DFSC 1316: digital forensic and information assurance fundamentals I

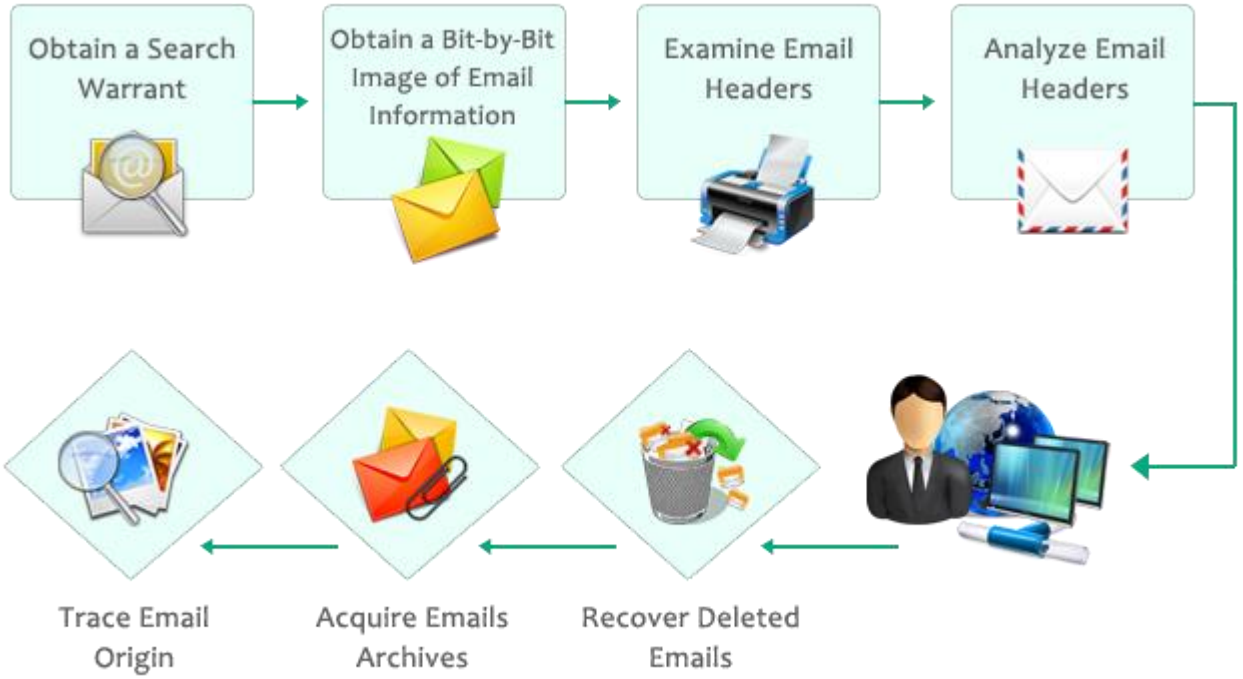
6. E-mail forensics

Introduction

E-mail has transcended social boundaries and moved from a convenient way to communicate to a corporate requirement. In many cases, incriminating unintentional documentation of people's activities and attitudes can be found through computer forensics of e-mail.

Investigating E-mail Crimes and Violations

- Broad steps of email investigation

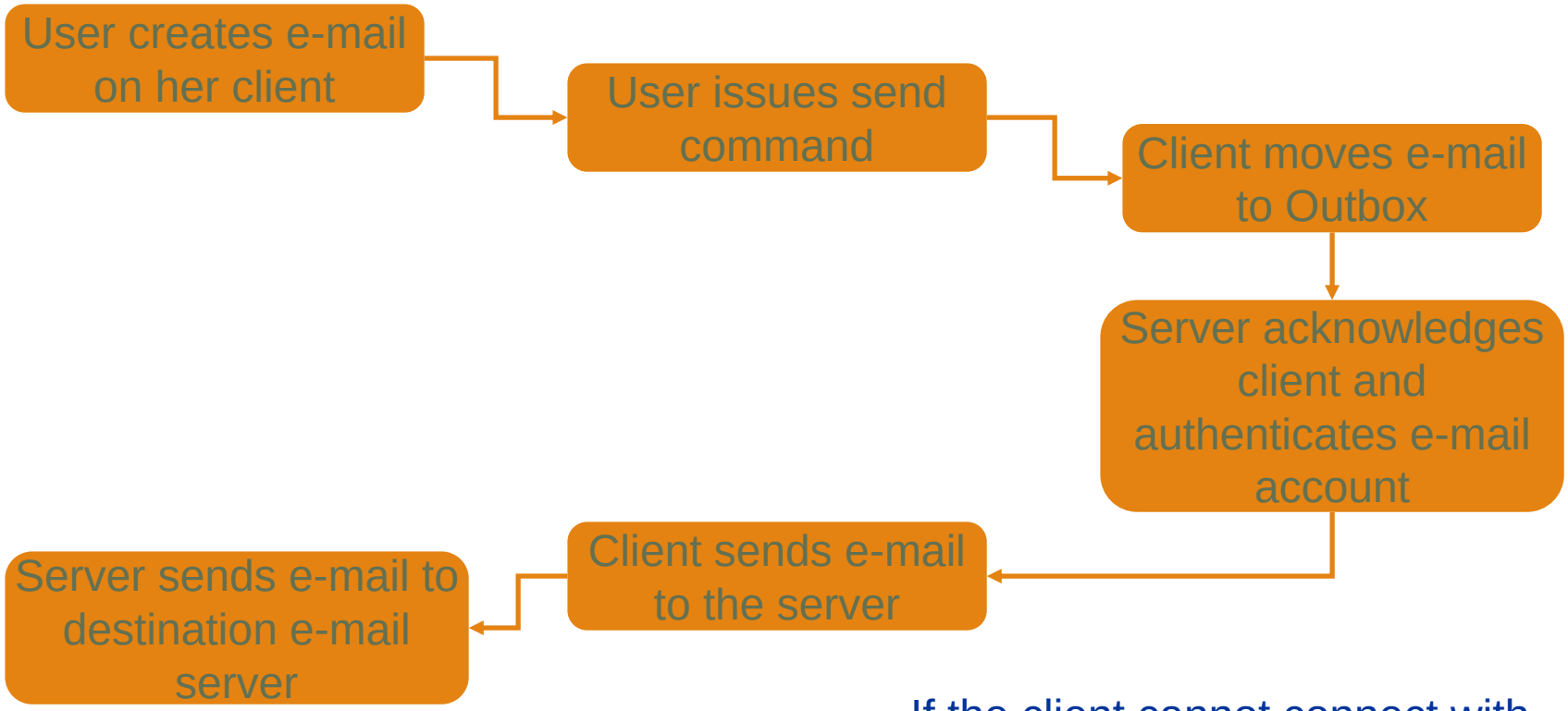


Importance of E-Mail as Evidence

- E-mail can be pivotal evidence in a case
- Due to its informal nature, it does not always represent corporate policy
- Many cases provide examples of the use of e-mail as evidence
  - *Knox v. State of Indiana*
  - *YouTube v. …*

Sending E-Mail with a Client

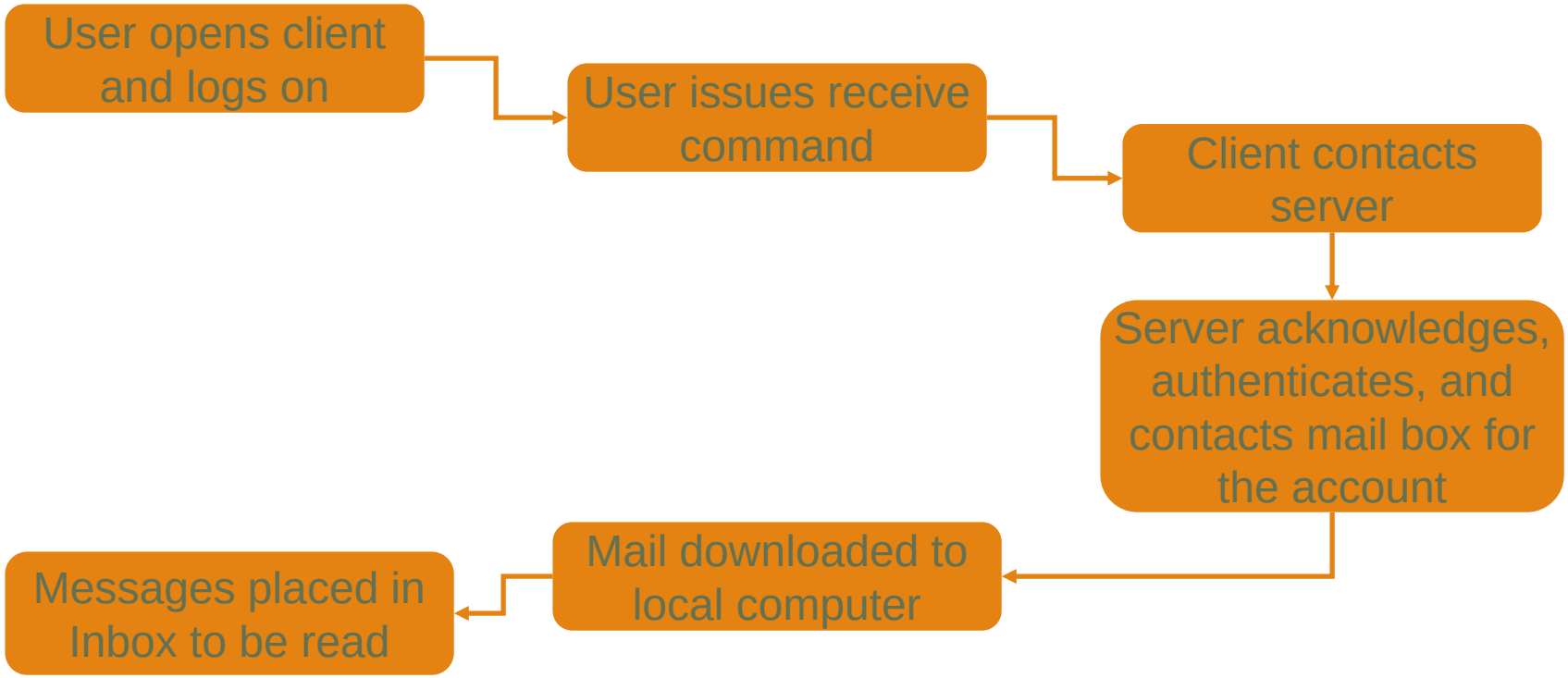
Sending E-Mail



If the client cannot connect with the server, it keeps trying

Receiving E-Mail with a client

Receiving E-Mail



POP deletes messages from server;
IMAP retains copy on server

Webmail

- Webmail data flow
  - User opens a browser, logs in to the webmail interface
  - Webmail server has already placed mail in Inbox
  - User uses the compose function followed by the send function to create and send mail
  - Web client communicates behind the scenes to the webmail server to send the message
  - No e-mails are stored on the local PC; the webmail provider houses all e-mail

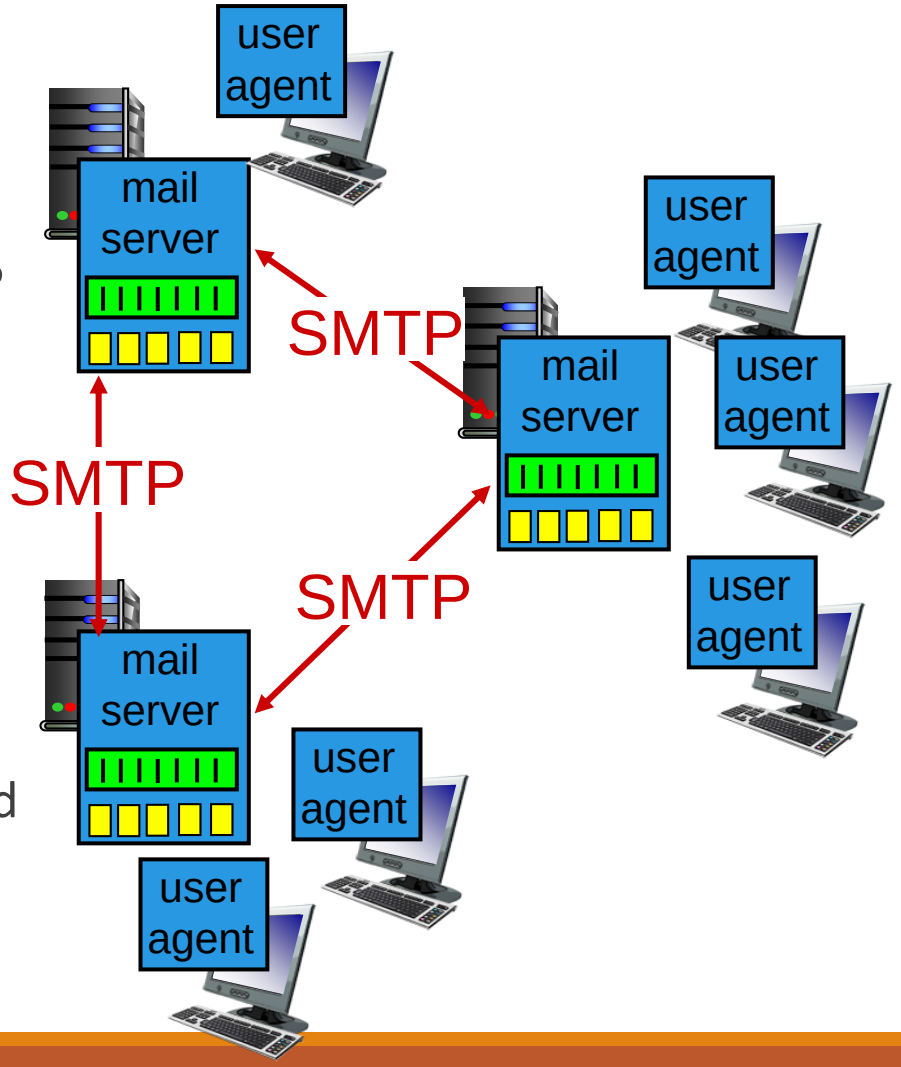
Electronic mail

Three major components:

- user agents
- mail servers
- simple mail transfer protocol: SMTP

User Agent

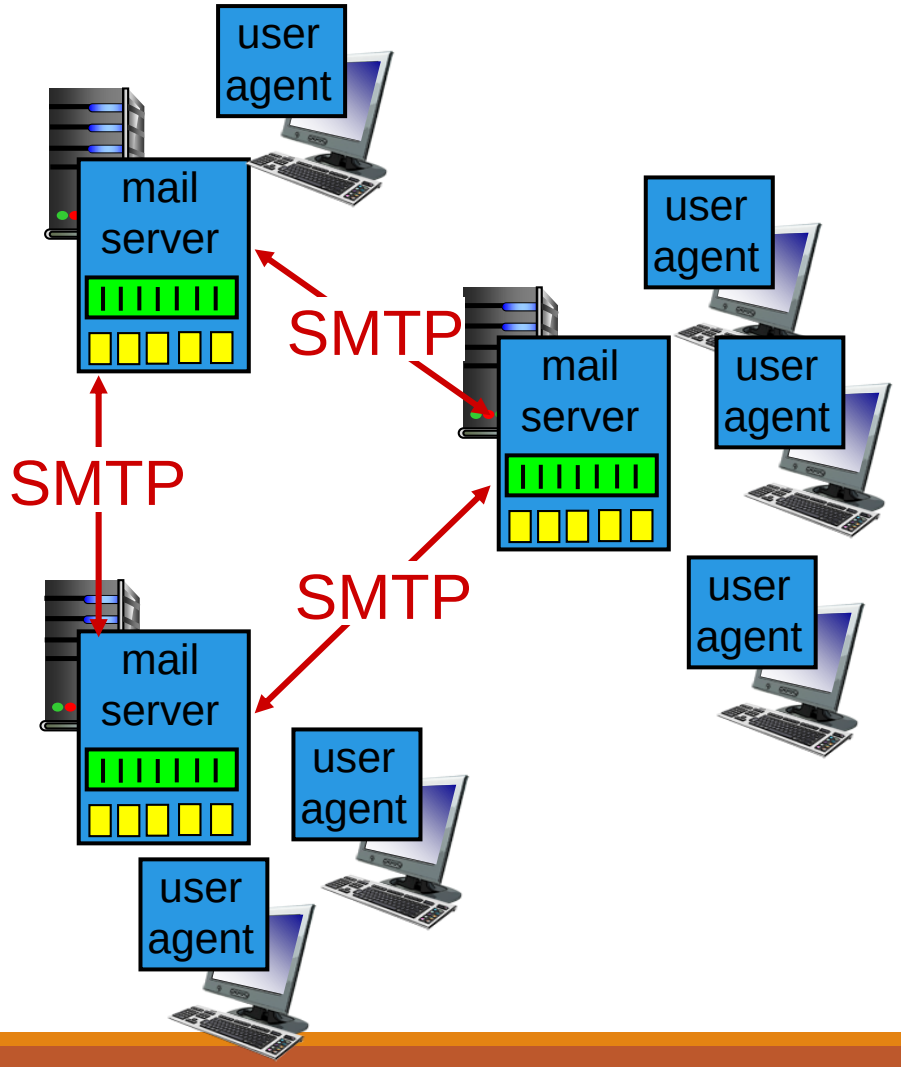
- a.k.a. “mail reader”
- composing, editing, reading mail messages
- e.g., Outlook, Thunderbird, iPhone mail client
- outgoing, incoming messages stored on server



Electronic mail: mail servers

mail servers:

- *mailbox* contains incoming messages for user
- *message queue* of outgoing (to be sent) mail messages
- *SMTP protocol* between mail servers to send email messages
  - client: sending mail server
  - "server": receiving mail server



Electronic Mail: SMTP [RFC 2821]

- uses TCP to reliably transfer email message from client to server, port 25
- direct transfer: sending server to receiving server
- three phases of transfer
  - handshaking (greeting)
  - transfer of messages
  - closure

Scenario: Alice sends message to Bob

1) Alice uses UA to compose message "to" `bob@someschool.edu`

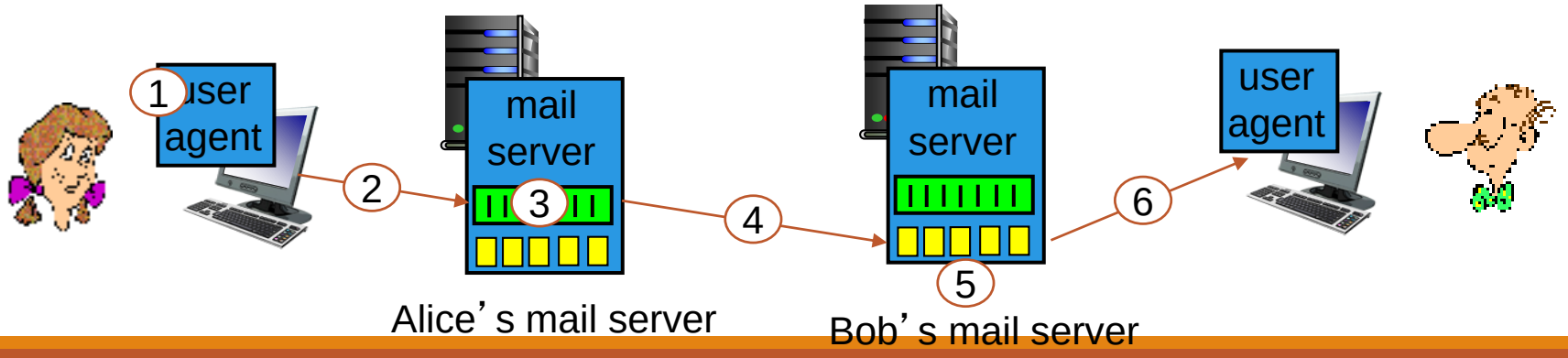
2) Alice's UA sends message to her mail server; message placed in message queue

3) client side of SMTP opens TCP connection with Bob's mail server

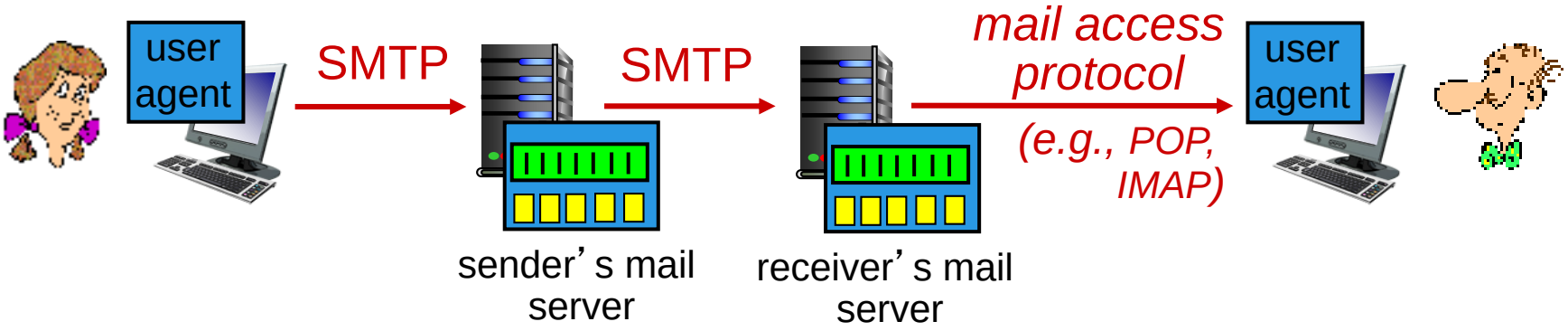
4) SMTP client sends Alice's message over the TCP connection

5) Bob's mail server places the message in Bob's mailbox

6) Bob invokes his user agent to read message



Mail access protocols



SMTP: push mail to receiver's server

mail access protocol: retrieval from server

- POP: Post Office Protocol [RFC 1939]: authorization, download
- IMAP: Internet Mail Access Protocol [RFC 1730]: more features, including manipulation of stored messages on server
- HTTP: gmail, Hotmail, Yahoo! Mail, etc.

Try SMTP interaction for yourself:

- **`telnet servername 25`**
- see 220 reply from server
- enter HELO, MAIL FROM, RCPT TO, DATA, QUIT commands

above lets you send email without using email client (reader)

Sample SMTP interaction

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

E-mail Header

- Understanding e-mail headers
  - The *header* records information about the sender, receiver, and servers it passes along the way
  - Most e-mail clients show the header in a short form that does not reveal IP addresses
  - Most programs have an option to show a long form that reveals complete details

E-Mail Header

- Most common parts of the e-mail header are logical addresses of senders and receivers
- Logical address is composed of two parts
  - The *mailbox*, which comes before the @ sign
  - The *domain* or *hostname* that comes after the @ sign
    - The mailbox is generally the userid used to log in to the e-mail server
    - The domain is the Internet location of the server that transmits the e-mail

E-Mail Header

- Information in the email header that indirectly will help the forensics process:
  - Sender of the email
  - Network path it traversed and path of origination
  - SMTP Servers it went through
  - Time Stamp Detail
  - Email Client information
  - Encoding information

E-Mail Header

- Where to find email header
  - Outlook:
    1. Open a mail
    2. Click on “file” tab
    3. Select “properties”

  - Gmail
    1. From a browser, open Gmail.
    2. Open the email you want to check the headers for.
    3. Next to “Reply”, click the Down arrow.
    4. Click “Show original”.

E-Mail Header

- Online automated tools are available for parsing email headers.
  - For example: https://mxtoolbox.com/EmailHeaders.aspx

Crime Related to E-Mail

- Email spamming
- Mail bombing
- Phishing
- Email spoofing

Related Laws

- **The CAN-SPAM Act of 2003** establish requirements for those who send commercial emails, spells out penalties for spammers and companies whose products are advertised in spam.
- According to the **Electronic Communications Privacy Act**, emails that stored on a 3-party server can be searched by government after 180 days.