CA169: Week 11

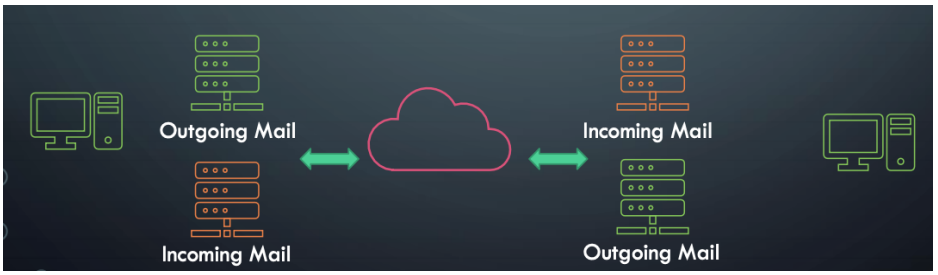
Email - SMTP, POP, IMAP

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

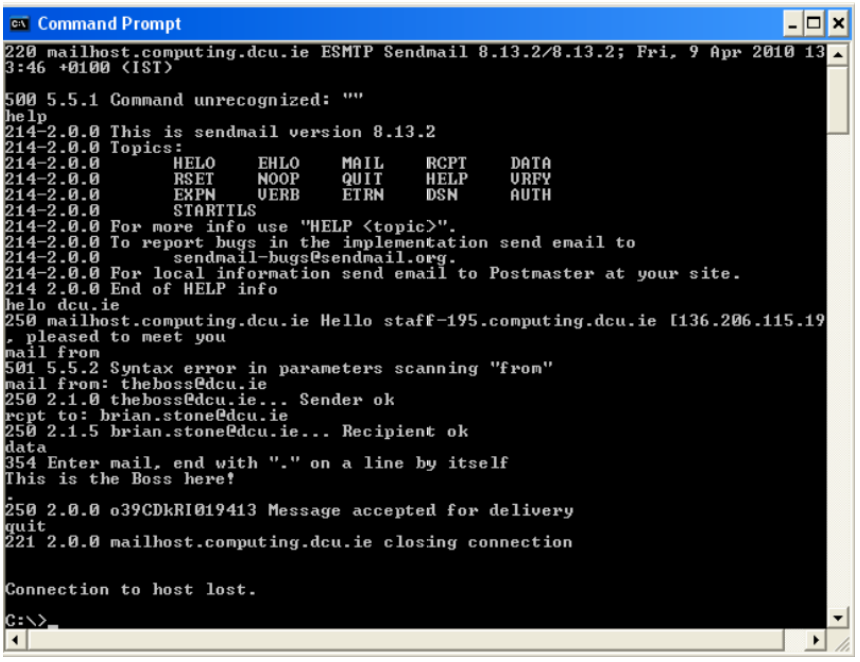


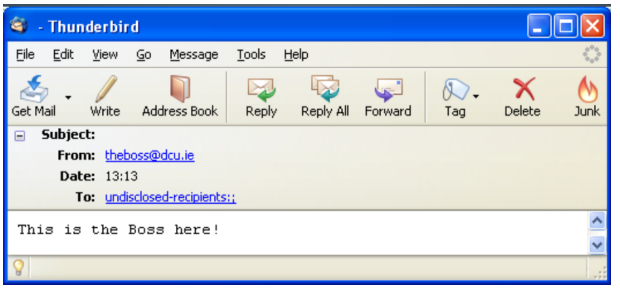
SENDING MAIL (SMTP)

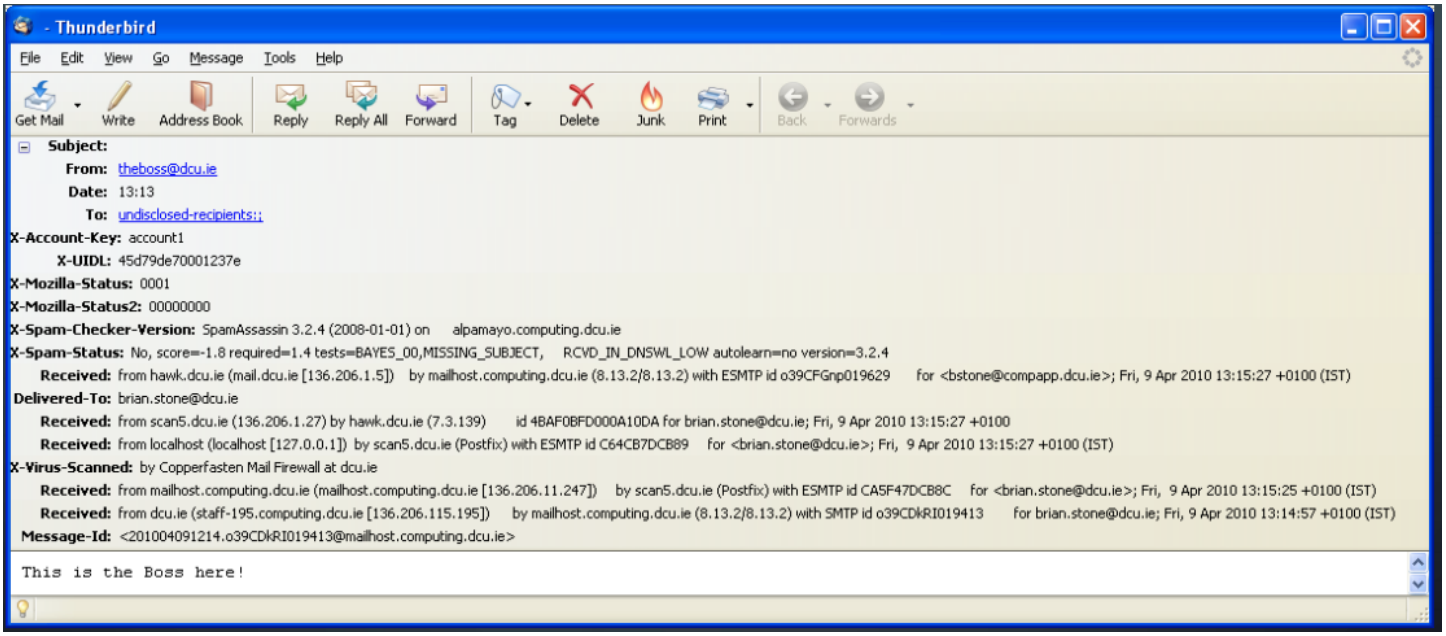
- Sending mail is handled by mailservers
- Your local mail server (gmail) takes responsibility to deliver the mail
- It is sent to the recipients incoming mail server

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.





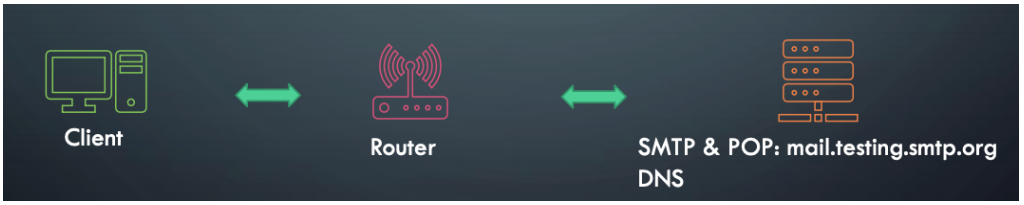


USING EMAIL

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

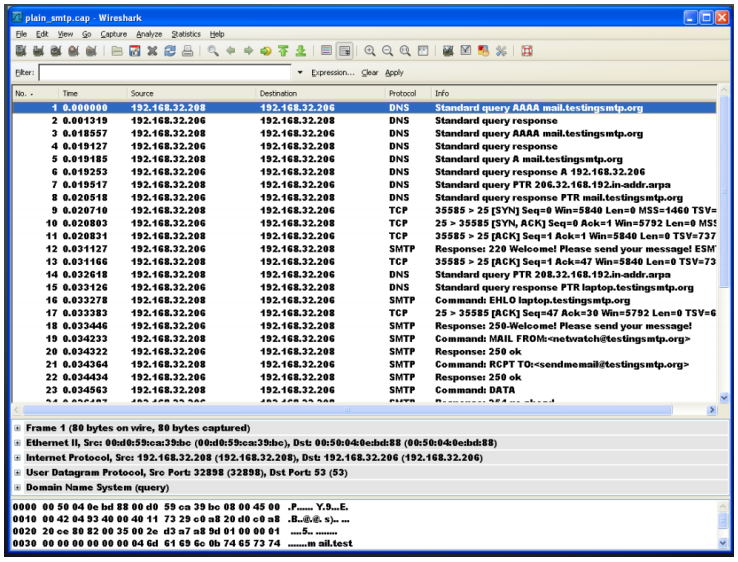
SAMPLE CONFIGURATION

- 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 qmail 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



OUTGOING MAIL

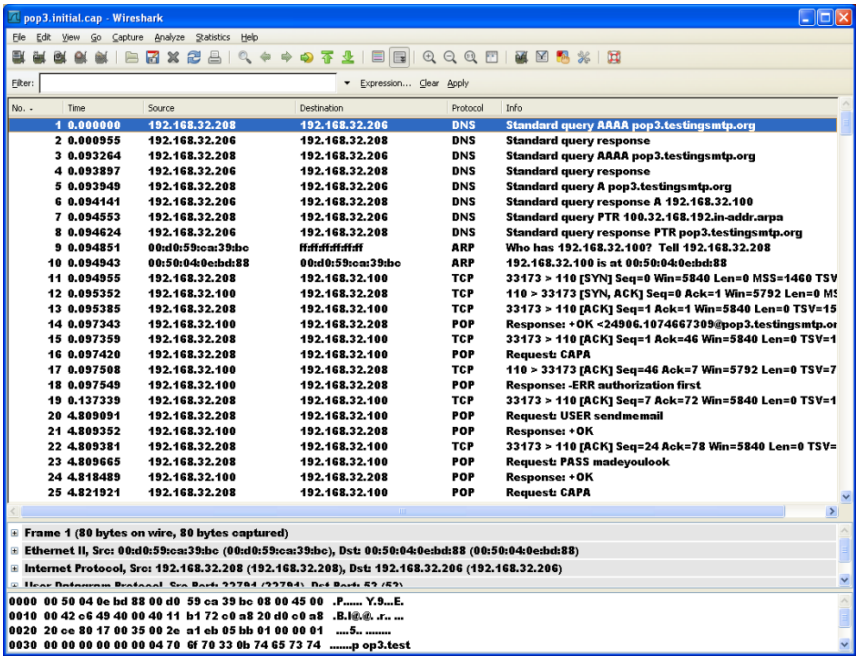
- Look at the Wireshark capture file
- plain.smtp.cap
- `netwatch@testingsmtp.org` sends an email from the laptop
- Things start off with several DNS requests (P1,P3,P5) and ass for the address of the outgoing mail server
    - `mail.testingsmtp.org`
- P1,P3 are AAAA requests for compatibility with IP 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 me 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



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 (qmail 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 qmail server.
    - qmail placed it in the user sendmemail@tectingsmtp.org and added the header “Delivered-To: sendmemail.testingsmtp.org”
    - qmail 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 massages, 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.