The Honorable John C. Coughenour

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JAMES S. GORDON, Jr., a married individual, d/b/a 'GORDONWORKS.COM'; OMNI INNOVATIONS, LLC., a Washington limited liability company, Plaintiffs, v. VIRTUMUNDO, INC, a Delaware corporation d/b/a ADNOWLEDGEMAIL.COM; ADKNOWLEDGE, INC., a Delaware corporation, d/b/a ADKNOWLEDGEMAIL.COM; SCOTT LYNN, an individual; and JOHN DOES, 1-X, Defendants.	NO. CV06-0204JCC **DECLARATION OF DR. NEAL KRAWETZ IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** NOTE ON MOTION CALENDAR: February 16, 2007

I, Neal Krawetz, swear under penalty of perjury under the laws of the United States to the following:

1. I am over age 18, and competent to be a witness. I am making this Declaration based on facts within my own personal knowledge.

2. I have been retained as an expert witness by Defendants Virtumundo, Inc. ("Virtumundo") and Adknowledge, Inc. ("Adknowledge").

3. I am a computer security researcher with a Ph.D. in Computer Science from

Texas A&M University (1998). Much of my work has been focused on tracking on-line entities, including the use and development of novel forensic techniques.

4. The Internet is an interconnected network of computer networks.

5. Each computer connected to the Internet has a network address, commonly represented by a unique 32 bit number called an Internet protocol address (an “IP address”).

6. The IP address is usually represented by four decimal numbers (octets) separated by periods.

7. The IP address system is a part of a communication architecture standard known as TCP/IP (i.e., Transmission Control Protocol (TCP) and Internet Protocol (IP)). In 1969, TCP/IP was adopted as the basis for the ARPAnet. By the mid-1980’s, the ARPAnet was replaced by other networks including the Internet.

8. The architecture of today’s Internet is based on the TCP/IP concept.

9. Communications over the Internet are made possible in large part because of network development based on the TCP/IP communication architecture.

10. The "domain name system" (or "DNS") was developed to convert between machine-readable IP addresses and user-friendly alphanumeric host names (hostnames).

11. Sets of related computers are grouped by domain names, such as “example.com”. Related hostnames include “host1.example.com” and “www.example.com”. The use of hostnames dates to 1971 and DNS was conceived in 1981.

12. The domain name system operates through a series of databases that "resolve" or link domain names with the IP addresses with which they are associated.

13. In order to connect to the Internet, a user’s computer must have an IP address. Consumers’ computers are typically provisioned with IP addresses by their Internet service provider, or “ISP”.

14. The term “ISP” generally refers to organizations or entities that provide Internet connectivity through means such as dial-up, cable modem, and digital subscriber

line ("DSL") connections, although it also encompasses companies that provide server hosting and other connectivity services.

15. A server is a computer (in this context, connected to the Internet) that provides services to other computers or applications. A server may be dedicated to this role, or it may be used simultaneously for other purposes, such as a desktop workstation. Services provided over the Internet (network services), such as web sites and email, generally consist of software running on server computers.

16. I have reviewed Exhibit "A" to the declaration provided by Mr. Gordon in Opposition to Defendants' Motion to Compel Discovery Re Lynn Interrogatories (Dkt. No. 76-1).

17. Mr. Gordon's statements in Exhibit "A" to his declaration reflect a misunderstanding of the technical operation of the Internet in general and email in particular. Specifically, Mr. Gordon seems to believe that one who initiates an email can control the information prepended, appended, modified, or added to its header while it is in transit and at the time of delivery. This is untrue.

18. For the reasons described in my report, a true and correct copy of which is attached hereto as Exhibit A, some or all of the "bad" headers of which Mr. Gordon complains were outside the control of Virtumundo and/or Adknowledge. Many of the headers of which Mr. Gordon complains were added by his own email program.

19. I have reviewed Mr. Gordon's deposition testimony. In it, he makes a number of statements that I consider questionable. My analysis of his testimony is contained in my report attached hereto as Exhibit A.

20. Domain names are provided by name servers. Gordon/Omni uses name service providers to register and host their domain names. Gordon/Omni does not host his own domain name.

21. WHOIS is a network based query/response protocol through which users can access contact information for the registrants of domain names and network addresses. WHOIS data is compiled by registrars from information submitted by

registrants.

22. All emails attributed to Virtumundo/Adknowledge came from subnets registered to them and listed in WHOIS.

DATED this 22nd day of January, 2007 at Fort Collins, Colorado.

22-Jan-2007

Dr. Neal Krawetz

EXHIBIT A

Expert Report of Dr. Neal Krawetz

Initial Expert Report of Dr. Neal Krawetz

Gordon, et al. v. Virtumundo, Inc. et al. United States District Court, W.D. Wash. Case No. CV06-0204JCC

January 22, 2007

Revision 2.1

Revision History

1.0 16-January-2007 Initial release

2.0 19-January-2007 Minor revision changes

Corrected number of emails attributed to vm-mail.com. The count was off by 939 emails. This error was due to 939 emails from SpamAssassin where the content was removed and the original email header was duplicated in the email content, leading to the “From:” line being counted twice. The correct value is 6,987 and not 7,926.

Revised transcript references. In version 1.0, I had cited the draft transcripts. Now I have the final transcripts.

2.1 22-January-2007 Minor additions

Per request, added information about root access and Plesk. Reviewed Exhibit A (76-1) and revised my comments concerning the “R3” headers.

1. Qualifications of Dr. Neal Krawetz

I am a computer security researcher with a Ph.D. in Computer Science from Texas A&M University (1998). Much of my work has been focused on tracking on-line entities, including the use and development of novel forensic techniques.

My research began in 1996 when I recognized that the problems with undesirable email (spam) were not being adequately addressed by existing filter-based technologies. I applied the scientific method and began investigating alternate anti-spam solutions by observing people who send spam (spammers), tracking their activities, developing theories and alternative explanations, and testing the theories. In 1997, I publicly identified my first spammer[1]. This led to the end of their spamming operations.

Since 1998 I have presented in a variety of forums on the topics of email and spam. Some of my public presentations include:

- *You Are What You Type: Non-Classical Computer Forensics*. Presented at the Black Hat Briefings, Las Vegas NV, August 2006.
- *Nobody's Anonymous: Tracking Spam and Covert Channels*. Presented at the Black Hat Briefings, Las Vegas NV, July 2004. (Presented under the pseudonym, "Curtis Kret".)
- *Evil with Email: Evaluation of an Insecure Network Service*. Presented at the ISSA Colorado Springs chapter security seminar, March 2004.
- *Nobody's Anonymous: Tracking Spam*. Presented at the Black Hat Briefings, Seattle, WA, January 2004. (Presented under the pseudonym, "Curtis Kret".)
- *Spam Tracking and Covert Channels*. Presented at InfowarCon, Washington DC, October 2003.

Three of these presentations were at the Black Hat Briefings. This is one of the leading conferences on computer security. The attendees include people from academic, commercial, law enforcement, government, and military backgrounds.

Beyond presentations, I have written a college textbook: *Introduction to Network Security*, Charles River Media, 2006 (ISBN 1-58450-464-1). This book includes an entire chapter on email including how it works, how to trace email headers, and its vulnerabilities. Although this book has been available for less than a year, it is already a required text for many university courses on networks and security.

One of my duties at my company, Hacker Factor Solutions (dba Hacker Factor) is the creation of white papers on specific research projects and existing trends. Samples of my public spam-related papers include:

- *A Guide to Building Secure Web Applications and Web Services*. (*http://www.owasp.org/documentation/guide/guide_downloads.html*) Open Web Application Security Project (OWASP), June 2005. I assisted with the document and wrote a section on spam and phishing for this document.
- *Anti-Phishing: Page Encoding*. (*http://hackerfactor.com/papers/ap-page_encoding.pdf*) Hacker Factor, April 2005. This document describes a novel approach for addressing the threat from phishing attacks.

[1] http://groups.google.com/group/comp.security.unix/browse_thread/thread/c9381bf882886fe7/70fa5c82a82c89d2?lnk=st&q=nealk%40net66&rnum=1&hl=en

- *Anti-Spam Solutions and Security*, Part I and Part II. (*http://securityfocus.com/infocus/1763* and *http://securityfocus.com/infocus/1766*) Security Focus, February and March 2004. This two-part paper evaluates existing anti-spam solutions, their effectiveness, and their limitations.
- "Anti-Honeypot Technology". *IEEE Security and Privacy*, January-February 2004 (Vol.2, No.1). This paper identifies a method used by spammers to identify honeypots. Honeypots are systems used to collect and evaluate new threats.
- *Banking Scam Revealed*. (*http://securityfocus.com/infocus/1745*) Security Focus, November 2003. This paper covers some of my novel research and how I identified a specific phisher. In November 2003, I sold this paper to a security company who, in turn, resold it to Security Focus. The only change to my original text is the title and removal of my name – it was originally titled *Bank Closed: Gone Phishing*.

Although I have given presentations, assisted law enforcement and government agencies, and provided consulting services to security and anti-spam companies, this is my first experience as an expert witness. For this case, I am charging $250 per hour for expert witness reports.

2. Overview of my Conclusions

This lawsuit involves the identification of false or misleading emails and an interpretation based on the CAN-SPAM act between Gordon, et al. and Virtumundo, Inc., Adknowledge, Inc., and Scott Lynn. My comments are focused on the email archives that I have been provided:

- adknowledgemailcom.mbx
- virtumundo-omni.mbx
- virtumundo.mbx
- virtumundo2.mbx

I am not an expert in law and wish to avoid expressing opinions about any legal interpretations. In addition, my evaluation is based on the facts presented to me and not on my opinion concerning the ethics or socially acceptable actions demonstrated by either party.

For this evaluation, I have been asked to respond to a specific set of questions.

1. Do any of the emails contain false or misleading header information? This includes the alteration or concealment of header information in a manner that would impair the ability of an individual to identify, locate, or respond to the person who initiated the email message.
2. Do any of the emails contain information used to obscure or misrepresent the email's point of origin (sender)?
3. Do the "From:" lines in the emails accurately identify the sender?
4. Is the sender clearly identifiable in the email header?
5. Is the sender clearly identifiable in the email content?
6. Is James Gordon or Omni Innovations, LLC (Gordon) an Internet access service?

These questions address requirements found in the CAN-SPAM act [15 U.S.C. 7701 (2003)]. In particular, unsolicited commercial email must contain no forged nor misleading header elements, no deceptive subject lines, and a clearly identifiable opt-out mechanism. The sender of each unsolicited email must be readily identifiable.

In addressing these factual issues I have arrived at the following conclusions. Please note that the conclusions summarized here are described and evaluated in greater detail in Sections 3 and 4 of this statement.

With respect to the first two factual issues, I will testify that the emails have been modified by mail transport agents (MTA) and the recipient's mail user agent (MUA, the Eudora mail reader). These modifications occurred after the email messages were initially transmitted. However, nothing in the modified headers, nor in the pre-modified header components indicate false or misleading header information. The email headers provide enough information to readily identify and locate the message sender.

With respect to the third factual issue, I will testify that I have made no attempt to contact the message senders in order to validate that they use valid response addresses. However, nothing appears to be fictitious and the domain names match the information in the content and throughout the header where the sender is identified.

With respect to the fourth and fifth factual issues, I will testify that the sender is clearly identifiable in the email header and content, and identifies an opt-out mechanism.

With respect to the sixth factual issue, I will testify that James Gordon does not appear to be an Internet access service as defined in the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

3. Email Analysis

This part of the testimony establishes critical definitions and background information about email functionality, email headers, and spam.

3.a. Email Transport Requirements

Email is the common name for messages sent using the Simple Mail Transport Protocol (SMTP). SMTP is defined by a series of de facto standard documents called the Request For Comments (RFCs). The RFCs are currently maintained by the Internet Engineering Task Force (IETF). The RFCs are not laws or standards. Instead, they represent a common repository for information sharing. This way, different developers can create compatible systems. In many cases, RFCs become proposed and are not widely adopted or are eventually discarded – many anti-spam recommendations never passed the proposal phase. In other cases, RFCs define one standard but the community implements a different standard. This is the case with VoIP and peer-to-peer technologies – the accepted RFCs came after the de facto standards were developed. Usually the recommendations made by RFCs are used to provide some form of common guidelines when no official standards exist.

Each RFC defines a different proposed standard or technical specification and is available from the IETF. RFC524 (*http://www.ietf.org/rfc/rfc524.txt*, June 1973) provided the initial framework for today's email. This defines an email messages as having one sender and one or more recipients. Additional RFC documents revised the specifications and added additional functionality. Occasionally new SMTP RFC documents are released that obsolete previous SMTP documents and attempts to unify all of the modifications and changes into one single document. RFC821 and RFC822 (1982) performed one of the first unifications (RFC821 defines SMTP and RFC822 defines the message format). These documents were replaced by RFC2821 and RFC2822 (2001).

Email was designed for reliable – but not immediate – message delivery. Each email contains a single sender and one or more recipients, identified by email addresses. Each email address contains two required components: an account name and a host. The host may be a specific computer or a domain name where the account is located. The account represents an individual mailbox (recipient) located at the host. In addition, email addresses may be associated with text strings (comments). The comments have no impact on email delivery.

Email is transmitted by a set of relays, called Mail Transport Agents (MTA). An MTA may receive emails from other MTAs (relaying) or from a sender's Mail User Agent (MUA). Similarly, an MTA may pass a message to another MTA or save it on the system (mail spool). The recipients MUA eventually retrieves the email from the mail spool. For example, I can send an email from my Gmail account to my YahooMail account. Gmail's web interface acts as the sender's MUA. The email is sent from the MUA to Gmail's MTA (the first relay hop). Gmail then sends the email to YahooMail (second relay hop) where it is stored in Yahoo's mail spool. I can then use Yahoo's web interface as the recipient's MUA in order to receive the email. The path becomes MUA→MTA→MTA→MUA.

It is very possible to route an email through multiple MTAs. Some of this routing can be natural; if a direct path is not available then email will be transported indirectly. Other routing can be intentional. Intentional routing can be done to explicitly route around a network congestion. However, it is also used to obscure a sender's path. Unscrupulous email senders frequently use open mail relays (publicly accessible MTAs) for obscuring email delivery and anonymizing the initial sender. In cases of explicit routing or mailing-by-proxy, the Received headers added by subsequent MTA systems provide logs for traceability.[2]

The normal delivery case relies on mail exchange records (MX records in DNS, see RFC974). These records are created by the owners of each MTA's domain. In general, the sender has no control of the email's delivery route. The route is determined by the recipient's MX records, as determined by the host in the email address.[3] As with the intentional and proxied routing methods, Received headers added by intermediate MTAs permit tracking the email's normal delivery route.

3.b. Email Header Structure

Every email contains three components: header, blank line, and content. The header consists of "field: value" pairs and provides meta-information for the email. The meta-information includes sender (From:), recipient (To:, Cc:, and Bcc:), subject (Subject:), and other fields. These headers are intended to be transmitted between MTAs – even if the MTA does not know the meaning of the field. The only headers with universal meaning to the MTAs are the sender and recipient lists. The header is well defined, including permitted character sets and some fields and values.

After the header is a single blank line that is used to separate the header from the content. Finally, there is the content. This is a large text block. Whether the block contains a text message, HTML, or attachments is independent of this definition; this is strictly the "content area".

RFC822 defined a minimal SMTP mail header. Every email must contain a "Date:", "From:", and a recipient – either "To:", "Cc:", or "Bcc:". In addition, the first MTA must create a "Message-ID:" field containing a unique identifier for tracking the email. The Message-ID is used for tracking mailing errors (debugging) and linking response emails (chaining email messages). Finally, every MTA prepends the email message with a "Received:" header for tracking the email's delivery route. (The Received header has a very well defined format, containing the source, destination, optional protocol, and date.) For example, the MUA can send the following header to the first MTA:

[2] Although an intermediate MTA could modify the Received headers, this is virtually never seen. In particular, the people who are most interested in disguising headers are senders who desire anonymity. Since the sender has no control over intermediate MTAs, there is no incentive for an MTA to modify existing headers.

[3] Technically, there are other routing methods available besides MX records. These other methods are also controlled by the MTA and not by the sender.

```
From: Pete <pete@silly.example>
To: John <jdoe@one.test>
Date: Thu, 13 Feb 1969 23:32:54 -0330
Subject: test
```

The first MTA will add in the Message-ID and Date (if either is not present), and a Received header for tracking the email.

```
Received: from user.machine by smtp.server.machine; 21 Nov 1997 10:05:43 -0600
From: Pete <pete@silly.example>
To: John <jdoe@one.test>
Date: Thu, 13 Feb 1969 23:32:54 -0330
Subject: test
Message-Id: <12345@cowabunga>
```

RFC822 was obsoleted by RFC2822. RFC2822 specifies that emails should have the minimal headers, but the minimal headers are no longer required. A message may be sent without a Date, Message-Id, etc. In particular, RFC2822 says:

```
When RFC 822 format is being used, the mail data include the memo
header items such as Date, Subject, To, Cc, From.  Server SMTP systems
SHOULD NOT reject messages based on perceived defects in the RFC 822 or
MIME message header or message body.  In particular, they MUST NOT
reject messages in which the numbers of Resent-fields do not match or
Resent-to appears without Resent-from and/or Resent-date.
```

While RFC documents specify de facto standards, they are not standards unto themselves. For example, some MTAs do not follow the defined Received header format, and some may not even add in Received headers. This leads to a complexity when tracking emails. In addition, protocols other than SMTP can be used to transfer email messages. The most common are the Post Office Protocol (POP3) and the Internet Message Access Protocol (IMAP). These protocols do not modify emails or their headers. Because some MTAs and MUAs may use RFC822, RFC2822, or some intermediary (or post-RFC2822) specifications, formats may appear similar but not explicitly compatible. Finally, spam filters and recipient MUAs may alter the email content by modifying headers, removing hostile content, or generating additional content.

3.c. Spam and CAN-SPAM

Email is a system ripe for abuse. In my presentations, I frequently refer to SMTP as "the poster child for how ***not*** to build a secure network protocol." Since the MTA can receive email from an MUA or another MTA, a sender can generate false Received headers and false or misleading sender email addresses without any way for the MTA or recipient MUA to validate the information. This single weakness – email is unauthenticated – has directly led to today's spam problem. Unscrupulous email senders frequently include false or misleading information in order to obscure the delivery trail, deterring their identification.

Each Received header contains information about the sender (MUA or MTA). This is either a hostname or an IP address (and usually both). To obscure the trail, many unscrupulous email senders relay the messages through proxies that provide an alternate network address from the original sender.

The CAN-SPAM act was one attempt at defining spam, when it can be used, and when it is in violation of the law. The use of forged mail headers, anonymous proxies, and misleading headers is forbidden by the CAN-SPAM act.

4 Email Archive Evaluation

The email archives that I received were reportedly provided to Derek Newman from Gordon et al. They contain a large number of email messages, including the headers. They are reportedly from a Eudora mail client (the recipient MUA). A sample email is as follows:

```
From ???@??? Mon Feb 06 09:36:07 2006
X-Persona: <gordonworks.com>
Return-Path: <faye@gordonworks.com>
Delivered-To: 7-jim@gordonworks.com
Received: (qmail 20163 invoked by uid 0); 6 Feb 2006 10:39:04 -0600
Date: 6 Feb 2006 10:39:00 -0600
Message-ID: <20060206163900.18822.qmail@gordonworks.com>
Received: (qmail 17088 invoked from network); 6 Feb 2006 10:38:49 -0600
Received: from vm208-28.adknowledgemail.com (216.21.208.28)
  by celiajay.com with SMTP; 6 Feb 2006 10:38:49 -0600
X-ClientHost: 102097121101064103111114100111110119111114107115046099111109
X-MailingID: 46823899
From: Franchise <FranchiseOpportunity@adknowledgemail.com>
To: <faye@gordonworks.com>
Errors-To: errors@adknowledgemail.com
Reply-To: return46823899@adknowledgemail.com
Subject: Work for yourself, not by yourself with a franchise.
Mime-Version: 1.0
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 8bit
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on gordonworks.com
X-Spam-Level:
X-Spam-Status: No, hits=-0.2 required=7.0 tests=BAYES_20,
        HTML_FONTCOLOR_UNSAFE,HTML_MESSAGE,MIME_HTML_ONLY,
        MSGID_FROM_MTA_HEADER autolearn=no version=2.63

<x-html>
<HTML>
<head><meta http-equiv="charset" content="iso-8859-1"></head>
...
```

This email message shows a number of modifications from the original sent message. The following list of points evaluate the email message from bottom to top because many headers are prepended to the message during delivery.

- **Modified content**. The message content begins with an <x-html> tag. This was likely added by the Eudora mailer. In particular, it was likely added after the email was delivered to the mail spool. The web site *http://www.slipstick.com/config/e2mtips.htm* provides a list of modifications made by the Eudora mailer.

- **Blank line**. A blank line separates the header from the content.

- **SpamAssassin headers**. The series of X-Spam headers were added by an anti-spam tool called SpamAssassin. SpamAssassin categorizes emails based on common attributes found in spam message and assigns a point value to each attribute. If the number of points exceeds a threshold set by the recipient, then the email is automatically classified as spam. For example, most emails contain a Date header, so the absence of a Date header awards the email a point. The use of the word "viagra" awards a point, as does the use of HTML. The items that can be awarded points and the point values are configurable by the user. The SpamAssassin classification method differs from the definition found in the CAN-SPAM act. In addition, SpamAssassin adds header information to the bottom on the header rather than the top of the header – an action that is non-standard by RFC822 and RFC2822.

① The X-Spam-Status line lists the number of points awarded, threshold value, and rules that trigged the spam value. In this case, all but one of the rules concern the email content. The one rule for the email header is MSGID_FROM_MTA_HEADER. This indicates that the Message-ID was added by an intermediate MTA rather than by the sender. SpamAssassin found no other spam-like items in the header.

- **Original headers**. The next ten headers (from “X-ClientHost:” to “Content-Transfer-Encoding:”) are likely the original headers generated by the sending MUA and/or first MTA. The original headers contain two non-standard headers (X-ClientHost and X-MailingID) which are likely used by the initial sender to track the email message in case of delivery error.

- **First Received header**. The first Received header (`from vm208-28.adknowledgemail.com`) appears to have been created by the sender’s MTA. This includes an IP address (216.21.208.28) logged by the MTA of the sender’s machine. This IP address matches the sender’s domain name. In particular, the registrant information for this IP address says:

```
[whois.arin.net]

OrgName:    Adknowledge, Inc.
OrgID:      ADKNO
Address:    4600 Madison Ave, Suite 1000
City:       Kansas City
StateProv:  MO
PostalCode: 64112
Country:    US

ReferralServer: rwhois://rwhois.adknowledge.com:4321

NetRange:   216.21.208.0 - 216.21.223.255
CIDR:       216.21.208.0/20
NetName:    ADKNO
NetHandle:  NET-216-21-208-0-1
Parent:     NET-216-0-0-0-0
NetType:    Direct Assignment
NameServer: NS1.AK-NETWORKS.COM
NameServer: NS2.AK-NETWORKS.COM
Comment:
RegDate:    2003-07-30
Updated:    2004-06-22

OrgTechHandle: ISPRE-ARIN
OrgTechName:   ISP Relations
OrgTechPhone:  +1-816-931-1771
OrgTechEmail:  isprelations@adknowledge.com
```

- **Second Received header**. The second Received header (`qmail 17088`) was added by the recipient’s mail relay (MTA). In this case, the MTA is a program called Qmail. Qmail is a common MTA, however it does not follow the Received header formats defined by the RFCs. In particular, Qmail includes two or three Received lines on every message and does not include all required information (“from”, “by” and “date” subfields). Two Received headers are used if Qmail is the final MTA, and three if Qmail is relaying to another MTA.

- **Qmail headers**. Between the two Received headers added by Qmail are a Date and Message-ID header. These were added by Qmail per the requirements in the RFCs. In particular, if the Date or Message-ID do not exist, then the MTA should add them. They should have been added by the first MTA, however their appearance is not mandatory. In this case, they were added by the second MTA. Failing to add them at the first MTA does not invalidate the email header, per RFC2822.

- **Eudora headers**. The next three header (X-Persona, Return-Path, and Delivered-To) are likely to have been added by Eudora. In particular, Eudora adds an X-Persona header, and may add Return-Path and Delivered-To headers depending on the user's configuration.
- **From separator**. The top-most header does not follow the normal "field: value" convention (it is missing the colon.) This is the From Separator and is used by the Unix mailbox format (mbox) to distinguish between different mail messages in the same file. Eudora uses a variation of the Unix mailbox format, but uses the same From Separator. The use of "???@???" for the From Separator's email address is a distinctive attribute set by the Eudora mail agent. For a comparison, a Unix mbox would include the sender's email address instead of "???@???".

Because of the flexibility within SMTP and the email format, it is easy to imitate other systems. For example, the Qmail headers could have been created by some non-Qmail MTA that is imitating the Qmail format. However, it is more likely that the header was created by Qmail. Similarly, I attribute some of the email formatting to Eudora and SpamAssassin. However, these could be attributed to other mail agents. Since the mail header says "SpamAssassin" and is consistent with SpamAssassin, I see no reason to assume otherwise. Similarly, the emails were reportedly from a Eudora mail archive and are consistent with Eudora. The Qmail header is consistent with the mail server located at `gordonworks.com`, which reports as being a Qmail server.

```
$ telnet gordonworks.com 25
Trying 208.109.91.140...
Connected to gordonworks.com.
Escape character is '^]'.
220 gordonworks.com ESMTP
HELP
214 qmail home page: http://pobox.com/~djb/qmail.html
quit
221 gordonworks.com
Connection closed by foreign host.
```

4.a. Differences between Mail Archives

Four email archives (Eudora mailboxes) were provided for evaluation. There are slight differences between each of the email archives.

- **adknowledgemailcom.mbx**. This mailbox contains 1,695 email messages. Most of the emails appear to be from Adknowledge.
    - ① Emails dated 1-April-2004 to 1-June-2005 were delivered from Adknowledge to a variety of domains. The primary domain was gordonworks.com, however chiefmusician.net was also used. These emails have been processed by Qmail and Eudora.
    - ① Emails dated 2-June-2005 to 11-June-2005 were processed by SpamAssassin. SpamAssassin included the email header from the message but removed the email's content. These email messages are incomplete. However, the included original headers match Adknowledge's headers.
    - ① Emails dated 12-June-2005 to 14-December-2005 appear similar to the first date range; the emails were from Adknowledge and processed by Qmail and Eudora. However, these emails were delivered to a wide range of domains including greatnorthwest-alpha.org,

itdidnotendright.com, anthonycentral.com, ehahome.com, rcw19190020.com, jaycelia.com, jammtomm.com, chiefmusician.net, celiajay.com, gordonworks.com, xj4x4.net, clrobin.com, jaykaysplace.com, and omniinnovations.com. All of these domains are found in the final Qmail Received headers indicating that they are the final destination. Since all emails were delivered to Gordonworks.com, they are likely owned by the same registrar. In addition, many of the domains appear to have registrants with names similar to James Gordon. For example, jaycelia.com is registered to:

```
Registrant:
   Jay Gordon
   200 Waldron Avenue
   Apt. #4
   Richland, Washington 99354
   United States
   Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
   Domain Name: JAYCELIA.COM
      Created on: 17-Jun-05
      Expires on: 17-Jun-07
      Last Updated on: 25-Jun-06
   Administrative Contact:
      Gordon, Jay  jaygordon@charter.net
      200 Waldron Avenue
      Apt. #4
      Richland, Washington 99354
      United States
      (509) 943-8858      Fax --
```

- ① A few emails (e.g., 19-June-2007, subject “Graduate school. A whole new level of learning.”) show a Symantec anti-virus filter processed the email before Eudora.
- ① Emails dated 15-December-2005 to 16-December-2005 were processed using SpamAssassin and are missing their content. The headers indicate that the sender was Adknowledge.
- ① Emails dated 16-December-2005 to 6-February-2006 were processed using a different SpamAssassin configuration, leaving the email content intact. These emails were processed by Qmail, SpamAssassin, and Eudora. As with the earlier messages, these were delivered to a large variety of domains.

- **virtumundo-omni.mbx**. This archive contains 7,016 email messages. Most came from Virtumundo. They contain the same original header fields as the Adknowledge emails.
  - ① The first email (7-December-2005) is an enrollment confirmation from Virtumundo.
  - ① The remaining emails, dated 15-December-2005 to 14-April-2006 came from Virtumundo and were delivered to a variety of domains; the same domains found in the Adknowledge archive. These emails were processed by Qmail, SpamAssassin, and Eudora.
- **virtumundo.mbx**. This archive contains 5,101 email messages. Most came from Virtumundo. The emails were delivered to a variety of hosting providers. The emails are intermixed within the email archive. These emails span the date range 7-October-2003 to 13-June-2004.
  - ① Many of the emails were delivered to Affinity, a hosting provider used by James Gordon. Either Affinity’s mailing system or Gordon’s email retrieval system modified the email header, adding in a “Date:” header that is not compliant with RFC822 nor RFC2822. In particular, a space is missing after the colon. In addition, tabs have been added to the From:

and To: fields (they should be spaces). Affinity also added a Message-Id. To restate this finding, the Message-Id, tabs, and Date header fields were not not added by Virtumundo. Instead, the Message-Id was added by Affinity, and the Date and tabs was either added by Affinity or by the recipient’s email application. A sample header:

```
From ???@??? Tue Oct 07 18:26:02 2003
X-Persona: <ValueWeb>
Received: from cust_req_fwding (faye@gordonworks.com --> jim@gordonworks.com) by
  ams.ftl.affinity.com id <4406176-22862>; Tue, 7 Oct 2003 19:31:23 -0400
Received: from vm096.vmadmin.com ([216.64.222.96]) by ams.ftl.affinity.com with
  ESMTP id <3784754-30738>; Tue, 7 Oct 2003 19:30:09 -0400
Received: from vmadmin.com (192.168.3.11)
  by vm096.vmadmin.com with SMTP; 07 Oct 2003 18:30:08 -0500
X-ClientHost: 102097121101064103111114100111110119111114107115046099111109
X-MailingID: 154978
From:   1800 Inkjets <QualityInkCartridges154978@vmadmin.com>
To:     Faye <faye@gordonworks.com>
Errors-To: errors@vmadmin.com
Reply-To: MailCenter <mailcenter+154978@virtumundo.com>
Subject: FREE Inkjets...No gimmicks - with our quality
Mime-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit
Message-Id: <03Oct7.193009-0400_edt.3784754-30738+970@ams.ftl.affinity.com>
Date:Tue, 7 Oct 2003 19:30:09 -0400
```

① Some emails were directly delivered to gordonworks.com and were not sent to Affinity.

① The final email (6-February-2006) appears to be from Jim Gordon <Kamau@charter.net> to bob@msfseattle.com (redirected to BertShawn@aol.com). The email bounced as undeliverable. In the email, Gordon appears to be including information about a potential defendant. The potential defendant in question does not appear to be Adknowledge nor Virtumundo; nothing in the email suggests otherwise. In this bounced email, Gordon wrote to “Bob” about a bounced email that he sent to the potential defendant:

```
Bob:
This "bounced email" is one of close to 100 emails that have
bounced from spam by marketers for "Bed N Bath", a Boston
company. Bill Silverstein and Joe Wagner (CA residents) will be filing a
lawsuit against this company in March (after waiting for the demand
letter...). I checked my spam repository and found over 700 spam from Bed
N Bath. One of my clients has also asked to join this action. By the way,
Bill and Joe will be suing this company in Boston (they have selected an
attorney to represent them). I would prefer the federal district
court...
My client will sue under its business name and I as
"gordonworks.com". There may be one or two additional
plaintiffs in this case. I should have firm details by Tuesday the
7th.
Thank you considering this case.
Best Regards,
Jim Gordon
```

- **virtumundo2.mbx**. This archive contains 5,047 email messages that appear to mostly be from Virtumundo and are dated 7-October-2003 to 24-March-2006. As with the other email archives, these were delivered to a variety of hosting sites and processed by SpamAssassin, Qmail, Eudora, and other email relays at hosting sites such as Affinity.

4.b. Inconsistency within the Mail Archives

Each of the email archives appear to be collections from a variety of email accounts:

```
FAYE@GORDONWORKS.COM
JAMES@GORDONWORKS.COM
JAY@GORDONWORKS.COM
```

```
ant@anthonycentral.com
bonniegg@gordonworks.com
business@gordonworks.com
celia@celiajay.com
chuck@anthonycentral.com
dewayne@anthonycentral.com
faye@gordonworks.com
hum@ehahome.com
indi@jammtomm.com
james@gordonworks.com
jamila@gordonworks.com
jay@gordonworks.com
jay@jaycelia.com
jim@gordonworks.com
jim@itdidnotendright.com
jim@rcw19190020.com
jobs@gordonworks.com
jon@jaykaysplace.com
jonathan@gordonworks.com
katie@ehahome.com
mila@jammtomm.com
sandy@anthonycentral.com
tj@anthonycentral.com
```

The email collections were processed using a variety of tools after the email message left control of Adknolwedge and Virtumundo. They were processed using SpamAssassin, Eudora, and some MTAs. None of this post-processing is surprising or unexpected. However, the variety of systems used, including different SpamAssassin configurations and different hosting sites per collection adds complexity to the analysis due to inconsistencies within the email archives.

4.c. Messages Not from Virtumundo

Not all of the email messages in the archives came from Virtumundo or Adknowledge. This is determined from the sender's IP address logged in the receiving MTA's Received header and from the set of original email header, before any recipient MTA and MUA modifications.

- **adknowledgemailcom.mbx**. There are 14 email messages not from Adknowledge. These appear to come from a different company: Digital Connexxions (aka WKI Data). Their headers use capitalized "To:" addresses, different header orderings from Adknowledge and Virtumundo, and are missing the X-ClientHost and X-MailingID headers found in Adknowledge and Virtumundo emails. These emails also include a Date: and Message-Id header that are set by the sender; Adknowledge and Virtumundo do not include these fields. A sample header:

```
From ???@??? Thu Jan 19 15:17:10 2006
X-Persona: <gordonworks.com>
Return-Path: <JAMES@GORDONWORKS.COM>
Delivered-To: 7-jim@gordonworks.com
Received: (qmail 11330 invoked by uid 0); 19 Jan 2006 15:46:21 -0600
Received: (qmail 7242 invoked from network); 19 Jan 2006 15:46:15 -0600
Received: from smtp16.prefersend.com (HELO smtp.prefersend.com) (207.53.245.26)
  by jammtomm.com with SMTP; 19 Jan 2006 15:46:15 -0600
Content-Transfer-Encoding: 7bit
Content-Type: multipart/alternative; boundary="_----------=_11377071587729947"
MIME-Version: 1.0
X-Mailer: MIME::Lite 2.117  (F2.6)
Date: Thu, 19 Jan 2006 21:45:58 UT
To: JAMES@GORDONWORKS.COM
From: Electronic Federal Tax Payment System <EFTPS@prefersend.com>
Reply-To: EFTPS@prefersend.com
```

```
Subject: EFTPS: Faster, Simpler Tax Payments
X-Campid: cid=199-uid=1821060-mid=1218-pid=47--
X-Eid: JAMES@GORDONWORKS.COM
Message-Id: <20060119214558.57A4E28F390B@smtp.prefersend.com>
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on gordonworks.com
X-Spam-Level:
X-Spam-Status: No, hits=-0.7 required=7.0 tests=BAYES_00,HTML_60_70,
        HTML_FONTCOLOR_RED,HTML_FONTCOLOR_UNSAFE,HTML_IMAGE_ONLY_10,
        HTML_IMAGE_RATIO_04,HTML_MESSAGE,HTML_TAG_BALANCE_A,MIME_HTML_ONLY,
        MIME_HTML_ONLY_MULTI,RCVD_IN_SBL autolearn=no version=2.63
```

- **virtumundo-omni.mbx**. There are six email messages not from Virtumundo or Adknowledge. These emails appear to have come from WKI Data.

- **virtumundo.mbx**. There are 15 emails not from Virtumundo or Adknowledge. Some appear to be from WKI Data, while others came from Popular Enterprises and other spammers. Some of these emails contain forged email headers.

  ① One email message was sent by James Gordon. This email, menioned above, is dated 6-February-2006 and appears to be from Jim Gordon <Kamau@charter.net> to bob@msfseattle.com. This email does not appear to be related to Virtumundo or Adknowledge.

  ① In one of the emails (27-January-2005 from "Carrie a"), the email uses forged a Virtumundo email address in the Reply-To field. Spammers running scams frequently impersonate domain names in their forged headers in order to anonymize the sender. As with the other non-Virtumundo emails, this email includes fake Received headers, a Message-ID and Date (real Virtumundo emails are missing these), and a partial SpamAssassin filter header, indicating that this header line is also forged. The full non-Virtumundo header is as follows, with forged components highlighted in bold text. This email actually originated from 211.184.9.3 (Korea), as noted on the first real Received line. The forged headers and Korean originator are inconsistent with the thousands of email samples from Virtumundo and Adknowledge. This leads me to conclude that this email is not from Virtumundo or Adknowledge.

```
From ???@??? Thu Jan 27 06:20:42 2005
X-Persona: <spam>
Return-Path: <uleon@yesmeds-now.net>
Delivered-To: virtual-gordonworks_com-spam@gordonworks.com
Received: (qmail 7424 invoked by uid 10003); 27 Jan 2005 10:30:50 -0000
Received: (qmail 7401 invoked from network); 27 Jan 2005 10:30:49 -0000
Received: from unknown (HELO 66.230.220.20) (211.184.9.3)
  by ns48.webmasters.com with SMTP; 27 Jan 2005 10:30:49 -0000
Received: from 234.30.43.48 by 211.184.9.3; Thu, 27 Jan 2005 04:21:53 -0600
Message-ID: <OMALLWDHYOTXAFSCDVVGG@webone8.com>
From: "Carrie a" <ULeon@yesmeds-now.net>
Reply-To: "Israel F Story" <CWilliam@virtumundo.com>
To: business@gordonworks.com
Subject: What IS OEM software and why do you care?
Date: Thu, 27 Jan 2005 14:21:53 +0400
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="--4172417560795376943"
X-Spam-Filter: F3_Unwanted_To_Address: business@gordonworks.com
```

- **virtumundo2.mbx**. There are 17 emails not from Virtumundo or Adknowledge. As with virtumundo.mbx, these came from a variety of spammers. Some emails contain forged headers, content hash-busters (used to bypass hash-based spam filters), and false or misleading sender information as specified in the CAN-SPAM act.

4.d. Factual Issues in the Case

There are six factual issues that have been requested in the expert report. My testimony is as follows:

1. Do any of the emails contain false or misleading header information? This includes the alteration or concealment of header information in a manner that would impair the ability of an individual to identify, locate, or respond to the person who initiated the email message.

The headers attributed to Adknowledge and Virtumundo do not contain false or misleading information. The headers are minimalistic and compliant with accepted email formatting specified in RFC2822.

2. Do any of the emails contain information used to obscure or misrepresent the email's point of origin (sender)?

There are no false or proxied Received headers used to obscure the sender's identity. The reverse lookup information for the IP address information accurately identifies Adknowledge or Virtumundo.

3. Do the "From:" lines in the emails accurately identify the sender?

Each of the "From:" lines specify the domain name of the sender.

All of the Adknowledge emails from adknowledge.mbx are from "@adknowledgemail.com" (1,673 emails) or "@my-freemail.com" (8 emails). The my-freemail.com messages came from an IP subnet owned by Adknowledge and the domain is registered to Venture Direct. According to a representative from Adknowledge, Venture Direct is a client and they were permitted to use the IP range.

The emails from all of Virtumundo archives (virtumundo-omni.mbx, virtumundo.mbx, andvirtumundo2.mbx) came from a variety of domains managed by Virtumundo and Adknowledge: adknow-net.com (1,198 emails), virtumundo.com (25 email), vm-mail.com (6,987 emails), vmadmin.com (5,643 emails), vmadmin.com (5,643 emails), vmamdin.com (8 emails), vmlocal.com (3,165 emails), and vtarget.com (100 emails).

The only false domains appear to be the eight emails from "vmamdin.com". These appear to be a typographical error from "vmadmin.com". These eight emails were sent within the same minute to eight email addresses on 23-January-2004. Although the "From:" line was invalid, the "Errors-To:", IP addresses, and content's contact information all identify Adknowledge and Virtumundo.

Virtually all of the "From:" lines contain different accounts within the Adknowledge and Virtumundo domains. However, the account names appear related to the email content and do not appear to be false or misleading.

4. Is the sender clearly identifiable in the email header?

With the exception of the eight typographical errors, all Virtumundo and Adknowledge emails are clearly identifiable by the "From:" header. Even with the eight errors, the senders are identifiable by their origination IP addresses, reply email address, and errors email address.

5. Is the sender clearly identifiable in the email content?

To answer this question, I am ignoring the emails where the recipient's SpamAssassin removed the content. In those emails, there is no content to evaluate. The removal of the content was performed by the recipient and outside of the control of Adknowledge or Virtumundo.

Each of the Virtumundo and Adknowledge emails with content contain URLs to their domains and a sentence or paragraph stating who it came from. In most of the emails, the paragraph is very explicit. For example:

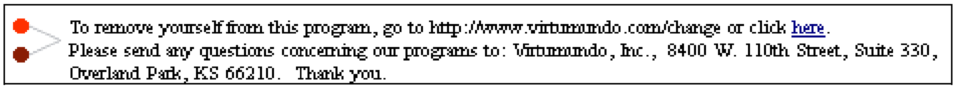
> You received this email because you signed up at one of Virtumundo's websites (see the "Properties" listed at http://privacy.virtumundo.com/properties.html) or you signed up with a party that has contracted with Virtumundo. To unsubscribe from the Virtumundo Rewards List, go to http://www.virtumundo.com/unsub or go here [URL]. To read Virtumundo's privacy policy, go to Privacy Policy [URL]. The products and/or services advertised in this email are the sole responsibility of the advertiser, and questions about this offer should be directed to the advertiser.
>
> (c) 1998-2003 Virtumundo, Inc. All rights reserved.

In these emails, the font size is specified as “1” (1 point font). However, most web browsers set a minimal font size that is larger than 1 pt, so the text should be readable.

In other emails, the paragraph is less wordy. for example:

> To unsubscribe click here [URL].
> 428 River View Plaza
> Trenton, New Jersey 08611
> Can-spam Act 2003 Compliant

In a few of the emails, there is no text identifying the sender, but there are hyperlinks and images from Virtumundo sites. For example, an email from 8-June-2004 contains an image with text stating who sent the email. The image (http://v1.cc/ft/robot.gif) says:



To remove yourself from this program, go to http://www.virtumundo.com/change or click here.
Please send any questions concerning our programs to: Virtumundo, Inc., 8400 W. 110th Street, Suite 330, Overland Park, KS 66210. Thank you.

This image is associated with a URL.

In the “my-freemail.com” emails, the sender is identified with a paragraph as coming from company “MyFree.com” with the domain “my-freemail.com”.

Yes, I believe the sender is clearly identified in the content. I believe this primarily because the URLs in the unsubscribe links match the header information, but also because of the text (or images containing text) that identify the sender within the content.

Based on the presence of the opt-out removal instructions, it appears that Gordon was provided an opt-out mechanism. It appears that he had the opportunity to opt-out from future mailings.

6. Is James Gordon an Internet access service?

The Communication Act of 1934 defines an Internet access service (47 U.S.C. 231(e)(4)) as follows:

> The term “Internet access service” means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.

Based on this definition, I see no evidence suggesting that Gordon is an Internet access service. Gordon’s role with the Internet access services appears to have been as a customer. The list of service providers found in the email archives include Affinity and GoDaddy. The email headers show no evidence of Gordon owning or operating a service that enables users to access Internet services.

In addition to the email recipient providers, there is the previously mentioned email dated 6-

February-2006 from Jim Gordon <Kamau@charter.net> to bob@msfseattle.com. This email originated from 68.113.1.119. This IP address resolves as 68-113-1-119.dhcp.knwk.wa.charter.com, a Washington-based DHCP customer for Charter Communications. Charter is an Internet access service provider and Gordon appears to be a customer. There is no evidence in the logs of email being delivered to this IP address or of other people using this IP address. This IP address appears to be a residential service, and not a commercial service.[4] According to Charter's use policy (*http://www.charter.com/Visitors/Policies.aspx?Policy=6*), the service is only for use in a single household, and not as a third-party to email or other Internet services.

In the Gordon testimony (Page 112, lines 10-25), Gordon states that he uses GoDaddy for server hosting and identifies that he does not have root access on the systems. The "root" account is the administrator on Unix/Linux systems. Without root access, the user is not the system administrator. (Root for Unix is similar to the Microsoft Windows "Administrator" account.) However, some system services may be managed by user accounts (non-root). For example, GoDaddy provides an administrative tool called Plesk (*http://www.swsoft.com/plesk/*) for managing DNS information. Gordon states that he uses Plesk (page 109, lines 9-20) to administer the domains that he has registered or manages. In particular, GoDaddy only permits the management of domains registered through GoDaddy (*http://help.godaddy.com/article.php?article_id=663&topic_id=163&&*); this excludes third-party hosting. Although Gordon may be a domain administrator for a set of domains, he is not an Internet access service for DNS hosting. To fully illustrate this relationship:

- The domain "ehahome.com" is registered to "Emily Abbey" through GoDaddy. The DNS servers for managing this host are "ns1.gordonworks.com" and "ns2.gordonworks.com".
- The domain "gordonworks.com" is registered to "Omni Innovations, LLC" through GoDaddy. The DNS servers for managing this host are "ns1.gordonworks.com" and "ns2.gordonworks.com".
- On 22-January-2007, the host "ns1.gordonworks.com" resolved to the IP address 68.178.150.119. This IP address has a reverse-lookup of ip-68-178-150-119.ip.secureserver.net. The domain "secureserver.net" is owned and operated by GoDaddy. The host "ns2.gordonworks.com" resolves to 208.109.91.7 with a reverse lookup of ip-208-109-91-7.ip.secureserver.net; another GoDaddy address.

For Gordon to use GoDaddy's server and administer the "ehahome.com" domain, he must have administrative rights but not hosting rights. The company providing the hosting rights is GoDaddy. GoDaddy permits Gordon to administer the domain. Thus, GoDaddy is the Internet access service, while Gordon is a customer of GoDaddy.

5. Addressing Existing Testimony

Derek Newman requested that I review James Gordon deposition transcripts. Within the transcripts are some technical inaccuracies.

Seattle, Washington; January 9, 2007, 9:23 AM. Deposition of James S. Gordon, Junior.

Page 81, line 25.

[4] Determined from the ARIN (American Registry for Internet Numbers) registration records for the subnet and from a DNS scan. The ARIN records do not identify the subnet as a commercial subnet. However, this is not conclusive. A DNS scan of the subnet 68.113.1.0 – 68.113.1.255 do not identify any domain names beyond "charter.com". Although not conclusive, this is a very strong indicator of a residential subnetwork. In contrast, the Charter subnet 68.113.3.0 – 68.113.3.255 contains alternate DNS names and "static" instead of "dhcp" in the hostnames, suggesting commercial customers.

Gordon states that SpamAssassin identifies spam relays. This is not entirely correct.

SpamAssassin uses data from third-party RBS (Realtime Blacklist Systems) to identify networks linked to the distribution of undesirable email. RBS lists identify IP addresses and subnets associated with sending spam. This could be due to open relays and compromised hosts, or because a company is sending directly but the company is identified as a spammer.

In many cases, RBS lists can lead to false-positives, where an IP address or subnet is classified as a spammer even though the owner never sent any spam emails. For example, this can happen if a user (or company) is assigned an IP address previously used by a spammer. Some companies have been blacklisted as a pressure-move and not due to spam. For example, nearly all Comcast IP addresses assigned to cable modems have been blacklisted. This is not because they are all spammers or that Comcast is a spammer. This is because Comcast is reported as doing little to prevent malware from being used to send spam from their customer's computers. The blacklist is intended to pressure Comcast into filtering their customer's web access.

I believe it is important to point out that all RBS providers operate outside of government or legal influence. They are run by teams of individuals without any external oversight. Furthermore, some anti-spam groups such as SpamHaus offer methods to contest a RBS listing. However, since they use their own RBS lists, it can be difficult for an accused spammer to contact them.

Per page 131 line 23, it is also important to mention that the definition of spam from SpamHaus and other RBS providers differs from the definition found in the CAN-SPAM act.

Page 98, line 10.

Gordon states that the email was delivered because it was not bounced.

This is a minor technical issue. Not every email system generates a delivery failure message. Bounce-back messages are occasionally used by spammers to re-mail spam and has been used for email based denial-of-service (DoS) attacks. As a result, many servers have disabled this functionality. In addition, spam filters on the receiver's end may discard the email before delivery. While most of the time no response means it was delivered, this is not always the case. It is plausible that Gordon's emails were sent to a bad address or filtered by Adknowledge as spam. I cannot speak on the probability of this.

Page 255, line 4.

Gordon states that the systems were up because they were reachable using Visual Route.

Visual Route performs a traceroute function, used to identify the direct network path to a host. Traceroute does not necessarily nor usually follow the path taken by email. Traceroute also does not validate whether any network services are available besides ICMP (a network-layer protocol). In particular, traceroute does not check if a mail server is active on the destination system.

Seattle, Washington; January 10, 2007, 9:07 AM. Deposition of James S. Gordon, Junior.

Page 297, beginning at line 15.

Gordon explains how an email's "From:" line should say who it comes from. He implies that it should be a person's name.

RFC2822 gives some example email addresses including ones where the "From:" line's text field contains a comment. On Unix systems, the "From:" line's text string is usually taken from the GECOS field in the password file. The **G**eneral **E**lectric **C**omprehensive **O**perating **S**upervisor field contains the name associated with an account, office location, phone number, and other meta-information. All parts of the GECOS are optional. On Windows system, there is no directly equivalent information to the GECOS field and the default string is usually left to the user to enter.

Neither RFC822 nor RFC2822 require a string to be present nor specify the purpose of the string associated with an email address. While using a person's name is common for emails from individuals, it is not common for emails from companies or other organizations. A few examples:

```
From: "Challenge" <challenge@dc3.mil>
```

> I received this email from the Department of Defense's Cyber Crime Center (DC3). The email was related to a Forensic Challenge that I entered. (I was the highest scoring team among civilian contestants.) Although it was sent by an individual, the sender's name references the contest described in the email content.

```
From: <watch.help@wsp.wa.gov>
```

> An email reply from the State of Washington concerning a criminal background check I requested in 2004. There is no string identifying the sender.

```
From: "sbirhelp" <sbirhelp@brtrc.com>
```

> This is comes from an email I received in 2003 from the Department of Defense's SBIR grant process. It contains the account name in the text field.

```
From: NW Customer Services <customer_service@nww.com>
```

> This header comes from Network World's magazine subscription system. The domain does not say "Network World" but is related to the content.

Each of these example services generate opt-in emails and provide an opt-out mechanism. In many cases, the opt-out method was similar to the process provided by Adknowledge and Virtumundo.

Finally, in the sample email archive virtumundo.mbx, the last email was sent by James Gordon. It says:

```
From: Jim Gordon <Kamau@charter.net>
```

The string associated with the email address does not match the email address and does not match any domains owned by Gordon. In addition, the email address does not match the content. However, this does not indicate that the sender nor the email address is fictitious, forged, or misleading.

Page 306, beginning at line 7.

Gordon attempts to explain how email is transmitted and when headers are added. In his explanation, he mistakenly states that the sender adds in headers and tracking information. Received headers are intended to be added by the receiving MTA and not the sending MTA. Any IP address or hostname listed in the Received header was added by the recipient, not the sender.

There are two common situations where the sender creates Received headers. First, the MTA may be passing the email between processes on the same server. This is why Qmail includes additional Received headers. The second situation is in spam with false Received headers. The spammer may include false Received lines in order to obscure their origination address. The Adknowledge and Virtumundo emails do not contain false Received headers.

Page 306, beginning at lines 17-20.

Gordon states that the emails from Adknowledge and Virtumundo are missing Received headers. I see no evidence of missing Received headers. In addition, there are Received headers in the email as sent from Adknowledge and Virtumundo. These headers were added by the recipient, outside of the control of the sender. Gordon's testimony in this case is incorrect.

Gordon continues on page 307 to state that the emails from Adknowledge and Virtumundo lack chaining between the Received headers. I see no indication of this. In fact, I explicitly see chaining between the mail agents, indicating no false Received headers.

Page 355, line 17.

Gordon attempts to describe Received headers. He states, "The "from" token in R3, which according to Internet protocol...".

The Internet Protocol (IP) does not define any such "R" tokens. Nor are "R" tokens defined in any of the email RFC documents. These tokens appear in Exhibit A and are attributed to the interpretation from a tool called eMailTracking Pro.

Because Received headers are added by each receiving mail relay, there are frequently many of them. There is no consistent enumeration method for identifying specific headers. Some researchers count the top-most header a "1", and subsequent headers as "2", "3", etc., and other people begin counting from the bottom of the list. The only consistent terms are "first" and "last". The "first" Received header is at the bottom of the stack and was added "first". The top-most Received header is the "last" Received header because it was added last.

To reiterate, the Received headers and their content are added by the receiving MTA. There is no evidence of forged Received headers being added by Adknowledge or Virtumundo.

Examples of the eMailTracking Pro tool used by Gordon (page 122, line 24) are reportedly included in Exhibit A (76-1). The first example (page 5, subject "Test your internet connection lynkstation") shows an email with forged Recevied headers. However, this email is not attributed to Adknowledge or Virtumundo. In particular, the email is missing all of the identifiers found the thousands of emails attributed to Adknowledge and Virtumundo: the origination IP address is not from a subnet owned by Adknowledge or Virtumundo, the header is missing the X-ClientHost and X-MailingID headers, and the "From:" domain does not specify a domain owned by Adknowledge or Virtumundo. Although this example does contain forged and misleading headers, there is no indication that is came from Adknowledge or Virtumundo; it likely came from someone else.

The remaining examples (beginning with page 8, under the heading "Email Analysis – Virtumundo") show all of the features attributed to the emails from Virtumundo. However, nothing in the analysis indicates forged or misleading email headers, including the Received headers. In particular, all of the received headers properly chain, providing a log that does not appear to be forged or misleading.

Page 356, line 13.

Gordon is asked about the IP address 192.168.3.11. His answer is incorrect.

RFC1597 initially defined a set of non-routable IP addresses for use in private environments. The range includes:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 – 192.168.255.255

Virtually all home firewalls use addresses within this range for use within the home. Many companies use these ranges too. In order to route email or traffic outside of the firewall, a router or gateway is used to connect the private subnet with a public subnet.

Although RFC1597 first defined subnets for private use, it is not the only RFC to do so. The list of special purpose subnets was extended by many other RFC documents; most notably, RFC3330.

Page 358.

This page discusses time within the email headers. Although I do not know which specific email is being discussed, there seems to be some confusion about time within the headers. In particular, each Received header includes a timestamp (with the noted exception of headers from Qmail). The time represents the time on the recipient's system, not the sender. There is nothing in any of the email RFCs requiring computers to have synchronized clocks. The discussion is discussing clocks that are off by as much as 15 minutes. This is definitely not uncommon. Most users rarely synchronize the clocks on their computers. Times between two computers may be off by a few minutes, and 15 minutes (or even hours with Daylight Saving Time) are not uncommon.

Some spammers do try to set a time to a random interval (+/- 12 hours) to deter tracking. In addition, a common spam trick is to choose a time in the future so the email appears at the top of the recipient's sorted mailbox listing. However, I see no evidence of Virtumundo or Adknowledge using these deceptive tactics.

Page 360, line 23.

Gordon states that the presence of "unknown" in the Received header is a deceptive tactic by the sender. This is incorrect.

A sample email header with the line in question highlighted in bold:

```
From ???@??? Wed Jun 09 14:59:46 2004
Return-Path: <mailcenter308901@vmadmin.com>
Delivered-To: virtual-gordonworks_com-jim@gordonworks.com
Received: (qmail 22046 invoked by uid 10003); 9 Jun 2004 20:51:58 -0000
Delivered-To: virtual-gordonworks_com-jay@gordonworks.com
Received: (qmail 22043 invoked from network); 9 Jun 2004 20:51:58 -0000
Received: from unknown (HELO vm114.vmadmin.com) (216.64.222.114)
  by ns48.webmasters.com with SMTP; 9 Jun 2004 20:51:58 -0000
Received: from vmadmin.com (192.168.3.11)
  by vm114.vmadmin.com with SMTP; 09 Jun 2004 15:51:55 -0500
X-ClientHost: 106097121064103111114100111110119111114107115046099111109
X-MailingID: 308901
From: Advanced Diabetes Supply <AdvancedDiabetes@vmadmin.com>
To: Jay <jay@gordonworks.com>
Errors-To:  errors@vmadmin.com
Reply-To: Advanced Diabetes Supply <AdvancedDiabetes308901@replies.virtumundo.com>
Subject: Diabetic Testing Supplies Direct to You
Mime-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit
```

The Received header in question was added by the server "ns48.webmasters.com". Webmasters.com is a hosting provider used by Gordon. The word "unknown" was added because the IP address (216.64.222.114) could not be resolved by a reverse DNS lookup to a text hostname by the server. This could be due to a configuration error at the recipient system, extended DNS delays due to a busy network, or a variety of other network or configuration issues. It could simply be an IP address without a hostname – IP addresses are not required to have hostnames[5].

In the HELO subfield, the sending system identified itself as "vm114.vmadmin.com". I performed a host lookup of this hostname and found that vm114.vmadmin.com has the address

[5] IP addresses are defined in a series of RFC documents, most notably RFC791 (1981). Hostnames come from the Domain Name System (beginning with RFC881 (1983)). In particular, a hostname may map to any number of IP addresses (zero or more), and an IP address may be associated with zero or more hostnames. There is no requirement for an IP address to have a hostname.

216.64.222.114. Thus, the inability for the recipient to identify the hostname appears to be an error on the recipient’s part, not a deceptive practice by the sender.

Page 246, line 14 and Page 345, beginning at line 11.

Gordon makes repeated references to using a tool called Evidence Eliminator for removing files from his computer. According to their Web site (*http://www.evidence-eliminator.com/*), this tool removes system histories and logs, and securely deletes files. Tools such as this make it virtually impossible for common forensic tools to recover data from hard drives.

Gordon states that his reason for using Evidence Eliminator is to remove system viruses. However, this is not an anti-virus tool. This type of tool is commonly called a file wiper or file shredder. Evidence Eliminator performs file wiping (secure erasing) as well as history cleansing.

As a security consultant, I do recommend wiping and cleaning tools for systems that contain sensitive information and are at risk of theft or infection by spyware. (Many spyware variants search Web caches for login and account information.)

In Gordon’s case, the use of Evidence Eliminator could potentially interfere with email analysis. In the emails where SpamAssassin removed the content, the content was reportedly saved to his hard drive. The use of Evidence Eliminator could permanently delete these content files. For example, in this email from the file adknowledgemailcom.mbx, SpamAssassin reports that the content has been saved to the file system (bold added for highlighting):

```
From ???@??? Mon Jun 06 15:38:46 2005
X-Persona: <Virtual Server - spam>
Return-Path: <mailcenter6528395@adknowledgemail.com>
Delivered-To: 7-faye@gordonworks.com
Received: from localhost by omniinnovations.com
        with SpamAssassin (2.63 2004-01-11);
        Mon, 06 Jun 2005 15:06:11 -0600
From: CD Duplication <DiscDuplication@adknowledgemail.com>
To: <faye@gordonworks.com>
Subject: *****SPAM***** Find professional CD duplication here.
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on omniinnovations.com
X-Spam-Level: ********
X-Spam-Status: Yes, hits=8.8 required=3.0 tests=DATE_MISSING,HTML_70_80,
        HTML_IMAGE_ONLY_06,HTML_MESSAGE,MIME_HTML_NO_CHARSET,MIME_HTML_ONLY,
        RCVD_IN_BL_SPAMCOP_NET,RCVD_IN_SORBS,X_MAIL_ID_PRESENT autolearn=no
        version=2.63
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----------=_42A4BAC3.33B0B65B"

Spam detection software, running on the system "omniinnovations.com", has
identified this incoming email as possible spam.  The original message
has been attached to this so you can view it (if it isn't spam) or block
similar future email.  If you have any questions, see
the administrator of that system for details.

Content preview:  URI:http://ak2.cc/oc/160/16046/newsletter_01.jpg
  URI:http://ak2.cc/oc/160/16046/newsletter_02.gif
  URI:http://ak2.cc/oc/160/16046/newsletter_03.jpg [...]

Content analysis details:   (8.8 points, 3.0 required)
 pts rule name              description
---- ---------------------- --------------------------------------------------
 1.0 DATE_MISSING           Missing Date: header
 2.8 X_MAIL_ID_PRESENT      Message has X-MailingID header
 1.7 HTML_IMAGE_ONLY_06     BODY: HTML: images with 400-600 bytes of words
 0.0 HTML_MESSAGE           BODY: HTML included in message
 0.1 HTML_70_80             BODY: Message is 70% to 80% HTML
 0.1 MIME_HTML_ONLY         BODY: Message only has text/html MIME parts
 0.7 MIME_HTML_NO_CHARSET   RAW: Message text in HTML without charset
 2.2 RCVD_IN_BL_SPAMCOP_NET RBL: Received via a relay in bl.spamcop.net
```

```
               [Blocked - see <http://www.spamcop.net/bl.shtml?216.21.210.20>]
 0.1 RCVD_IN_SORBS          RBL: SORBS: sender is listed in SORBS
                            [216.21.210.20 listed in dnsbl.sorbs.net]
```

The original message was not completely plain text, and may be unsafe to open with some email clients; in particular, it may contain a virus, or confirm that your address can receive spam. If you wish to view it, it may be safer to save it to a file and open it with an editor.

```
Received: (qmail 32226 invoked from network); 6 Jun 2005 15:06:09 -0600
Received: from vm210-20.adknowledge2.com (HELO kc-sb02.ak-networks.com) (216.21.
210.20)
  by itdidnotendright.com with SMTP; 6 Jun 2005 15:06:09 -0600
Received: from adknowledgemail.com (10.10.50.60)
  by sb01.adknownet.com with ESMTP; 06 Jun 2005 16:05:57 -0500
X-ClientHost: 10209712110106410311111410011110119111114107115046099111109
X-MailingID: 6528395
From: CD Duplication <DiscDuplication@adknowledgemail.com>
To:    <faye@gordonworks.com>
Errors-To:  errors@adknowledgemail.com
Reply-To: return6528395@adknowledgemail.com
Subject: Find professional CD duplication here.
Mime-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit
```

Attachment Converted: "c:\program files\qualcomm\eudora\attach\SPAM Find professiona.htm"

This file should be located on the hard drive used by Gordon to run SpamAssassin. If the file is not there, then it is very probable that Evidence Eliminator has deleted any record of it.

Various Pages.

Throughout the deposition, Gordon seems to confuse his role at various Internet Service Providers (ISPs). For example, on page 77, starting with line 4, Gordon states that he has used Earthlink, Webmasters, ValueWeb as well as Godaddy and AOL. Later he states (page 79, lines 19-20) that ValueWeb and Webmasters were his service providers.

Each of these companies are hosting providers and Gordon appears to have been a customer. The "Affinity" hosting that I mentioned earlier is very likely the ValueWeb that Gordon mentioned – ValueWeb and Affinity are the effectively same company.

There is also some confusion as to who provides which services. For example, on page 79 (line 2-5), Gordon states that he manages his own email accounts. This is not exactly true. There is a DNS provider who registers and manages the domain name. Currently, "gordonworks.com" is registered through GoDaddy (a domain registrar and hosting site). All emails to "gordonworks.com" are sent to GoDaddy. GoDaddy also provides email hosting services and email redirection services. In the former case, GoDaddy provides the mail spool. In the latter case, the emails are redirected to another email hosting provider. GoDaddy permits customers to specify email addresses within their registered domains for receiving or forwarding email.

This misunderstanding leads back to the original question concerning who is the Internet Access Service. In these cases, GoDaddy, Affinity/ValueWeb, WebMasters, Earthlink, and AOL are the Internet Access Services. Gordon is a customer to these services.

6. Conclusion

I was engaged by Derek Newman on behalf of Adknowledge, Virtumundo, and Scott Lynn as an expert witness due to my extensive background on networks and email analysis. I was asked to provide an expert opinion on six questions, based on a set of email archives and deposition records. My findings are as follows:

1. None of the emails in the archives that are attributed to Adknowledge and Virtumundo contain intentionally false or misleading header information. There are only 8 emails that appear to represent a one-time typographical error rather than any intentional misrepresentation; these emails were all sent within the same minute to multiple recipient accounts. There are some emails in the archives that do contain false or misleading headers, but they were not sent by Adknowledge or Virtumundo and it is unclear why they were included in these archives.
2. None of the emails attributed to Adknowledge or Virtumundo contain information used to obscure or misrepresent the email's point of origin.
3. All of the emails attributed to Adknowledge or Virtumundo have "From:" lines that appear to accurately identify the sender, with the exception of the previously mentioned 8 typographical errors. In these 8 emails, other header fields correctly and accurately identify the sender. In all cases, I have made no attempt to contact the provided email addresses and I cannot attest to the validity of the email addresses.
4. All of the emails attributed to Adknowledge or Virtumundo clearly identify the sender in the email header.
5. All of the emails with content and attributed to Adknowledge or Virtumundo clearly identify the sender in the email's content.
6. James Gordon does not provide an Internet access service.

In addition to these six questions, I was asked to review the Gordon deposition transcripts and identify any technical inaccuracies. I identified a number of inaccuracies surrounding the description of the email headers and how email operates. I also identified concerns surrounding how the email archives have been managed.

This expert report is based on my preliminary analysis of the provided information. I reserve the right to revise or amend this report, depending of the development of additional facts or circumstances.

Neal Krawetz

Neal Krawetz, Ph.D.
Hacker Factor Solutions
P.O. Box 270033
Fort Collins, CO 80527-0033