32.168.192.in-addr.arpa
8	0.004624	192.168.32.206	192.168.32.208	DNS	Standard query response PTR pop3.testingsmtp.org
9	0.004851	00d0:59ca:39db	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.32.100? Tell 192.168.32.208
10	0.004943	00d0:59ca:39db:88	00d0:59ca:39db	ARP	192.168.32.100 is at 00d0:59ca:39db:88
11	0.004955	192.168.32.208	192.168.32.100	TCP	33173 > 110 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
12	0.005352	192.168.32.100	192.168.32.208	TCP	110 > 33173 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
13	0.005385	192.168.32.208	192.168.32.100	TCP	33173 > 110 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=15
14	0.007343	192.168.32.100	192.168.32.208	POP	Response: +OK <24906.1074667309@pop3.testingsmtp.or
15	0.007359	192.168.32.208	192.168.32.100	TCP	33173 > 110 [ACK] Seq=1 Ack=46 Win=5840 Len=0 TSV=1
16	0.007420	192.168.32.208	192.168.32.100	POP	Request: CAPA
17	0.007508	192.168.32.100	192.168.32.208	POP	110 > 33173 [ACK] Seq=46 Ack=7 Win=5792 Len=0 TSV=7
18	0.007549	192.168.32.100	192.168.32.208	POP	Response: -ERR authorization first
19	0.137339	192.168.32.208	192.168.32.100	TCP	33173 > 110 [ACK] Seq=7 Ack=72 Win=5840 Len=0 TSV=1
20	4.809091	192.168.32.208	192.168.32.100	POP	Request: USER sendemail
21	4.809352	192.168.32.100	192.168.32.208	POP	Response: +OK
22	4.809381	192.168.32.208	192.168.32.100	TCP	33173 > 110 [ACK] Seq=24 Ack=78 Win=5840 Len=0 TSV=
23	4.809665	192.168.32.208	192.168.32.100	POP	Request: PASS madeyoulook
24	4.818489	192.168.32.100	192.168.32.208	POP	Response: +OK
25	4.821921	192.168.32.208	192.168.32.100	POP	Request: CAPA

Frame 1 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: 00d0:59ca:39db (00d0:59ca:39db), Dst: 0050:040e:bd88 (0050:040e:bd88)
Internet Protocol, Src: 192.168.32.208 (192.168.32.208), Dst: 192.168.32.206 (192.168.32.206)
Hypertext Transfer Protocol, Seq: 33173, Port: 80, Len: 80
0000 00 50 04 0e bd 88 00 d0 59 ca 39 db 08 00 45 00Y.9...E
0010 00 42 06 49 40 00 00 11 b1 72 c0 a8 20 d0 c0 a8R.H.B.B. J...
0020 20 0e 80 17 00 35 00 2e a1 eb 05 bb 01 00 00 01S.....
0030 00 00 00 00 00 00 04 70 6f 70 33 0b 74 65 73 74op3.test

INCOMING MAIL

- pop3_initial.cap has the retrieved client side email
- P1-P8 contain DNS interactions
- P11 the POP connection starts. POP3 is version 3 of the Post Office Protocol POP
- Server speaks first
 - +OK24906.1074667309@pop3.testingsmtp.org
- CAPA is first command issued by client, requests that server return a list of capabilities including saying which authorisation mechanisms it supports
 - Server does not do this (it is an extension of the basic protocol) and answers –ERR authorisation first
- Client sends username and password in plain text with USER and PASS commands.
- Server responds that both are OK
- Client once again tries CAPA, server responds –ERR unimplemented, so authorisation was required to get anything out of the server
- UIDL 1, LIST and UIDL commands used to gather information about user `sendmemail@testingsmtp.org`
- There are 2 messages
- LIST returns a list of messages with their size in bytes
- UIDL returns a list of messages with an identification number
 - POP does not specify how these numbers are assigned exactly
- LIST and UIDL provide information to client to allow it to decide whether to download the messages
 - May look at identification number to see if it has it already
 - Look at the size to see if it is too big do download over perhaps a slow network.
- RETR 1 requests that message 1 be sent over the channel.
- This is the message sent in plain.smtp.cap

EMAIL HEADERS

- Received emails carry a lot of information in their headers, more than outgoing email
- Email servers add headers as they process the email
- Take the email from the Wireshark file
- Start with header immediately above Subject header
 - First line added is “Received from laptop.testingsmtp.org (192.168.32.208) by mail.testingsmtp.org with SMTP; 21 Jan 2004 06:40:40 -0000”
 - Second line added, “Received (gmail 24897 invoked from network); 21 Jan 2004 06:40:40 -0000” This indicates that as soon as it was received by the SMTP server from the client, it transferred the message to the gmail server.
 - gmail placed it in the user `sendmemail@tectingsmtp.org` and added the header “Delivered-To: sendmemail.testingsmtp.org”
 - gmail adds a Return-Path header to reflect the contents of the MAIL FROM field used in transferring the message
- Full set of headers sent to recipient, you can see them by turning on full headers in your email client.
- Headers are useful in tracking unwanted email
- Headers can be forged!

POP3

- Simple download and delete (optional)
- Uses well-known port 110
- May be encrypted with TLS or SSL on well-known TCP port 995 (gmail does this)
- RFC 1939 and RFC 2449 and RFC 1734
- No new proposals since 2003
- IMAP is now becoming the more common one to use

IMAP

- Set up your email client to use either POP or IMAP
- Some advantages over POP
- Download only the headers, download full emails one, by one
- Track state of messages, been read, replied to, deleted, state stored on server
- Multiple clients on same mailbox (forbidden in POP)
- Stay connected or not, for users with many or large messages, may result in faster response times.