Email Crimes

Forensic Science
Emails have enabled an efficient means of communication, without the limitations of time zones, speed or cost, usually associated with many of the other forms of communication. Though advantageous in this manner, emails can easily be used for negative purposes as well, making SPAM and virus emails a problem. This section covers some basics that the everyday email user can do to trace down an offending email sender.
An IP Address

- IP addresses are an effective means used to track down and differentiate between different computers. Each computer's IP address is therefore, naturally unique, composed of 32 bits and grouped into four lots of eight bits. The IP address is recorded every time your computer makes contact with a server, including when you first log on with your ISP (internet service provider) to when you access different web pages. Different websites also have an IP address composed of bits, but for convenience, the long chain of numerals is instead interpreted into an easier-to-remember word address using a domain name service (DNS). During the trace back of an email message, the IP address of the various protocols used to transfer the email from one location to another can be quite useful.
Email Programs

- There are a variety of email programs used to manage, store and compose emails. Email programs such as Outlook and Eudora specialise in encoding and decoding received email messages, to make them understandable, not unlike the encryption and decryption process described in the next section, but slightly simpler. All of the encoding is mapped to an email standard, a form of coding which holds information for the posting of messages from place to place. Some common email standards are MIME (multipurpose internet mail extensions) and uuencode, of which the latter is more often used in attempts to hide information in a message, but can be easily decoded by various decoding utilities that come with major operating systems.
Email Logs

- Email logs are generally kept on all email servers, being a record of the emails which were sent, received, the email addresses involved and the time/date of posting/receipt. However, it may be a problem if some servers use what is known as circular logging, where a certain amount of data space is allocated for the storage of log files, but once this space is full, the beginning (earliest of the log files) is overwritten and this overwritten data is deleted for good. The log files are commonly formatted into just plain text and their main use is for identifying the source of the offending email/s. Different email servers have different forms of email logs, but the information these files provide are the same.
Email Headers

- Email headers prove information not unlike that of an email log, but details the path the email took in terms of which protocols were used to transfer the messages and thus work backwards.

- The return path of the email, the email address to which your email program will send a reply, is often not the source of the message when an offender deliberately tries to disguise his/her tracks.

- Each email also has a unique message ID, which may correspond to data contained in a message log.

- This information is not normally shown by default, but is easily accessible in most email programs. For example, Microsoft Outlook displays this information when the property of an email is displayed and 'view source' is chosen.

- The screen to the left is an example 'message source' of the welcome message Microsoft Outlook sends.