



DataSec White Paper

Evidential Value of Email

DataSec Limited

Allen House
Station Road
Sawbridgeworth,
Hertfordshire
CM21 9JX.

UK

Tel. +44 (0)1279 313007

Fax +44 (0)1279 313130

Email office@datasec.co.uk

A White paper on the Evidential value of email

Philip Bowles, Senior Forensic Analyst, DataSec Ltd

Simon Belfield, Partner, Frisby & Co Solicitors

John Cooper, Leading criminal barrister and "The Times" legal media columnist

Executive summary

Email is significantly different from paper mail. In normal use it leaves a digital audit trail. A knowledgeable person can forge parts of that audit trail and the mail itself with relative ease. Verification of that audit trail is therefore essential if "best evidence" is to be presented. In a case where allegations are made that email was never sent or received, a paper-based copy of an email without that audit trail is significantly devalued evidentially.

Differences

While physical evidence has been well understood by the all parties in the court process for centuries, email is non-physical electronic concept whose public perception can be measured in less than two decades. It is created, managed and delivered by a technology that creates as similar an apprehension and bewilderment as does "rocket science" to the majority of people outside of the IT industry.

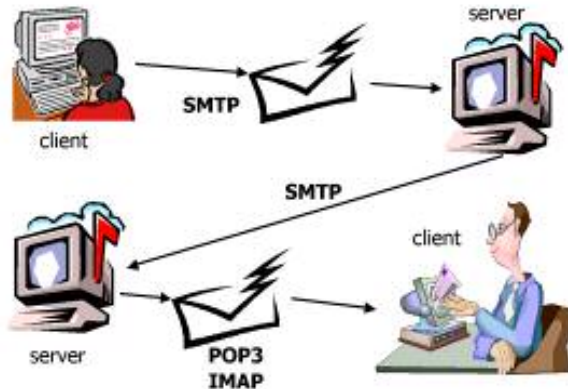
It is human nature to draw analogies between new concepts and old as an aid to understanding. This is true of email in the legal process where it is explained and examined in terms of its similarity with conventional mail. There is always a danger with this approach that the analogy can be stretched beyond the point where it truly relates to the newer concept.

To demonstrate this point, consider the following scenarios that are eminently possible in the email world, but beyond comprehension in the world of conventional mail:

- Mail is not stolen, diverted or lost but simply spontaneously vanishes into thin air
- Between one letter and the next, the sorting office relocates itself to another country (and therefore jurisdiction)
- A mail is altered, its envelope changed, the postmark tampered with and no physical evidence is produced
- A single letter is simultaneously delivered to multiple recipients
- The same mail appears visually different to two different viewers

These are merely a few of the reasons why email should not be treated evidentially in the same manner as "real mail". The "e" that precedes "Mail" may be a small one, but its effect is huge. Email is a pattern of digital pulses that are transmitted between two computers, according to strict rules or protocols. It is more a *process*, than a *thing*. A printed copy of an email is merely a visible representation of the results of that process, and by definition, no longer deserves the preceding "e". Paper is not electronic.

Email mechanics



Email is generally manipulated according to three protocols: Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3) and Internet Mail Access Protocol (IMAP). The "delivery" and "collection" process is often described as a "Client / Server" model, where the user (or client) requests that remote computer (or server) delivers an email to a recipient's electronic mailbox. The recipient then again acts as a client in requesting that the server holding his or her mailbox then makes that mail available for reading. It is a common occurrence for a single email to be passed from one server to another prior to being read by the final client - the recipient.

Commonly, SMTP is used to send mail to a server, and either POP3 or IMAP to then retrieve the mail. The major difference in the latter two is the conceptual location of the user's mailbox: in IMAP it is on the final server, in POP3 it is on the client's own machine. Generally when using POP3, the mail is deleted from the final server once delivered to the client's own machine, but it perfectly simple to leave a copy on the server also. Again *in general terms only*, an IMAP client is offered a remote "view" of his mailbox on the server, though he or she is at liberty to save copies locally and think of those local copies as his or her own "inbox".

An important point here is that for reasons of history and Internet topography, it is not uncommon for the intervening servers to exist physically outside of UK jurisdiction (frequently in the USA).

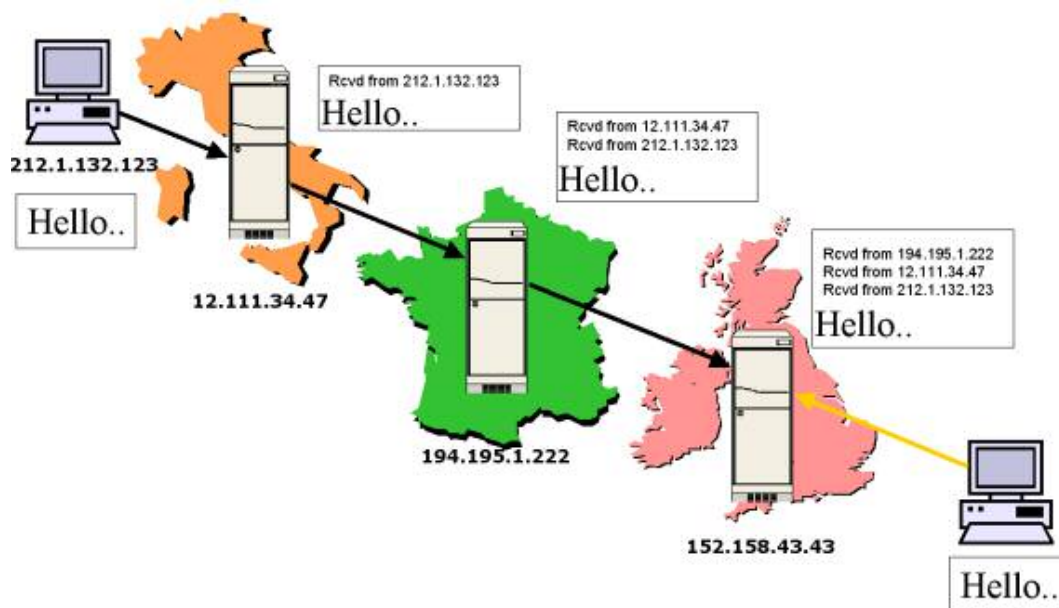
Audit trail / headers

Software that supports the SMTP protocol is commonly configured to maintain a log of mail that it has delivered locally or forwarded. The international nature of the Internet means that no rules or standards can be globally enforced - protocols are agreed between developers, ratified and approved organically and become *de facto* once they have gathered sufficient critical mass to edge out other competing protocols. This process is much like the adoption of VHS over Betamax - it "just happened". Because of this lack of regulation, many localised variations in procedures are able to exist.

Any software that conforms with the SMTP protocol at its lowest technical level is at liberty to perform any other task - determined solely by the whim of the developers. Such tasks could (and do) include deliberate removal or obfuscation of audit trail or logging information.

Until such time as the majority of international software developers agree new protocols that enforce different rules, investigators and legal practitioners must accept that sometimes logs and audit trails are *not* kept, and that almost nothing in the email world can be taken for granted. The radical concepts behind such a sea-change are explored in depth by Lawrence Lessig - Professor of Law at Stanford Law School - in his book "Code and other laws of cyberspace"

In the normal course of events, where audit trail data is not in doubt, each server adds what is known as a "header" to the front of each email prior to forwarding it. The header will show the Internet identity or "IP address" of the machine from which it received the mail, as the following diagram shows:



It is extremely important at this point to understand that this IP address is not necessarily unique over time. Different physical machines - even in different countries - can possess the same IP address at different times. One single machine therefore may identify itself with many different IP addresses on different occasions.

It is a broad generalisation that well established SMTP servers belonging to reputable organisations will tend to maintain the same IP address over long periods, whereas clients (especially home users) will have a dynamically-allocated IP address, i.e. one that it almost certain to be different - albeit within a known range - on each Internet connection.

With this in mind, an audit trail that is required to show - beyond reasonable doubt - the electronic path of an email must take into account all of these common variances, with strict regard to time, often across international time zones. Producing such an audit trail for presentation in court is likely therefore to be a non-trivial task.

The vast majority of email users have no need to view these headers - as long as "the mail gets through" they are of no further use. Their highly technical content is therefore usually hidden - or worse, removed - by most common email software. This gives rise to the dangerous evidential situation where a printed copy of the email as the user saw it - i.e. without the headers - is of very little value in itself as the sender, recipient and date - as seen - are easily forged.

The British Standards Institution, in their 1999 "Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically", have this to say with respect to audit trail data:

*"When preparing information for use as evidence, it is often necessary to provide further supporting information. This information may include details such as date of storage of the information, details of the movement of information from medium to medium and evidence of the controlled operation of the system. These details are known as 'audit trail' information. The audit trail as defined for the Code consists of the aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the information management system"*²

There seems to be no doubt then that the onus is upon whomever produces email evidence to support it with an audit trail if the *best evidence* is to be offered.

Forging of "Headers" and "Spam"

Most responsibly run SMTP servers are configured so that they will only forward or "relay" email for known clients or groups of computers. In this configuration, the server will usually check the authenticity of the recipient and/or sender in order to prevent unauthorised use. This greatly assists the investigator and lends much greater evidential weight to the audit trail.

There are many servers on the Internet however that are configured - whether by accident or design - as "open relays" i.e. they will forward mail for any client who asks. This lack of a requirement for authentication can allow a user to forward mail to another server, without being required to provide a valid sender's email address. This configuration lies at the heart of the growing problem of unsolicited commercial email or "spam" that any email user will be all too familiar with. The primary intent of the "spammer" is that the *true* source of the email cannot easily be determined - if it were, it is almost certain that his /her Internet access would be withdrawn by his/her service provider.

Another common -and simple - technique used by spammers is to add spurious headers to the email, or to alter the existing headers to include false information in a deliberate and often successful attempt to obfuscate the true source.

SMTP is merely a *contract* between two machines to *deliver* the mail - it has few rules regarding the validity or otherwise of its *content*.

The O'Reilly text "Stopping Spam"³ is an excellent resource for those wishing to look deeper into the subjects covered here.

More importantly for this paper, the same techniques may be used by criminals not only in the commission of an offence, but also to subvert the investigative and / or legal process. An experienced technician with authenticated access to an SMTP server can cause an email to be sent appearing to have come from almost any source and containing almost any content he / she desires. Even without such access, locating an SMTP open relay will allow even greater freedom and more choice of misdirection.

Freely downloadable software tools exist to search for open relays on the Internet, for example "Open Relay Checker" <http://www.openrelaycheck.com/orc/checker.asp>

R v Rowe / Bhatt

An excellent opportunity to demonstrate the nexus of the legal and technical issues involved is the case of R. Rowe and Bhatt (Canterbury Crown Court, February 2003). The case presented unique and significant challenges to the defence teams.

John Cooper, Leading Defence Counsel for Bhatt (instructed by Frisby & Co) presented to the Judge and Jury, during the course of the trial, a visual presentation, simulating a link to the Internet to create and explain how electronic communications can be manipulated in real time. A special room was provided by the court for this cutting edge demonstration which laid bare the hidden potential of electronic data processing and in particular, the ease with which emails may be forged.

At the conclusion of the demonstration, Philip Bowles, the defence expert witness forged an email in real time via the simulated Internet link that appeared to have been sent to the defendant Bhatt. When the email was then "read" with a standard email client (in this case, Microsoft Outlook Express) it appeared no different from the paper emails that were offered by the prosecution as "proof" that the email had in fact been sent to Bhatt. Only a full technical examination of the "headers" within the Outlook Express system would have shown anything to the contrary, and even then a significant amount of network investigation would have been required in support. The significance of the demonstration was not lost on the Judge and Jury.

John Cooper says:

"The internet, whilst for most an invaluable and legitimate tool for business and pleasure is also a growing regime which is being exploited by criminals. Long gone are the days when a forger sits at his desk with pen and ink painstakingly producing an engrossed document. The Internet liberates and not only the innocent but also those with guilty intent.

The Courts are becoming more and more amenable to receiving Internet generated documentation. There are no longer the statutory hurdles that were placed in the way of those that wished to use computer evidence to hinder Internet manuscripts. However, sophisticated the criminal, few presently realise the information which the humble computer can hold and along with the mobile telephone this hardware has become the principal tool by which detectives obtain evidence.

Of course, the computer and correspondence held within it is also an invaluable friend to those who wish to prove their innocence. Thorough access and analysis to communications passing through an individual's mailbox, can categorically exonerate a person from prosecution allegations. It may not be, so much what exists in a computer but more what is absent which may go to establish that a defendant could not have created the incriminating documentation.

There is no doubt that as legal practitioners become aware of these developments analysis of electronic data will become more and more the norm in our criminal courts."

In a submission to the Criminal Courts Review in March 2000, Peter Sommer (Senior Research Fellow at the Computer Security Research Centre, London School of Economics & Political Science where his research speciality is Legal Reliability in Information Systems) said:

"To understand where evidence of Internet-related offences maybe located we need to recall how Internet connections are made and the forms they may take. Typically an individual uses his computer to connect to the Internet via an Internet Service Provider (ISP); home users dial in via a telephone network. There are thus four points at which evidence of various sorts may exist: on an individual's own computer, in his telephone bill, at the ISP and on remote sites."⁴

Later in the submission he adds:

"Most successful prosecutions rely on more than one stream of computer-derived evidence. What is needed is a multiplicity of independent streams of evidence, both computer- and non-computer-derived, which corroborate each other. Any single stream may fail either because of intrinsic inadequacy or because the courts find it too difficult to understand."

Conclusion

Even though computers are now an integral part of our lives, it appears that there is still a gulf between the legal and technical worlds that must be narrowed. All parties on the prosecution side from the police through to the judiciary need to become more aware of the implications of electronic evidence, especially email. Any forensic computer evidence offered *by either side* must take full account of the implications of email validity, its true source, destination and the myriad pathways between the two. More importantly, it must take into account the ease with which email can be forged without any obvious traces to the untrained eye.

Where a full audit trail exists and *can* be retrieved yet the prosecution do not offer this in support of any email evidence, the evidential value of that email will be greatly diminished in the eyes of the court.

Perhaps it is time to review the ACPO guidelines with respect to "best practice" in email investigations?

Contacts

John Cooper
25 Bedford Row
London

Simon Belfield
Frisby & Co.
26 Eastgate St
Stafford
ST16 2LZ

Philip Bowles
Datasec Ltd
Allen House
The Maltings
Sawbridgeworth
Herts
CM21 9JX

References

¹ "Code and other laws of cyberspace"

Author: Lawrence Lessig
Publisher: Basic Books; (June 2000)
ISBN: 0465039138
<http://cyberlaw.stanford.edu/code/>

² "Legal Admissibility and Evidential Weight of Information Stored Electronically"

Authors: Allen, Dyer, Galbraith, Mayon-White, Peggram, Shipman and Smith
Publisher: British Standards Institution (1999) (DISC PD 008)
ISBN: 0 580 33006 0
<http://www.bsi-global.com/Portfolio+of+Products+and+Services/Books+Guides/Doc+Management/pd0008.xalter>

³ "Stopping Spam"

Authors: Alan Schwartz and Simson Garfinkel
Publisher: O'Reilly
ISBN: 1-56592-388-X
<http://www.oreilly.com/catalog/spam/>

⁴ "Crime, Criminal Justice and the Internet (Special Issues)"

Editor: Clive Walker
Publisher: Sweet & Maxwell
ISBN: 042166990X

And

<http://www1.bcs.org.uk/DocsRepository/03900/3969/footprints.htm>