

CyberBytes

E-Mail Metadata and Headers

Metadata may be important to authenticate or establish the route taken by an e-mail. There are many metadata or “header” elements available in e-mail. E-mail headers and metadata are important because they contain valuable information about the message. Forensic experts can use this information to determine whether the message was forged, spoofed or falsified and to identify the sender or the computer from which the message was created.

BCC	This acronym stands for blind copied and means that a recipient of e-mail whose name is not visible to other recipients of the e-mail. It will not appear on a printout unless it is the sender's e-mail copy that is printed.
CC	Additional recipients who received the e-mail.
Date	The date on which the message was sent
Encrypted	Methodology used to encrypt the e-mail.
From	Sender's e-mail identity.
In-Reply-To	Identifies previous e-mail answered by this message
Message-ID	Unique machine ID for this particular e-mail. May be useful to authenticate e-mail.
Received	Shows the time when the recipient received the message and the route traveled from the sender's computer to the recipient's computer. This information may assist with authenticating e-mail. Also, it may indicate if other storage devices should be examined to locate e-mail.
References	Identifies previous e-mail referenced by this message. May be useful in authentication and validation check of whether other e-mail has been disclosed.
Resent	Provides information if the e-mail has been resent — bcc, cc, date, from, sender, path, etc.
Return-Path	Shows the address and route back to sender of e-mail.
Time and Date	Shows when e-mail was sent.
Sender	Shows the address of the user who sent the e-mail.
Subject	Displays the subject of the e-mail.
To	Shows the primary recipients of the e-mail

To view metadata, you must obtain the native computer file (e.g. Microsoft Outlook® .pst file) or enlist the services of a computer forensics firm to acquire the subject e-mails off of the computer hard drive on which the e-mail was originally created. Metadata will not be present in a paper document production or with an electronic TIFF or PDF format.

Reported Cases:

- *Armstrong v. Executive Office of the President*, 821 F. Supp. 761, 773 (D.D.C. 1993). The Court ordered restoration of backup tapes of e-mail records, holding that government e-mail is a record as defined by the Federal Records Act, and that it was insufficient for the government to preserve only the paper printouts of the e-mail.
- *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652-54 (D. Minn. 2002). “Simply booting a computer can possibly destroy valuable metadata . . . that could be relevant in a lawsuit.”
- *N.A.A.C.P. v. Acusport Corp.*, 210 F.R.D. 268 (E.D.N.Y. 2002). The Court discussed database metadata: “The BATF has produced two annotated data dictionaries that identify what data is contained in its databases and how it is arranged. *Data dictionaries are repositories of metadata, or information about data, such as its meaning, relationships to other data, origin, usage, and format.* Two dictionaries were necessary because, as indicated before, the FTS and FLS are separate databases maintained on separate servers.” (emphasis supplied).