If a message has an attachment, the name of the attachment is shown in the header itself. Attachments serve as supporting evidence in an investigation. An investigator should search for the attachment on the victim's hard drive. After retrieving the file, the investigator can copy it to preserve the evidence.

**“Received” Headers**

“Received” headers provide a detailed log of a message's history, and they make it possible to draw some conclusions about the origin of an e-mail, even when other headers have been forged.

If, for instance, the machine turmeric.com, whose IP address is 104.128.23.115, sends a message to mail.bieberdorf.edu, but falsely says HELO galangal.org, the resultant “Received” line might start like this:

```
Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...
```

**Forging “Received” Headers** A common trick e-mail forgers use is to add spurious “Received” headers before sending the offending mail. This means that the hypothetical e-mail sent from turmeric.com might have “Received” lines that look something like this:

```
Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...
Received: from nowhere by outer space (8.8.3/8.7.2)...
Received: This is a header. Move along.
```

The last two lines are complete nonsense, written by the sender and attached to the message before it was sent. Since the sender has no control over the message once it leaves turmeric.com, and “Received” headers are always added at the top, the forged lines have to appear at the bottom of the list.

This means that someone reading the lines from top to bottom, tracing the history of the message, can safely throw out anything after the first forged line; even if the “Received” lines after that point look plausible, they are guaranteed to be forgeries.

**Common Headers**

The following is a list of some common headers:

- **Content-Transfer-Encoding**: This header relates to MIME, a standard way of enclosing nontext content in e-mail. It has no direct relevance to the delivery of mail, but it affects how MIME-compliant mail programs interpret the content of the message.

- **Content-Type**: This is another MIME header, telling MIME-compliant mail programs what type of content to expect in the message.

- **Date**: This header specifies a date, normally the date the message was composed and sent. If the sender’s computer omits this header, it might conceivably be added by a mail server or even by some other machine along the route.

- **Errors-To**: This header specifies an address for mailer-generated errors, such as bounce messages, to go to (instead of the sender's address). This is not a particularly common header, as the sender usually wants to receive any errors at the sending address, which is what most mail server software does by default.

- **From**: This is whom the message is from.

- **Apparently-to**: Messages with many recipients sometimes have a long list of headers of the form “Apparently-to: rth@bieberdorf.edu” in them. These headers are unusual in legitimate mail; they are normally a sign of a mailing list, and in recent times mailing lists have generally used software sophisticated enough not to generate a giant pile of headers.

- **Bcc**: This stands for “blind carbon copy.” If this header appears in incoming mail, something is wrong. This header is used to send copies of e-mails to people who might not want to receive replies or to appear in the headers. Blind carbon copies are popular with spammers, since they confuse many inexperienced users who get e-mail that does not appear to be addressed to them.

- **Cc**: This stands for “carbon copy.” This header specifies additional recipients beyond those listed in a “To” header. The difference between “To” and “Cc” is essentially connotative; some mailers also deal with them differently in generating replies.

- **Comments**: This is a nonstandard, free-form header field. Some mailers add this header to identify the sender; however, spammers often add it by hand (with false information).