IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF TEXAS

LUBBOCK DIVISION

SUSAN POLGAR	§	
	§	
VS.	§	
	§	
UNITED STATES OF AMERICA	§	
CHESS FEDERATION, INC.,	§	
and	§	
BILL GOICHBERG, JIM BERRY,	§	
RANDY BAUER, and	§	
RANDALL HOUGH, all Individually and	§	
in their Representative Capacities as	§	C.A. NO. 5-08CV0169-C
Members of the Executive Board of the	§	
United States of America Chess Federation;	§	
BILL HALL, Individually and in his	§	
Representative Capacity as Executive	§	
Director of the United States of America	§	
Chess Federation; BRIAN MOTTERSHEAD;	§	
HAL BOGNER; CHESS MAGNET, L.L.C.;	§	
CONTINENTAL CHESS INCORPORATED;	§	
JEROME HANKEN; BRIAN LAFERTY;	§	
SAM SLOAN; KARL S. KRONENBERGER;	§	
and KRONENBERGER BURGOYNE, LLP	§	

DEFENDANTS' EXPERT WITNESS DISCLOSURE OF DR. FREDRICK B. COHEN

Section 1: My background relative to the matter at hand

My name is Fred Cohen and I have been asked to write a report discussing some of the issues involved in this matter. Specifically, within the limits of available time and information, I have been asked to provide opinions related to the claims by and against Plaintiff Susan Polgar including without limit, technical matters involving the operation of the Internet, and in particular, about the delivery, use, methods, and operations of email and newsgroup systems and servers, the content and indications associated with specific emails and newsgroup postings at issue in this case, and a variety of issues regarding evidence related to these emails, postings, and related events.

I have extensive knowledge of the Internet and its predecessor the ARPAnet, starting from when I was a computer operator for one of the early nodes in the ARPAnet (circa 1974). I have performed systems administration and related tasks for computers in stand-alone and networked environments continuously since that time. I have specific experience with electronic mail (email) and network-based newsgroups, including without limit, experience in designing, implementing, and operating email servers, bulletin boards, and similar systems, proxy servers, email and newsgroup clients and mechanisms, the use and technical interpretation of relevant specifications and the technical language used to define those specifications, and detailed knowledge of how email and newsgroup systems and servers operate in the Internet today, at the times in question related to this matter, and historically.

I earned and received a B.S. in Electrical Engineering from Carnegie-Mellon University in 1977, an M.S. in Information Science from the University of Pittsburgh in 1981, and a Ph.D. in Electrical Engineering from the University of Southern California in 1986. My dissertation was titled "Computer Viruses" and my graduate work in electrical engineering was largely oriented toward issues related to information protection and the design, analysis, and operation of information technology.

I have worked on and developed software and systems for use in digital forensic analysis, some of which are in use by law enforcement and private practices. I have published articles and given presentations in peer reviewed conferences and journals related to information security, digital forensics, and forensic examination and analysis of messages, including publications that identify and discuss some of the techniques used in the analysis performed for this matter. I have also taught and continue to teach courses at the graduate level in the area of digital forensics as well as other related areas and review articles and other publications written by others in these fields. I also regularly give talks at professional society meetings and elsewhere in issues related to digital forensics, information proteciton, risk management, and related issues.

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

I have worked as a research professor creating and teaching graduate level courses in related areas for the University of New Haven, collaborated in the creation of new curriculum for doctorate level graduate degrees in digital forensics for the California Sciences Institute, taught as a guest instructor in digital forensics for the Federal Law Enforcement Training Center, acted as a California POST certified law enforcement instructor in digital forensics, participated in the New York Electronic Crimes Task Force before there were regional task forces, and currently participate in the Bay Area Electronic Crimes Task Force, both of which are run by the United States Secret Service. I have taught courses for and students from government agencies including, without limit, the United States Secret Service, the National Security Agency, branches of the US Department of Defense, state police from many states, agencies that are now members of the Department of Homeland Security, and other intelligence agencies. I have performed and continue to perform research in this area. I led a research and development team at Sandia National Laboratories that developed digital forensic methods and mechanisms, participated in the development of national guidelines for digital forensic evidence, authored chapters in books and two full books on this subject, and performed and continue to perform a wide variety of other activities related to this field. I have recently been invited to give a keynote speech at the 2010 International Federation of Information Processing (IFIP) conference on Digital Forensics in Singapore.

In the late 1990s and early 2000s I did substantial research in the area of deception and the use of deception to influence cognitive mechanisms in people, organizations, computer systems, and combinations thereof, which resulted in several issued patents and published peer reviewed papers in this area. I have designed and implemented deception and counter-deception systems for use in the Internet and in non-public networks, some of which are in widespread use today, and I am familiar with a wide range of deception and counter-deception techniques and methodologies and their applications and limitations, particularly as they apply to information technologies such as those involved in the matters at hand.

I have published more than 200 articles and other papers in the information protection area, I have written several books on the subject, and I am a member of editorial boards of professional publications on issues relevant to this matter. I regularly attend and speak at conferences on related matters and this area has been the focus of my career since the 1970s.

I have included additional background information and my curriculum vitae in Exhibit A of this report, which includes a listing of my peer reviewed publications, and more details of my work history.

Section 2: Summary of my opinions in this matter

On or about February 19, 2008, I was contacted to assist the United States Chess Federation in legal matters related to the issues in this case, and I was subsequently retained to provide services in that regard.

Over the period between that time and the time of this report, I retrieved, received, and reviewed copies of the documents and records identified in this report, performed examinations described herein, and otherwise acted as described herein to understand and report on the issues in this matter.

The matter at hand

In the matter at hand, I have been asked to examine evidence and give opinions related to two issues:

1. The attribution of a set of newsgroup postings identified herein as the "Fake Sam Sloan" postings, to their source or sources.

2. The attribution of unauthorized accesses to and releases of privileged and/or confidential communications to the source or sources of those unauthorized accesses and releases.

My summary opinion

Based on the information that I am aware of at this time, which includes without limit, the information included in this report, the items made available to me to date with regard to this matter, the actions I took as documented within this report, and my knowledge, skills, education, experience, and training in the relevant areas associated with this matter; and subject to revision or amendment based on further facts, information, or analysis, it is my opinion that:

- There are several different and largely independent sets of traces and related evidence that are consistent with the conclusion that some or all of the "Fake Sam Sloan" postings identified herein were initiated and sourced by Hoainhan Truong (a.k.a. Paul Truong), identified further herein, and I have found no basis in the digital forensic evidence to refute such a claim.

- There are several different and largely independent sets of traces and related evidence that are consistent with the conclusion that some or all of the unauthorized accesses to privileged information identified herein were initiated and carried out under the control of Gregory Alexander, identified further herein, and I have found no basis in the digital forensic evidence to refute such a claim.

- There are at least two different and largely independent sets of traces and related evidence that are consistent with the conclusion that the first public releases of the privileged information identified herein were initiated and carried out under the control of Susan Polgar, a party to this litigation, and I have found no basis in the digital forensic evidence to refute such a claim.

- There are several different and largely independent sets of traces and related evidence that are consistent with the conclusion that after Susan Polgar initiated and carried out the release of privileged and/or confidential information identified herein, Gregory Alexander released privileged and/or confidential emails that he had taken, and I have found no basis in the digital forensic evidence to refute such a claim.

A summary of the bases for my opinions

The detailed bases for these opinions is provided later in this report. This summary of the bases is provided for clarity only, and to the extent that there are linguistic differences between the statements in this section and the detailed bases, the detailed bases are more definitive.

Hoainhan Truong appears to be responsible for "Fake Sam Sloan" postings

As detailed below:

- Parties have asserted that a set of postings to the news groups rec.games.chess.politics (RGCP) and rec.games.chess.misc (RGCM) constitute some or all of the "Fake Sam Sloan" (FSS) postings.

- I retrieved and examined more than 200,000 postings made to the news groups RGCM and RGCP.

- I found that the Internet Protocol (IP) addresses recorded as the sources of identified FSS postings were used at the times of those postings by a user logged in as "chessspammer@netzero.net", whose registration data indicated Truong and whose account was paid for over the period in question by Polgar. The terms of service indicate that Truong is responsible, and the same IP addresses and account were used for other business purposes by Polgar and Truong, including a posting to RGCP by Truong under his own name and from his user account at America Online.

- Within 64 out of the more than 200,000 postings to RGCP and RGCM, I found sequences regularly and contemporaneously recorded by servers not in the control or custody of parties to this case that normally record characteristics of computers used to make postings. These sequences

were common only to one posting made by Truong from his AOL account and 63 postings identified as part of the FSS postings. This header is consistent with a computer using a Mozilla version 4.0 Web browser on a computer with a Windows NT 6.0 operating system, using AOL 9.0, Microsoft Internet Explorer version 7.0, and with several other specific versions of specific software packages present, and that were only recorded for Truong's posting and FSS postings. This same information was indicated in 80 records of postings made by Truong's identity at the USCF online forum.

- I found that the same IP addresses recorded as the sources for FSS postings contemporaneously and independently by Web servers not under the control or in the possession of parties to this case, were also recorded in the USCF records, indicating that those same IP addresses were used in postings to the USCF internal forums under the identity used by Truong.

- I found that 9 different "posting account" identifiers were used in the postings identified with FSS. These identifiers are apparently used to indicate a particular login credential, and are recorded by systems not under the control or in the possession of parties to this action. All except one of these posting accounts were used exclusively for postings identified as FSS postings, the same IP addresses used for posting under three of these accounts was also used by Truong for postings from his AOL account, and they were all used from IP addresses also used by Truong's identity at the USCF site contemporaneously.

Gregory Alexander appears to have taken confidential and/or privileged emails

As detailed below:

- Two specific emails at issue and many other emails were identified by Mr. Hough as privileged and/or confidential.

- All parties to those two specific emails have indicated that they did not reveal any information regarding those emails to any person during the applicable time frames.

- Unauthorized accesses to Mr. Hough's email account, which contained the emails at issue, were made after those emails were in existence and stored in Mr. Hough's account, and before they were publicly released.

- At least 100 unauthorized access attempts to Mr. Hough's email account, some or all of which were apparently successful, including those related to the two specific emails identified above, came from IP addresses that:

- ◦ (1) were used in comparable time frames to post to the USCF online forum under Alexander's user name, and/or

- ◦ (2) were used in comparable time frames to post to the usenet forums under Alexander's identity, and/or

- ◦ (3) were used from an Anonymizer account that identified Alexander as the account holder and that was used from IP addresses (a) assigned to Alexander by Comcast, (b) used to make postings to the USCF online forum from Alexander's USCF account, and/or (c) used to make newsgroup postings under Alexander's identity.

- The two specific emails were subsequently first publicly released in emails sent by the account normally used by Susan Polgar, for whom Alexander worked on a volunteer basis, and whose Web site Alexander operated.

Susan Polgar appears to have received and then released the taken emails

As detailed below:

- Two specific emails were identified by Mr. Hough as privileged and/or confidential.

- All parties to those emails have indicated that they did not reveal any information regarding those emails to any person during the applicable time frames.

- After the time at which the emails in question existed, and before they were otherwise publicly released, Alexander, who worked for Polgar on a voluntary basis and operated her Web site, appears to have accessed an email account containing those emails.

- Those emails or portions quoted therefrom were subsequently released to parties not authorized to have them, via emails sent from Susan Polgar's email account, and she has not disputed having sent those emails.

- The dates of these releases are earlier than any other identified release dates of the contents of those emails.

Gregory Alexander appears to have then released taken emails

The sequence of events with respect to the "uscf-said.blogspot.com" Web site is summarized as follows:

- **2008-07-30 at 04:10:13 GMT**: The account "uscf_said@yahoo.com" was created on or about 2008-07-30 at 04:10:13 GMT from an IP address

128.241.107.234. This is in the IP address range of other addresses associated with Anonymizer and under the control of NTT America.

- **2008-07-31 at 02:00:33.739 GMT**: The "uscf-said.blogspot.com" blog was created using the "uscf_said@yahoo.com" Yahoo! account for ownership identification, and accessed at that time from Anonymizer IP address 207.195.241.249. Access through Anonymizer at this time was undertaken by the user identified as Alexander through Anonymizer records and from the IP address 76.121.230.165.

- **2008-07-31 from 02:02 to 03:57 GMT**: The "uscf-said.blogspot.com" blog was accessed repeatedly from IP address 207.195.241.249. Access through Anonymizer at this time was undertaken by the user identified as Alexander through Anonymizer records and from IP address 76.121.230.165.

- **2008-07-31 at 08:02:00 GMT**: The "uscf-said.blogspot.com" blog ws accessed two times from IP address 198.172.201.50.

- **2008-08-06 at 08:59:40 GMT**: IP address 207.67.148.229 was used, to obtain unauthorized access to the randallhough@yahoo.com email account, by an individual identified as Alexander according to the Anonymizer logs and analysis.

- **2008-08-07 at 04:43:00 GMT**: The same IP address, 207.67.148.229 was used to access the blog "uscf-said.blogspot.com"

- **2008-08-08 at 09:13:10 GMT**: The IP address 128.241.108.179 was used to obtain unauthorized access to the randallhough@yahoo.com email account, by an individual identified as Alexander according to the Anonymizer logs and analysis.

- **2008-08-08 at 21:52:39, 22:26:08, and 23:53:19 GMT**: The same IP address, 128.241.108.179 was used to access the "uscf_said@yahoo.com" Yahoo! account.

- **2008-08-31 at 13:22:48 GMT**: The IP address 128.95.225.11 was used to access the blog "uscf-said.blogspot.com". This is also an IP address previously used for postings to RGCP and RGCM under Alexander's identity, and an IP address at the University of Washington from an area at that University where Alexander works.

These comprise all of the sessions where postings and activities to control the "uscf-said.blogspot.com" blog were recorded by Google, the operator of this site. Polgar's attorney identified this as the site where she came to first possess the information. The printout provided thereby appears to show that this site had this information, but postdates Susan Polgar's release of that content.

Section 3: The detailed basis for my opinions

On or about February 19, 2008, I was contacted to assist the United States Chess Federation in legal matters related to the issues in this case, and I was subsequently retained to provide services in that regard.

Over the period between that time and the time of this report, I retrieved, received, and reviewed copies of the documents, records, and discovery responses identified in this report, performed examinations described herein, and otherwise acted as described herein to understand and report on the issues in this matter.

The matter at hand

In the matter at hand, I have been asked to examine evidence and give opinions related to two issues:

1. The attribution of a set of newsgroup postings identified herein as the "Fake Sam Sloan" postings, to their source or sources.

2. The attribution of unauthorized accesses to and releases of privileged communications to the source or sources of those unauthorized accesses and releases.

Electronic messaging, how it works, and related forensic issues

An electronic mail message, or email, from a technical standpoint and as it applies to the specifics of this case, is a sequence of 8-bit binary symbols called bytes, each such byte consisting of any of a subset of the possible 8-bit bytes, originated by some party, and sent from computer to computer through mail transfer agents (MTAs) over the Internet, using one or another version of the simple mail transfer protocol (SMTP). The MTAs at issue in this case are software programs that run in computers attached to the Internet, whose functions are described in relevant detail below.

A newsgroup message is, or posting, from a technical standpoint and as it applies to the specifics of this case, is a sequence of 8-bit binary symbols called bytes, each such byte consisting of any of a subset of the possible 8-bit bytes, originated by some party, and sent from computer to computer through newsgroup servers over the Internet or through other communications paths, using the network news transport protocol (NNTP) or, more recently, through other various means. The servers at issue in this case are software programs that that run in computers attached to the Internet, whose functions are described in relevant detail below.

I will now discuss details of how electronic mails work, then how the supporting infrastructures work, and finally, how newsgroups work.

How email works

How emails are originated and what they contain

When originated, an email normally consists of a series of "lines" starting with a "header" portion, followed by an empty line, followed by a "body" portion, the details of the contents of these being determined by the originator at their sole discretion, but with specific formats interpreted in certain ways by common agreement, fiat, or widely used protocols, typically defined in "Request for Comments" (RFC) documents.

The header portion of an email typically contains a sequence of lines starting with either (1) a header identifier, consisting of a header-name followed by a ":", or (2) one or more spacing characters indicative of a continuation of the header from the previous line. Header lines are comprised of sequences of characters from a subset of the American Standard Code for Information Interchange (ASCII), so limited and constructed in order to make parsing and analysis of messages more standard.

The body portion of an email normally consists of a series of lines containing a similar subset of the ASCII character set as for the header, but without the constraints on header identifiers associated with the header area.

Email messages produce various traces in digital form, and depending on the mechanism used to view these traces, they may appear in different formats. For the purposes of this Report, except where otherwise indicated, the format I will use for presenting traces will look like printouts of the ASCII codes as character sequences that would typically be seen in a text editor which does no special formatting. A sample trace of an email message is shown here as it appears in "native" format (with the header in boldface, emphasis added):

> **From dr.cohen@mac.com Thu, Jul 02 21:03:37 PDT(-0700) 2009**
> **Actually-From:dr.cohen@mac.com**
> **Actually-To: fc@all.net**
> **Received: from dr.cohen@mac.com[17.148.16.92:48524] (EST) by ssl-all-net.local/74.95.10.172:25 (all.net)**
> ** id 2009-07-02-21-03-37.466-10383 for fc@all.net (../mail/fc/2009-07-02-21-03-37.466) on or about 2009-07-02@21:03:37.466**
> **MIME-version: 1.0**
> **Content-transfer-encoding: 7BIT**
> **Content-type: text/plain; charset=US-ASCII; format=flowed; delsp=yes**
> **Received: from [10.0.1.2]**
> **(74-95-10-169-SFBA.hfc.comcastbusiness.net [74.95.10.169])**
> **by asmtp017.mac.com (Sun Java(tm) System Messaging Server 6.3-8.01 (built Dec 16 2008; 32bit)) with ESMTPSA id <0KM600FRJTZD6U00@asmtp017.mac.com> for fc@all.net; Thu, 02 Jul 2009 21:04:27 -0700 (PDT)**
> **Message-id: <1B1E36C9-7CC0-4E41-B023-6BB0A9F6DFD3@mac.com>**
> **From: Cohen Fred <dr.cohen@mac.com>**

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

To: Fred Cohen <fc@all.net>
Subject: Test email - this is the "Subject" line within the "header" section of the email.
Date: Thu, 02 Jul 2009 21:04:24 -0700
**X-Mailer: Apple Mail (2.935.3)**

This is a test email - and this is its body.

I can put anything I want into this body, including URLS, like http://all.net/
and almost anything else I want to put here.

FC
- This communication is confidential to the parties it is intended to serve -
Fred Cohen & Associates   tel/fax: 925-454-0171
http://all.net/   572 Leona Drive   Livermore, CA 94550
Join http://tech.groups.yahoo.com/group/FCA-announce/join for our mailing list

This example email message was sent from my "dr.cohen@mac.com" electronic mail address to my "fc@all.net" electronic mail address. Here is what the trace looks like when I view parts of it through my email graphical user interface in the Mac OSX operating system's mail program:
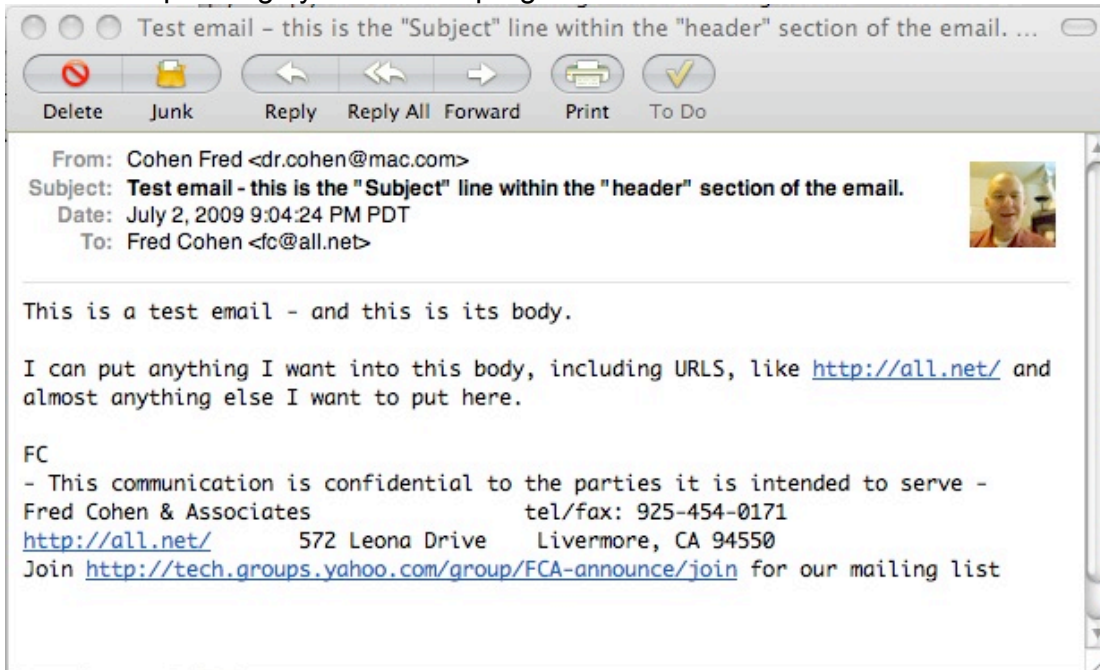
Here is what is displayed when the graphical interface depicts parts of this trace as part of the list of emails in my mailbox:

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

When I send an email using a non-graphical interface, such as through the use of the "telnet" command, which has proven reliable and is widely used for communications under the Transmission Control Protocol (TCP) used by mail transfer agents to transport the higher level protocol elements, the process works as follows (my typing in bold):

(1) I use the "host" command to identify the email servers for the destination domain (mac.com in this case).

(2) I then use the "telnet" command going to TCP port 25 (as will be discussed later) to start sending an email.

(3) Next, I enter a "HELO" protocol line and get a response.

(4) I enter a "MAIL FROM:" protocol line and get a response.

(5) I enter a "RCTP TO:" protocol line and get a response.

(6) I enter a "DATA" protocol line, and get a response.

(7) I enter lines of test that constitute the email, including the header and body areas.

(8) I enter a line with only a "." on it to signal the end of the email message and get a response.

(9) I enter the "QUIT" protocol element to end my email session.

At each step, the server on the other side replies with different messages indicating whether or not I have permission to continue, and it can refuse permission at any time by simply providing a negative response or closing the connection.

```
>host mac.com
mac.com has address 17.250.248.32
mac.com mail is handled by 10 smtp-mx6.mac.com.
mac.com mail is handled by 10 smtp-mx1.mac.com.
mac.com mail is handled by 10 smtp-mx2.mac.com.
mac.com mail is handled by 10 smtp-mx3.mac.com.
mac.com mail is handled by 10 smtp-mx4.mac.com.
mac.com mail is handled by 10 smtp-mx5.mac.com.
>telnet smtp-mx6.mac.com 25
Trying 17.148.20.69...
Connected to smtp-mx6.mac.com.
Escape character is '^]'.
220 smtpin138-bge351000 -- Server ESMTP (Sun Java(tm) System Messaging Server
6.3-8.01 (built Dec 16 2008; 32bit))
helo all.net
250 smtpin138-bge351000 OK, [74.95.10.169].
mail from:<fc@all.net>
250 2.5.0 Address Ok.
rcpt to:<dr.cohen@mac.com>
```

```
250 2.1.5 dr.cohen@mac.com OK.
data
354 Enter mail, end with a single ".".
Subject: This is the subject line I typed in
X-other-header: This is another header line I typed in.
Received: from fc@all.net from wherever I was at the time - and so forth.
X-more things: I can put anything I want in a header area

This is the body of the email.
I can type in whatever I want here as well.

When I am don, I exist
.
250 2.5.0 Ok.
quit
221 2.3.0 Bye received. Goodbye.
Connection closed by foreign host.
```

When I read this email message, I get the following "native format" trace:

```
Return-path: <fc@all.net>
Received: from smtpin138-bge351000 ([10.150.68.138])
 by ms283.mac.com (Sun Java(tm) System Messaging Server 6.3-7.04 (built Sep 26
 2008; 64bit)) with ESMTP id <0KM6009HGUIEK970@ms283.mac.com> for
 dr.cohen@mac.com; Thu, 02 Jul 2009 21:15:50 -0700 (PDT)
Original-recipient: rfc822;dr.cohen@mac.com
Received: from all.net ([74.95.10.169])
 by smtpin138.mac.com (Sun Java(tm) System Messaging Server 6.3-8.01 (built Dec
 16 2008; 32bit)) with SMTP id <0KM600FV0UFIZOD0@smtpin138.mac.com> for
 dr.cohen@mac.com (ORCPT dr.cohen@mac.com); Thu,
 02 Jul 2009 21:15:50 -0700 (PDT)
From: fc@all.net
X-Brightmail-Tracker: AAAAAA==
Date-warning: Date header was inserted by smtpin138.mac.com
Date: Thu, 02 Jul 2009 21:15:23 -0700 (PDT)
Message-id: <0KM600FVGUFSZOD0@smtpin138.mac.com>
Subject: This is the subject line I typed in
X-other-header: This is another header line I typed in.
Received: from fc@all.net from wherever I was at the time - and so forth.
X-more things: I can put anything I want in a header area

This is the body of the email.
I can type in whatever I want here as well.

When I am don, I exist
```
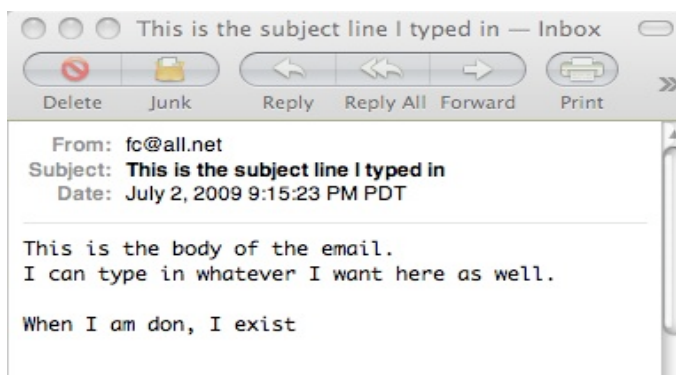
And when I view it in the graphical interface, it looks like this:

Whatever I place in the email and send through the protocol appears in the message as received, and it can be viewed in different ways using different interfaces. In addition, certain fields are added by the receiving computer, that I never typed in, and by other computers in the path from the origination to the destination.

Any party that has the ability to send messages over the Internet using the SMTP protocol may place any sequence of bytes into a message and originate that message by contacting an SMTP server and requesting delivery.

How MTAs send and receive emails and what they record

When an MTA is contacted with a proposed email message, it is first asked, through the SMTP protocol, whether the self-identified sender is allowed to send the message to the identified recipient(s). The message is then transferred if and only if the recipient authorizes it to be sent. This mechanism normally prevents misdirected email messages or email messages not sent to an actual and current user on a computer from ever being sent.

Many MTAs record the Internet Protocol (IP) address (a series of 4 bytes for IP version 4 (IPv4), or 16 bytes for IP version 6 (IPv6)) as presented in the IP datagrams used to send each message to them. In this case, for the issues involved in this report, only IPv4 IP addresses are relevant. Records of the processing of each email message is usually recorded both within system log files on the system operating each MTA, and within a "Received:" header that each MTA adds to the beginning of each message they choose to receive. This MTA reception process alters the incoming message by adding this "Received:" header to the beginning of the incoming message's header.

The IP address recorded by an MTA normally reflects the sequence of bytes contained within an IP datagram, typically by representing each byte of the IP address as a series of up to 3 decimal digits whose values range from 0 to 255, the full range of possible values for each byte, and by separating each such value by a "." in the case of IPv4. For example, the IP address that is present in

most of the email messages sent from my office is represented as 74.95.10.169 in this format.

The nature and reliability of the information recorded

The recorded value is not always probative in terms of identifying the particular computer whose MTA sent the message, because the routing of IP traffic in the Internet is sometimes complicated by the path by which datagrams are sent. Since there are only a total of about 4 billion possible 4-byte values for an IPv4 address, and since there is no such limit on the number of actual computers that may connect, either directly or indirectly, to the Internet; gateway computers, proxy servers, and any number of other mechanisms, may translate addresses of datagrams passing through them.

For example, the computers that originate email messages sent from my office pass through my network address translation (NAT) gateway computer, and they originate messages by sending them from IP addresses (10.0.1.2) in the examples above) that are different from the IP addresses that appear in the datagrams arriving at distant MTAs (74.95.10.169). Some of my internal computers are laptop computers, and they may be used from different locations, like a library, an office where I am having a meeting, or elsewhere. In this case, these computers are assigned IP addresses by the provider of local Internet access, and the IP addresses of the datagrams sending email messages from those locations will be those assigned by that provider. Those providers may also use gateways, proxy servers, or any other mechanism to provide those services. For these reasons, the IP address recorded by an MTA may not be the same IP address as the computer that originated the message.

For hardware efficiency reasons, one computer may also operate with many IP addresses, and one IP address may operate with many domain names. Similarly, for resiliency against failures or to increase apparent performance, many computers may share the same external IP address or name. For example, the computers that serve requests for Web pages for the domain "all.net" that I operate, also serve requests for Web pages for other domains, and there are two different IP addresses that may handle these requests, so that if one computer fails, the other can take over the processing. Similar methods are used to provide increased performance for heavily used Web sites and email servers.

Forensic issues with records and traces related to emails

Any party along the path of an email, including without limit, the final recipient or any party that comes into possession of or gains write access to a message or the media containing it, may add to, remove from, delete, replace, alter, or otherwise place any sequence of bytes into any message. Starting with the first possession of a message by a recipient and until the time, if any, that they

release possession to a third party, they are in sole control over the message, including its header and contents, and may do whatever they wish to it at their sole discretion. For this reason, the content of a message alone cannot be used to reliably identify where a message was originated, who originated it, what it originally contained, or even whether it was ever originated or sent anywhere. Any email-like sequence of the sort relevant to this matter can be generated by anyone with a computer.

Therefore, proper handling of messages and related records, including, without limit, the various traces and records associated with their processing, and the people, tools, and mechanisms used to process them, is vital to being able to authenticate the integrity of individual emails or collections of those emails and to being able to attribute emails to their origins. These records are normally retrieved for legal purposes through the use of timely preservation orders and subpoenas for these sorts of normal business records.

The "Received:" headers and other headers added en route, typically contain optional traces of information recorded by each MTA at its sole discretion, reflecting such information as the source, destination, routing, date and time, and other similar information about activities undertaken by the MTAs. This includes, without limit, MTA-generated "unique identifiers" such as the "SMTP ID" or "ESMTP ID" field within a "Received:" header, the "Message-ID:" header, and any number of other similar sorts of headers produced by different MTAs under different circumstances, at their sole discretion.

How the Internet works at a deeper level

As additional background, I will describe some basic information about how the Internet and Internet-based email of the sort relevant to this matter works, so that proper context can be applied to the issues in this matter, and clarity can be brought to various allegations.

The physical infrastructure

The Internet is, in essence, a collection of physical infrastructure elements consisting largely of wires, cables, optical fibers, and other transmission media including, without limit, radio transmission media, transmission and reception devices, digital to analog and analog to digital converters, digital switching and routing equipment, end-point switches and hubs, and computers of various sorts. By physically interfering with the underlying physical infrastructure, signals or devices can be altered so as to create forgeries and other sorts of mischief.

The Internet Protocols (IP)

The unifying concept underlying the Internet is that it uses a set of protocols called, as a group, Internet Protocol (IP),[RFC791] to communicate. By using a common set of protocols, the Internet allows any internal mechanisms of attached systems to use translations of their own making to and from the common protocol, IP, so as to facilitate communications between parties and devices. The IP protocols are loosely and imprecisely defined by a set of documents called "Request for Comments" (RFC) documents that are, as they are named, requests to the Internet community for comments on the use of these common methods of exchange in order to allow communications to take place. The RFCs of interest to this case are descriptions of syntax and semantics associated with communications between pairs of computers, also known as communications protocols.

IP exchanges information using sequences of binary symbols (bits) representing datagrams. A datagram is a sequence of bits of particular format and comprised of different parts with defined properties, portions of which are used by different physical devices within the Internet to make decisions about how to send and interpret the contents. IP datagrams are of limited maximum length, and so there are mechanisms to allow longer messages of various sorts to be broken into smaller sized messages that fit into datagrams to operate in different sorts of infrastructures, and to be reassembled at destination points for use. At the IP level, delivery of datagrams depends only on some of the initial bits of the datagram that indicate a pair of source and destination IP addresses. Because there are different versions of IP, the descriptions I will use will be of version 4 of the IP protocol (IPv4), the one most commonly in use today. Because datagrams are simply sequences of bits and can be generated by any computer anywhere, a sender or intermediary can potentially alter or create datagrams with IP addresses that are not those assigned for their use by the Internet Assigned Number Authority or the Internet registrars who register "ownership" of IP addresses. Such alteration would constitute IP address forgery.

The TCP and UDP IP protocols and higher level services

Datagrams are delivered in the Internet using "best effort" by participating parties. As a side effect, datagrams may arrive in a different order and with different delays than the way they were sent. As a result, there are three alternatives for meaningfully constraining the sequences associated with protocols between parties: (1) exchanged messages can be limited to a single datagram, (2) applications using datagrams can be designed so that ordering is unimportant, or (3) an additional layer of protocol can be used to assure ordered delivery between endpoints. In this matter, two of these techniques are relevant to the issues at hand because two protocols are at issue. One protocol, called

user datagram protocol (UDP)[RFC768], is used to exchange messages that require only a single datagram to be used for a request and one for response. The other, called transmission control protocol (TCP)[RFC793] adds additional layers of protocol within datagrams that allows endpoints to sort arriving datagrams so as to assure that delivery of content is in the same order as transmission. Again, because these protocols are simply sequences of bits embedded within sequences of IP datagrams, it is possible to create or alter datagrams so as to forge portions of exchanges between parties at these embedded protocol layers.

The UDP and TCP protocols are used to support higher level services in the Internet. In particular, and without limit, UDP is used to support the domain name system (DNS) and TCP is used to support the simple mail transfer protocol (SMTP) and other related services. These two protocols are related to the issues in this case.

The DNS UDP protocol and domain name registration and use

The domain name system is used to allow people and their programs to use names consisting of sequences of alphabetic, numeric, and other symbols instead of IP addresses to identify resources within the Internet. As an example, the universal resource locators (URLs) commonly used in the world wide web (Web) typically use names like "all.net" to identify a domain name. The DNS system allows people and their programs to look up names and translate them into IP addresses. For example, by using the command "host all.net" on one of my computers, I run a program on my computer called "host" that looks up "all.net" using the domain name system and returns the IP address 74.95.10.172 as the result. These four integers separated by "."s indicate the four octets (8-bit sequences) of bits contained within the actual IP datagram in the area of the datagram designated for the destination (or source) address, depending on whether the datagram is sent to (or from) the "all.net" site. Each octet is represented in this notation by a decimal number, so that the number "10" represents the sequence of bits "00001010". If the datagram is observed in transit, these bits will appear in the identified location within that datagram, and these bits will be used by the routing and switching infrastructure of the Internet to decide how to route the datagram through the Internet to its destination.

Because more than one domain name can be serviced by one IP address, looking up the domain name manalytic.com, another one of the domains I "own" and operate, yields the same IP address. DNS also supports "reverse" DNS lookup, but to a more limited extent. For example, when I looked up 74.95.10.172, I got "74-95-10-172-SFBA.hfc.comcastbusiness.net" as part of the response. This is because there may be many domain names associated with each IP address, and because different domain name servers are used for

forward and reverse DNS lookups. In addition, in some cases it is impossible to return the list of all of the domain names associated with an IP address using the UDP protocol in the manner that the DNS protocol operates because UDP cannot maintain ordering and only so much information can be placed in one datagram. Since there is no limit to the number of host names per IP address, it would be impossible at some point to fit the next name into the same UDP datagram.

The DNS registration mechanisms allow unique domain names to be registered within top level domains (TLDs) and lower level subdomains to be controlled by the registrants. For example, "all.net" is unique domain name consisting of two parts; "all" and the TLD "net". The "." in the middle is a separator between the parts of the domain name. Within the "all.net" portion of the domain name space, I control subdomains at my sole discretion, so I can create any number of subdomains, such as "www.all.net", "mail.all.net", and so forth, change those domain names, delete domain names, and use those domain names in whatever manner I wish and at any time.

I do this by creating records in domain name servers that I operate or control to reflect the translation between domain names and IP addresses. I can associate any syntactically valid name with any IP address within these records, however; this also means that I could create a DNS record such as "all.com" and place it in my domain name records. Since I don't "own" the "all.com" domain name, this could be considered a forgery. While there is no technical mechanism to prevent me from doing this, the way the Internet operates prevents this from being effective in normal use because, in order to find the DNS server serving a domain name, the requesting computer typically uses a DNS server that they trust, which in turn starts the lookup process by going to officially authorized and authoritative top level domain name servers. These servers then are tasked with identifying the authorized authoritative DNS servers for each registered domain, which the requesting DNS server then queries to find the authoritative answer, which it returns to the user. By entering and altering the top level DNS servers, the authoritative DNS servers for a domain, the trusted DNS servers involved in a lookup, or the datagrams used in the exchanges between these servers and/or the user's computer, an attacker could forge DNS responses and redirect traffic from legitimate locations.

Gateway computers, proxy computers, and address translation

By design, the Internet is intended to allow networks of computers to communicate with other networks of computers through many methods, including without limit, gateway computers, address translation mechanisms, and proxy mechanisms. As a result, the IP address seen at the receiving end of a communication may be different from the IP address configured in the sending

computer. As an example, within my infrastructure, I use a network address translation (NAT) gateway to allow multiple computers to communicate to the Internet through a single IP address. This is very common and most enterprises of substantial size use such gateways. Among other things, this provides for private [RFC1918] addresses within organizations that are not normally routed over the open Internet, reduces the need to consume large numbers of the finite space of available IP addresses, allows internal management to be independent of external management, and reduces the need to change internal addresses when changing external service providers.

As a result, when a computer within my internal address space places an IP address within the header of a message or otherwise records its address as part of its communication with other computers across the Internet, it uses the only address it has, an internal address that is different from the external address seen by the Internet. Similarly, within my infrastructure, as in many other companies, I maintain my own domain names. When a computer within my internal infrastructure communicates to computers across the Internet, if it places a domain name within the header or body of an email or other transmission, it uses the only domain name it has, an internal domain name, that is different from the external address seen by the Internet.

Another common practice is to use proxy servers or other similar methods to reduce the direct exposure of internal computers to attack from the Internet. This is advised in common practice for those using Internet services and is part of many modern firewalls and other similar security devices. A computer operating through a proxy server and placing true and accurate information within headers of emails or other content it transmits or originates may appear to be providing inaccurate information because of the mechanisms by which the datagrams are delivered to and from the Internet.

A computer configured to operate from an internal network or not properly configured may place information in headers of emails or other messages that are not accurate in terms of the external environment, even though they accurately depict the information available to the computer in which the mechanisms are operating. Indeed, as delivered, many computers have default settings that do not accurately reflect the use of those computers. There is no mandate that users or operators of computers reconfigure their systems to meet some external standard of naming conventions in order to be able to use the Internet and indeed it is common for people who operate computers, even in large numbers, not to make such changes unless they are necessary for functioning of those systems.

A computer that connects to the Internet through a "tunnel" using a technology such as Asynchronous Transfer Mode (ATM) or any of a host of other technologies that route traffic through intermediary machines transparently can

sometimes get an address at one end of the tunnel that is different from the address at the other end of the tunnel. For computers not acting as servers, this may go unnoticed for a long period of time and have no negative effect on the operation of the computer in the Internet.

There are many other similar things that can occur that can cause a mismatch between honestly or automatically placed information in headers or bodies of emails or other content.

RFCs are not strictly followed in normal Internet use

As someone who has implemented, analyzed, and reviewed many Internet systems, including many security devices and methods related to Internet security, I am aware of numerous cases where following the RFCs would be problematic and in which security demands that RFCs not be strictly followed.

For example, I wrote a series of articles in the 1990s titled "Internet Holes" in which I examined some of the RFCs to identify technical flaws that could be exploited.

From a purely technical standpoint, in the Internet, RFCs are not uniformly or consistently followed as a matter of course, and their interpretation is widely considered subjective in many cases. There are inconsistencies in the RFCs, including the ones identified in this matter, and the things identified by Plaintiff as violations in this case are common occurrences in emails sent and received with products including most commercial products on the market today.

News postings and how they operate

News groups, historically, operated using a variety of protocols operated by a widely diverse set of individual operators who communicated updates in news between sites using mechanisms like Unix-to-Unix-Copy (UUCP) and other similar mechanisms, many of which operated over dial-up connections starting long before the Internet and its predecessor the ARPA-net existed. The usenet news system is discussed in detail in [RFC850].

As these news groups emerged, and as the Internet grew, protocols like "Network News Transport Protocol" (NNTP) [RFC977] emerged, providing the means to send and receive news between servers containing news groups and users on their computers.

In order to take advantage of these protocols and allow users to view and post messages to news groups, a wide variety of different news readers came to be developed by different parties. While the protocols specified the means of communications, the individual mechanisms used to post and read messages used their own variations on how they implemented to optional and unspecified

elements of the protocols, the fields provided within those protocols, and the contents contained within those fields.

News postings generally include a "head" and "body" and are identified by the name of the newsgroup (e.g., rec.games.chess.politics) and an article number (e.g. 123456). The NNTP protocol allows the mechanism using it to identify a newsgroup and article number and retrieve the head, body, or entire article, or to post a new article. It also provides for listing article numbers present.

The defined format of a news posting is, according to [RFC850], specified in [RFC821], the same format used to define email messages above. News postings, like emails using that specification,

How news postings are originated and what they contain

When originated, a news posting normally consists of a series of "lines" starting with a "header" portion, followed by an empty line, followed by a "body" portion, the details of the contents of these being determined by the originator at their sole discretion, but with specific formats interpreted in certain ways by common agreement, fiat, or widely used protocols, typically defined in "Request for Comments" (RFC) documents.

The header portion of a news posting typically contains a sequence of lines starting with either (1) a header identifier, consisting of a header-name followed by a ":", or (2) one or more spacing characters indicative of a continuation of the header from the previous line. Header lines are comprised of sequences of characters from a subset of the American Standard Code for Information Interchange (ASCII), so limited and constructed in order to make parsing and analysis of messages more standard.

The body portion of an email normally consists of a series of lines containing a similar subset of the ASCII character set as for the header, but without the constraints on header identifiers associated with the header area.

News postings produce various traces in digital form, and depending on the mechanism used to view these traces, they may appear in different formats. For the purposes of this Report, except where otherwise indicated, the format I will use for presenting traces will look like printouts of the ASCII codes as character sequences that would typically be seen in a text editor which does no special formatting.

Demonstrations of how traces are produced by newsgroup mechanisms

In order to demonstrate how traces come to be in newsgroup postings and how they may be interpreted, I created a newsgroup at "Google.com" and named it "test", with email address "testgooglegroupsmechanisms@googlegroups.com". This allowed me to perform these tests without interfering with any other parties.

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

A sample trace of a news posting that I made to demonstrate these mechanisms is shown here as it appeared when I had my Web browser have the Web site display all of the details of the headers:

MIME-Version: 1.0
Received: by 10.101.1.1 with SMTP id d1mr1015189ani.4.1252770915510; Sat, 12
    Sep 2009 08:55:15 -0700 (PDT)
Date: Sat, 12 Sep 2009 08:55:15 -0700 (PDT)
X-IP: 74.95.10.169
User-Agent: G2/1.0
X-HTTP-UserAgent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_8; en-us)
    AppleWebKit/531.9 (KHTML, like Gecko) Version/4.0.3 Safari/531.9,gzip(gfe),gzip(gfe)
Message-ID: <e5963a83-ffd6-4640-a40f-52617f7746b7@m3g2000pri.googlegroups.com>
Subject: test2 - posted from Web
From: fc <dr.co...@mac.com>
To: test <testgooglegroupsmechanisms@googlegroups.com>
Content-Type: text/plain; charset=ISO-8859-1

I will call each header, including any "continuation lines" (when the line after a header line starts with spaces, it is a continuation of the same header) an "entry", and indicate the first header line and all of the continuations as "entry 1", and so forth. This entry 1 is "MIME-Version: 1.0", which is very common, and entry 2 is the "Received:" header including the third line indicating "   Sep 2009 ...".

For clarity, using the mechanisms on my computer that are designed to list these things, I confirmed that I was using an Intel-based MacBook running the OSX operating system, version 10.5.8, configured for English language, through the Safari browser (version 4.0.3 (5531.9) that comes with the MacBook. My external IP address for this session was 74.95.10.169, and I posted it on Saturday, September 12, 2009 at or about the time identified in the headers.

Note that the "X-HTTP-UserAgent:" header (entry 6) indicates information consistent with my computer and configuration details, that the date and time are reasonably in agreement with my computer system, and that the "X-IP:" header accurately reflects the IP address of the computer I used to post this message.

I then repeated the process of posting a message to this news group, but this time, I used a different browser, "FireFox", from the same computer, producing this result:

MIME-Version: 1.0
Received: by 10.150.130.5 with SMTP id c5mr1267757ybd.39.1252771609438; Sat,
        12 Sep 2009 09:06:49 -0700 (PDT)
Date: Sat, 12 Sep 2009 09:06:49 -0700 (PDT)
X-IP: 74.95.10.169
User-Agent: G2/1.0
X-HTTP-UserAgent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US;
        rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2,gzip(gfe),gzip(gfe)

Message-ID: <af9181af-97f0-4fa9-9a37-e728aa4e739f@f20g2000prn.googlegroups.com>
Subject: test3
From: fc <dr.co...@mac.com>
To: test <testgooglegroupsmechanisms@googlegroups.com>
Content-Type: text/plain; charset=ISO-8859-1

This result shows entry 6 as the "X-HTTP-UserAgent:" header, which accurately reflects that difference between the two browsers running on the same computer, showing version information consistent with my current version of FireFox, provides the same "X-IP:" address entry, and therefore accurately demonstrates the difference between the two uses.

This example email message was sent from my "dr.cohen@mac.com" electronic mail address to my "fc@all.net" electronic mail address. Here is what the trace looks like when I view parts of it through my email graphical user interface in the Mac OSX operating system's mail program:

I then posted a third message, in this case, using my emailer, and examined the resulting posting:

```
Received: by 10.143.21.37 with SMTP id y37mr1987767wfi.29.1252772136672;
        Sat, 12 Sep 2009 09:15:36 -0700 (PDT)
Received: by 10.143.21.37 with SMTP id y37mr1987766wfi.29.1252772136657;
        Sat, 12 Sep 2009 09:15:36 -0700 (PDT)
Return-Path: <dr.co...@mac.com>
Received: from asmtpout011.mac.com (asmtpout011.mac.com [17.148.16.86])
        by gmr-mx.google.com with ESMTP id
19si1204806pzk.8.2009.09.12.09.15.36;
        Sat, 12 Sep 2009 09:15:36 -0700 (PDT)
Received-SPF: pass (google.com: domain of dr.co...@mac.com designates
17.148.16.86 as permitted sender) client-ip=17.148.16.86;
Authentication-Results: gmr-mx.google.com; spf=pass (google.com: domain
of dr.co...@mac.com designates 17.148.16.86 as permitted sender)
smtp.mail=dr.co...@mac.com
MIME-version: 1.0
Content-transfer-encoding: 7BIT
Content-type: text/plain; charset=US-ASCII; format=flowed; delsp=yes
Received: from [10.0.1.2]
 (74-95-10-169-SFBA.hfc.comcastbusiness.net [74.95.10.169])
 by asmtp011.mac.com (Sun Java(tm) System Messaging Server 6.3-8.01
(built Dec
 16 2008; 32bit)) with ESMTPSA id <0KPV001FA95Z2...@asmtp011.mac.com>
for
 testgooglegroupsmechanisms@googlegroups.com; Sat,
 12 Sep 2009 09:15:36 -0700 (PDT)
Message-id: <59A0417B-A4F5-4933-8AD6-F518ACF6FD77@mac.com>
From: Cohen Fred <dr.co...@mac.com>
To: testgooglegroupsmechanisms@googlegroups.com
Subject: test from emailer
Date: Sat, 12 Sep 2009 09:15:35 -0700
X-Mailer: Apple Mail (2.936)

test posting
- This communication is confidential to the parties it is intended to
serve -
```

```
Fred Cohen & Associates              tel/fax: 925-454-0171
http://all.net/       572 Leona Drive    Livermore, CA 94550
Join http://tech.groups.yahoo.com/group/FCA-announce/join for our
mailing list
```

This posting shows a different sequence of headers, so that entry 6 is not a "X-HTTP-UserAgent:" Header, but rather it is an "Authentication-Results:" header entry. Thus the different mechanism of posting led to a different sequence and location of entries within the headers.

This posting also accurately indicates additional information relating to the mechanism that sent the posting, including such details as "74.95.10.169", my sending IP address (in one of the "Received:" headers), which is the same address identified for my Web postings above, and header like "Message-id: <59A0417B-A4F5-4933-8AD6-F518ACF6FD77@mac.com>" that identifies the message in a unique numbering scheme generated by the mailing system to allow the message to be traced for service and other purposes.

How news postings are transported

Unlike email, which is generally directed from point to point, newsgroup postings are intended to be widely distributed in more of a broadcast approach. As a result, the sets of servers and protocols providing newsgroup services are oriented toward the rapid and reliable duplication and distribution of messages rather than just their delivery.

Once a newsgroup server gets a posting, it has two jobs. One is to provide it as a news feed to its direct users, and the other is to provide the news to and get news updates from other newsgroup servers. There are different protocol elements used for posting and retrieving posts than for controlling the flow of news as it travels from place to place. In particular, the protocols identified as "cancel", "ihave", "sendme", "sendsys", "newgroup", and "rmgroup" are used to create and delete groups, cancel articles, indicate what messages are available, request that they be sent, and get information about communicating systems. Through the use of these commands, servers that support news services exchange newsgroup updates around the world over time.

In addition, not all news servers honor all commands. For example, some servers do not delete messages even if they are cancelled, and retain copies of those messages regardless of attempts to destroy them.

The transport of news may also be done over different channels, including, without limit, using unix to unix copy (UUCP) over dial-in lines, through electronic mail, of over transport arranged between individual news servers or their owners.

Other issues with newsgroup postings

News postings are, in many ways, similar to emails. For example, and without limit:

- Newsgroup servers typically don't record the entire path of travel of a newsgroup posting, but rather trust the initial recording for a source. While internal logs may demonstrate the path of travel for a posting, these are not typically retained very long and are rarely available except through legal process.

- All of the restrictions associated with the recording of IP addresses hold true for news servers just as they do for MTAs. Thus, the presence of gateways, proxy servers, NAT mechanisms, and so forth, all affect the available information at the time of recording.

- All of the forensic issues with emails apply to newsgroup postings, but in the case of newsgroup postings, as the copies of the news get spread through the infrastructure, the inherent redundancy of the system makes alteration without detection far harder as time passes.

- While newsgroup posting have historically been undertaken by news readers that operate on the user's computer, increasingly, they are used through Web interfaces, such as the ones at Google.com. In such cases, like any Web browsing, the sorts of records kept and the locations at which they are kept are related to the records kept by the browser at the user's computer and the server at the Web services computer. This we see the Web browser information recorded in headers of postings where a Web browser was used, and very different information recorded when a different interface is used.

- Depending on the interface used, very different header sequences and contents may appear, but the IP addresses recorded by the news server receiving the posting should be faithful to what it observed in the packets it received in processing the requests it serves, unless it is designed to falsify these records.

News summary

Postings made to news groups combine information placed in headers from different automated processes performed by different computers. As a result of variations in the different computers, processes, configurations, hardware, software, and event sequences that cause these postings to come to be, these header fields appear in particular orderings with particular values.

The information commonly available from the various header put in place by various mechanisms may include, without limit, IP addresses, user identifying information, system information, Web browser information, hardware information, operating system information, and other similar sorts of information.

With the exception of intentional forgeries, these commonalities in headers indicate commonalities in mechanisms that produce those common sequences. While such sequences are not necessarily unique or uniquely identifying because many different mechanisms may produce similar sequences, the same mechanism applied in the same manner, normally produces the same sorts of sequences.

How forensic examination reveals probative information

The various traces, including without limit, the information contained in headers of messages, the traces and records produced by MTAs and newsgroup servers, and other related records of handling and process controls, normally form a redundant set of consistent traces and records of what took place. These traces and records can normally be related to each other and to other traces and records to provide a level of certainty as to the integrity of message sequences, their sourcing, and their delivery path, from an evidentiary standpoint.

For example, the traces and records produced by the MTAs along the path from source to destination should collectively demonstrate the path and timing of the message, details of any carbon copies made along the way, date and time stamps that are consistent with the delivery process from end to end, and in conjunction with the finally delivered messages, the sizes, message identifiers, and number of times a message was handled by MTAs, should also be consistent.

If the traces within message headers are not internally consistent, if they are not consistent with related information, if they are not consistent with other traces and records such as the logs from newsgroup servers and MTAs, or if they present information that cannot be true according to real-world events, such as having times that are inconsistent with causality, this indicates that the handling of the messages or related records was not properly undertaken, and that the information contained in those messages cannot be relied upon for the purposes of attribution to sources, delivery dates and times, delivery paths, or for other related purposes.

If some of these traces or records are never generated or are not preserved, it may become difficult or impossible to definitively validate or challenge the validity of messages. For example, if traces produced by the final recipient MTAs or initial recipient News servers are not retained, if records from distant MTAs are

not preserved in time, or if records contained within headers are not properly preserved and chains of custody maintained, the necessary records may never be available or may prove unreliable.

Digital forensic evidence in general, is fragile, easily altered, complex to understand, and latent in nature. Proper handling, use of forensically sound tools, and skills, knowledge, and expertise beyond that of most people, are required in order to reliably preserve, produce, examine, and interpret these sequences.

Forensic issues with records and traces related to messages

Any party along the path of a message, including without limit, the final recipient or any party that comes into possession of or gains write access to a message or the media containing it, may add to, remove from, delete, replace, alter, or otherwise place any sequence of bytes into any message. Starting with the first possession of a message by a recipient and until the time, if any, that they release possession to a third party, they are in sole control over the message, including its header and contents, and may do whatever they wish to it at their sole discretion. For this reason, the content of a message alone cannot be used to reliably identify where a message was originated, who originated it, what it originally contained, or even whether it was ever originated or sent anywhere. Any message-like sequence of the sort relevant to this matter can be generated by anyone with a computer.

Therefore, proper handling of messages and related records, including, without limit, the various traces and records associated with their processing, and the people, tools, and mechanisms used to process them, is vital to being able to authenticate the integrity of individual messages or collections of those messages and to being able to attribute messages to their origins. These records are normally retrieved for legal purposes through the use of timely preservation orders and subpoenas for these sorts of normal business records.

In the case of newsgroup postings, the inherent redundancy of the news distribution process provides a multitude of records that are potentially available and that may be used to resolve differences, if any are identified.

The parties to this and related matters

The parties to this matter and related parties related to related matters include, without limit, and are identified by me herein as:

> **Polgar**: Susan Polgar, a party to this legal action.

> **Truong**: Hoainhan Truong (a.k.a. Paul Truong), the spouse of Susan Polgar.

USCF: The United States Chess Federation, a party to this legal action.

Sam Sloan: Samuel H. Sloan, identified within IL-A, itself identified below.

Alexander: Gregory Alexander, currently under indictment per CR-09 00719 for violations of 18 U.S.C. 1030(a)(2)(C) and (c)(2)(B)(ii) - intentionally accessing a computer without authorization, and 18 U.S.C. 1028(A)(a)(1) - Aggravated Identity Theft.

The materials reviewed relative to this matter

The materials reviewed with respect to this matter are referenced herein according to the names given here and included as references to and part of this report in the directory called "Referenced". Items marked with an "*" are included as part of this Report and include materials I produced as a result of the processes used to produce this report.

- ***RGCP**: A set of files resulting from my retrieval using network news transport protocol and subsequent analysis of news postings to the "rec.games.chess.politics" news group, comprised of more than 120,000 such postings, with filenames named by combining RGCP with the newsgroup article number (e.g., RGCP326446).

- ***RGCM**: A set of files resulting from my retrieval using network news transport protocol and subsequent analysis of news postings to the "rec.games.chess.misc " news group, comprised of almost 100,000 such postings, with filenames named by combining RGCM with the newsgroup article number (e.g., RGCM200380).

- **FSSP**: A file called "USCF Post by Fake Sam Sloan (REC'D 10.24.07) - KRON001556.txt" identified to me as containing exampled believed to be postings to one or more news groups by the party identified as the "Fake Sam Sloan".

- **IL-Complaint**: A file named "Complaint (DATED 12.29.08).PDF" containing what was provided to me as the complaint of the United States Chess Federation v. Susan Polgar and Hoainhan Truong (a.k.a. Paul Truong), and action files in state court in Illinois.

- **IL-Exhibits**: A file named "Exh A - M to Complaint (DATED 12.29.08).PDF", containing what was provided to me as the Exhibits to the complaint of the United States Chess Federation v. Susan Polgar and Hoainhan Truong (a.k.a. Paul Truong) and the enclosed exhibits identified as:

   IL-A: New York Litigation

   IL-B: Fake Sam Sloan Postings

IL-C: XO Communications Response

IL-D: United Online Response

IL-E: Mottershead Report

IL-F: Jones Report

IL-G: Ulevitch Report

IL-H: USCF Demand Letter to Defendant Truong

IL-I: Defendant Truong Pay Stub and Southwest Airlines Receipt

IL-J: Defendant Truong Executive Board Campaign

IL-K: Defendant Truong New York Bankruptcy Petition

IL-L: California Litigation

IL-M: Texas Litigation

- **FSS-Posts**: A file named "PostsByFakeSamSloan.txt" provided to me on or about 2008-04-04 and asserted to be newsgroup postings associated with the matter at hand.

- **USCF-Logs:** A file named "USCF Posts by Time 3.10.06 - 9.20.07 (REC'D 10.24.07).TXT" identified in IL-E as "chesspromotion-uscf-posts.txt"

- **Polgar-Depo**: ORAL AND VIDEOTAPED DEPOSITION OF SUSAN POLGAR June 30 & July 1, 2009

- **Polgar-Tax**: A file named "Polgar Foundation Tax Return.pdf" containing the tax returns of the non-profit foundation run by Susan Polgar.

- **UOL-SEC**: A file called "United Online SEC Filing 10-Q.txt" represented to be an accurate depiction of an SEC filing by United Online.

- **Indictment**: CR-09 00719 for violations of 18 U.S.C. 1030(a)(2)(C) and (c)(2)(B)(ii) - intentionally accessing a computer without authorization, and 18 U.S.C. 1028(A)(a)(1) - Aggravated Identity Theft.

- **POPP**: Plaintiff's Opposition to Defendant Polgar's Motion to Compel Production of Documents withheld on an invalid assertion of the attorney-client privilege.

  ◦ **POPP-A**: Exhibit A to POPP - Google's response to subpoena.

  ◦ **POPP-B**: Exhibit B to POPP - Yahoo!'s response to subpoena.

  ◦ **POPP-C**: Exhibit C to POPP - Washington State's response to subpoena.

- **POAMD**: Plaintiff's opposition to Alexander's Motion to Dismiss for lack of personal jurisdiction. Which includes:

  ◦ **POAMD-A**: Yahoo! account records and affidavit showing IP addresses and date and times in which those addresses were used to login to the account randallhough@yahoo.com.

  ◦ **POAMD-B**: Images of IP address lookups to identify the operator providing these IP addresses to their clients.

  ◦ **POAMD-D**: Letter from Comcast to Alexander identifying that it has been subpoenaed to provide information that links Alexander to an IP address at issue in this case.

  ◦ **POAMD-E**: Yahoo! account records and affidavit showing IP addresses and date and times in which select IP addresses were used to login to the account randallhough@yahoo.com.

  ◦ **JMR-Dec:** "Declaration of Jeffrey M. Rosenfeld in support of Plaintiff's Opposition to Alexander's Motion to Dismiss for lack of personal jurisdiction".

  ◦ **POAMD-G**: "Account Screen from Anonymizer for Gregory Alexander, and Affidavit of Anonymizer, Inc.'s Custodian of Records".

  ◦ **MN-Dec**: "Declaration of Michael Nolan in support of Plaintiff's Opposition to Alexander's Motion to Dismiss for lack of personal jurisdiction".

  ◦ **HOUGH**: Declaration of Randall D. Hough in support of Plaintiff's opposition to Alexander's Motion to Dismiss for lack of personal jurisdiction.

- **Polgar-Dec**: Declaration of Susan Polgar in support of Defendant's Reply to Plaintiff's Opposition to Motion to Transfer".

- **Polgar-Request**: An email authenticated by Pulgar sent to Alexander with regard to Alexander's services to Pulgar.

- **PE1**: Polgar's email to Mr. Browne, dated 13 Jan 2008 at 16:51:53 EST from SusanPolgar@aol.com and included as a redacted reference document as part of this Report in "1.13.08.pdf".

- **PE2**: A non-privileged email from Bill Goichberg to Randy Hough and Jim Berry received by Randy Hough at his "randallhough@yahoo.com" email account on or about June 22, 2008 at or about 17:48:24 CDT, with the subject line, "Military liaison." ("Military liaison email 6.22.08.PDF").

- **PE3**: An email from Susan Polgar quoting the contents of PE2. ("Polgar Email 6.23.08 to JB.pdf")

- **NTT-Resp**: A file named "NTT America Response to USCF Federal Subpoena (DATED 3.4.09).PDF".

- **NTT-Resp2**: A file named "NTT America's Response to Subpoena (DATED 8.13.08).PDF".

- **Anon**: A file named "Response from Anonymizer - logs of gregory alexander.pdf" containing a listing of the uses of the Anonymizer service by the user identified as Gregory Alexander.

- **Joomla**: A file called "USCF Joomla Bridge Doc 10.24.07.txt" containing technical records of uses of the USCF chess forum by the user identified as "ChessPromotion" (a.k.a. Truong).

- J**oomla-Truong-String.out**: A file I generated by extracting relevant portions of Joomla indicative of the browser information associated with the "ChessPromotion" user of the USCF forums.

- **USCF-AccessIPs**: A file called "Plaintiffs' Production Docs, Bates No. USCF000601-USCF000652 (DATED 6.26.09).pdf" containing IP addresses, dates, and times of postings to USCF forums made by Truong, Polgar, and Alexander.

- **Affit**: A file named "Combined Affidavits re Stolen Emails.PDF".

- **NotDisclosed**: I am informed that PE2 was not disclosed by the parties to it within the relevant time frames for this case.

- **AOLTOS**: America OnLine Terms of Service for users who are registered with AOL ("AOL-TermsOfService.html")

Attribution of the source of the "Fake Sam Sloan" postings

According to IL-A, plaintiff Samuel H. Sloan indicated that he did not post a set of news postings to the Internet news groups named "rec.games.chess.politics" and "rec.games.chess.misc", including specific identified content of "Subject:" header fields. IL-A asserts that these and other postings were in fact made by Polgar and Truong, identified within IL-Exhibits.

Through whatever sequence of events that took place, these news postings came to be identified as the "Fake Sam Sloan Postings" by various parties.

I refer to these, yet to be fully or perfectly identified set of postings, collectively, as "FSS", and identify specific Items identified in the process of my report and elsewhere by others by their RGCP or RGCM names.

The color codes for this section of this report

The color coding in this section has been used to demonstrate how different elements are linked together. In particular:

The yellow coloring of letters is associated with the postings with the ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0 posting account. This posting account appears to have been used by many parties from many locations.

The green background and lettering is associated with posting accounts and postings that involve a small number or one apparent party and IP addresses and that are additionally linked to Truong through the previous attribution involving XO Communications.

The blue background and lettering is associated with posting accounts with postings from IP addresses among those used by to post information "From:" a user named in the headers as "Paultruong@aol.com".

The gray background and *gray italicized writing* is associated with IP addresses used by Truong to access the USCF systems under the "ChessPromotion" name Truong commonly uses on that site also used with the identified posting accounts used for FSS-Posts. This is only used if another color has not already been applied to it.

I retrieved and processed RGCP and RGCM

In order to perform analysis and examination of the evidence and issues in this matter, on or about April 13, 2008, I used a small Unix script that I created for the purpose to retrieve newsgroup postings that were available through my Internet Service Provider at that time, including, without limit, all of the postings that I found available to me at that time from the news groups rec.games.chess.misc and rec.games.chess.politics. The results of these retrievals are included herein by reference as part of this report, and are provided in digital form within the directory "Included" within directory names associated with these newsgroups.

The limits or reliability of newsgroup postings

Because of recent changes associated with the Internet, the service provider that I used at that time (Comcast) and most other service providers I have been able to identify, no longer provide the service of allowing such newsgroups to be downloaded in this manner, and increasingly, such archival information is difficult to obtain.

At the time I retrieved these records, they were records created and maintained by the providers I used to retrieve them, and were relied upon for the purpose of providing services to their customers in the day-to-day use of newsgroups.

The method used to retrieve these records has limited reliability in terms of retrieving complete records. In particular, and without limit:

- The protocols used were operated using the transmission control protocol (TCP) protocol [RFC793] within the Internet Protocol [RFC791], and TCP provides for reliable sequencing of information delivered.

- The protocols sometimes fail because of server, software, and/or infrastructure problems, and in the high bandwidth usage associated with my retrieval of information from these groups, such failures appear to have occurred when retrieving some of the bodies of some of the postings.

- As a result, the information retrieved may be incomplete, but what was retrieved can be reasonably relied upon to accurately reflect what was presented by the server in question (newsgroups.comcast.net).

- The records kept at newsgroups.comcast.net, as records of newsgroups kept throughout the Internet, were of only limited reliability. Many postings are missing for one reason or another, including, without limit, that they may have been deleted by newsgroup owners or operators (which still happens today) or lost in process or handling in their path from place to place. Indeed, this server no longer operates news services for Comcast and they indicate that, as a company, they no longer support the newsgroup service.

- The process I used to retrieve these newsgroup posting recorded the returned elements of the NNTP protocol along with the article numbers and the articles themselves. This can be seen in the files named by the posting identifier and ending in the ".out" extension as well as in the extracted headers from these files located in the "Headers" directory within each newsgroup directory provided with this report.

I summarize:

> **The records that I retrieved, while reasonably accurate as to what they contain, are likely to be incomplete in that they are missing traces of event sequences that may have happened over time.**

> **Similar records are available on a record by record basis from "Google" and at other archival sites, and any specific results I have given may be verified against the records at these various locations in order to confirm their accuracy.**

Processing of these records of newsgroup activities

I processed and examined the headers of the postings I retrieved using the tools identified above and the Unix "less", "wc", "ls", "diff", "grep", "sort", "awk", and

"sh" tools that are part of the standard Unix distribution, and the computer languages "perl" and lisp", all of which are and has long been widely used for this and related purposes, and that I have extensively tested and found reliable for the purposes they were used for in this case, and that are used as part of the processes described in peer reviewed articles.

Identifying FSS

While FSS has not been fully or perfectly identified to date, IL-A identifies "Subject:" headers associated with FSS, IL-B identifies postings associated with FSS, IL-Complaint identifies Internet Protocol (IP) addresses associated with FSS, FSSP includes what are asserted to be some posts that part of FSS, and FS-Posts contains what I understand to be asserted as newsgroup postings identified as "fake Sam Sloan" postings.

Attributes of identified elements of FSS

In order to understand more clearly the attribution of the identified elements of FSS to a source or sources, I analyzed the traces identified in IL-A, IL-B, IL-Complaint, FSS-Posts, and FSSP from RGCP and RGCM to identify what attributes they had in common and that were readily amenable to automated analysis and examination with existing tools that have been used reliably for similar purposes in other legal matters.

Other postings with attributes attributed to the identified FSS

Based on the attributes identified with FSS above, I examined RGCP and RGCM to identify other postings with attributes identified for FSS. These will be detailed below.

How the identified attributes link postings to Polgar and Truong

There are two independent paths by which the attributes associated with the identified FSS postings are linked with Polgar and Truong. As I will show below:

> **The Internet Protocol (IP) addresses recorded as the postings were made are consistent with addresses used by the user(s) of accounts paid for by Polgar and registered under Truong's name, address, and phone number.**

> **The Internet Protocol (IP) addresses recorded as the postings were made are consistent with the same such addresses used by Polgar and Truong to log into and post entries in the United States Chess Federation (USCF) online forum under their own identities and in the same time frames.**

IP addresses used at the USCF online forums

According to [USCF-AccessIPs], Polgar's user identity made posting to USCF forums using the IP addresses: 12.161.42.5 24.149.255.225 24.90.223.35 64.12.116.9 67.101.14.132 67.105.2.131 69.154.49.244 152.163.100.132 166.217.77.42 205.188.116.14 205.188.116.6 205.188.117.12 208.54.94.65 208.54.94.89 216.199.27.2

According to [USCF-AccessIPs], Alexander's user identity made posting to USCF forums using the IP addresses: 24.113.49.39 24.17.236.99 24.17.87.129 24.19.168.76 24.22.224.107 67.182.136.218 71.197.185.14 71.197.185.76 71.231.174.197 76.104.213.144 76.121.230.165 128.95.225.11 128.95.73.132 140.142.77.32 202.137.100.239 207.195.246.171 207.195.249.48

According to [USCF-AccessIPs], Truong's user identity made posting to USCF forums using the IP addresses: 12.162.143.67 12.181.201.130 12.182.238.2 12.33.93.210 24.193.133.108 24.90.222.139 24.90.223.35 63.145.202.34 64.12.116.12 64.12.116.141 64.12.116.200 64.12.116.77 64.12.116.9 64.12.117.17 64.12.117.5 64.122.192.10 65.74.197.98 66.90.26.164 67.135.101.10 67.88.206.99 68.15.241.155 69.154.49.244 69.88.112.106 70.18.61.151 70.19.108.87 72.255.6.142 75.111.194.9 75.111.199.177 82.69.14.94 129.118.87.222 139.133.7.37 139.133.7.38 141.155.155.176 141.155.158.69 152.163.100.13 152.163.100.132 152.163.100.14 152.163.100.145 152.163.100.207 152.163.100.67 152.163.100.70 152.163.101.11 152.163.101.14 162.83.134.76 162.83.163.124 166.217.112.32 166.217.125.255 166.217.189.34 166.217.235.185 172.163.82.246 195.93.60.138 198.211.223.116 205.188.116.136 205.188.116.14 205.188.116.198 205.188.116.199 205.188.116.203 205.188.116.66 205.188.116.9 205.188.117.12 205.188.117.14 207.200.116.14 208.54.14.17 208.54.94.17 208.54.94.25 208.54.94.81 216.226.194.194 216.89.5.128

The IP addresses of postings were traced to "chessspammer@netzero.net"

One of the attributes that some of the identified FSS postings have in common is the Internet Protocol (IP) addresses identified as the source of these postings within the headers of the postings themselves. In IL-B, the postings listed had "NNTP-Posting-Host:" fields. I found the following 47 postings associated with these IP addresses:

IP address	RGCM	RGCP
66.2.156.114	RGCM241561 RGCM241562 RGCM241563	RGCP280453 RGCP280454 RGCP280455 RGCP280456 RGCP280457

IP address	RGCM	RGCP
66.2.156.201	RGCM237022	RGCP273611 RGCP273612 RGCP273613 RGCP273615 RGCP273616 RGCP273617 RGCP273619
66.2.156.208		RGCP278953 RGCP278955 RGCP278956 RGCP278958 RGCP278960
66.2.156.214		RGCP273230 RGCP273231 RGCP273232 RGCP273233
66.2.157.248	RGCM237082 RGCM237083 RGCM237087	RGCP273724 RGCP273725 RGCP273726 RGCP273727 RGCP273739 RGCP273740 RGCP273742 RGCP273743 RGCP273744 RGCP273745 RGCP273746
201.134.236.150	RGCM283192 RGCM283193 RGCM283205 RGCM283216 RGCM283284	RGCP314435 RGCP314436 RGCP314456

Table 1 - Postings associated with identified IP addresses

Except for the 201.134.236.150 IP address, which will be addressed later in this report, all of the other addresses were identified as being associated with a source in IL-C. According to IL-C, the Internet Service Provider "XO Communications" that has the rights to control these IP addresses, indicates that their reseller, United Online, Inc., leased the use of these IP addresses, during the times of the FSS postings from those IP addresses, to an individual whose email address, which was used to authenticate the use at that time, was:

> chessspammer@netzero.net

This name is, apparently, consistent with the activities at issue. These records also show the dates and times of logins, and other related details.

Truong's information was associated with "chessspammer@netzero.net"

United Online, Inc. is, according to FCC filings, [UOL-SEC] the owner of the dial-up service provider "NetZero", the provider whose domain name (netzero.net) is associated with the user identity that used the IP addresses from which these postings were sent at the time they were sent.

In IL-D, United Online, Inc. indicates that, according to the records it keeps in the normal course of business, the account "chessspammer@netzero.net" was:

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

- Active at the times at issue and the time of their response,

- Paid for regularly and included Internet and email services,

- Had a member name of "Paul Truong"

- Was originally started on March 13, 2005

- Had an address of 67-15 102nd St. 7U, Forest Hills, NY, 11375, USA

  - According to Polgar-Tax and other related tax documents, copies of which are included herewith, this is one of the official addresses of Polgar and Truong.

- Had a home phone of 212-748-9587

  - I used the "google.com" Web site to search for this phone number and found it predominantly displayed in multiple Web pages identified with Polgar and Truong. Among these are:

    http://www.chesscafe.com/text/polgar31.pdf [polgar31.pdf]

      which identifies "FM Paul Truong c/o Polgar Chess Center 103-10 Queens Boulevard (Suite 1C) Forest Hills, NY 11375 – Tel: (212) 748- 9587 – E-mail: PaulTruong@aol.com "

    http://polgargirls.blogspot.com/2006_05_01_archive.html [ChessBlogForGirls05-01-2006.html]

      which identifies "FM Paul Truong c/o Polgar Chess Center 103-10 Queens Boulevard (Suite 1C) Forest Hills, NY 11375 - Tel: (212) 748-9587 - E-mail: PaulTruong@aol.com"

    http://www.susanpolgar.com/rulesinvitegirls2007.pdf [rulesinvitegirls2007.pdf]

      which identifies "FM Paul Truong c/o Polgar Chess Center 103-10 Queens Boulevard (Suite 1C) Forest Hills, NY 11375 - Tel: (212) 748-9587 - E-mail: PaulTruong@aol.com "

    http://main.uschess.org/content/view/7726/319/ [USCF-3rdSusanPolgar.html]

      which identifies "Please contact Mr. Paul Truong at (212) 748-9587 or e-mail PaulTruong@aol.com for this event."

- Paid for with an American Express Optima card of which Polgar is today, and was at the times in question, the account owner. (details withheld)

Polgar paid for the "chessspammer@netzero.net" account

The American Express Optima card used to pay for the NetZero account was held, and paid for over the entire period in question, by Polgar. [Polgar-Depo p542]:

```
13      Q.  (BY MR. HUTTENBACH) Do you have any
14   explanation one way or the other why your American
15   Express card number might have paid for some of the
16   internet services used to do these postings?
17      A.  Absolutely not.
```

and [Polgar-Depo p655-6]:

```
19          Do you have a record of the credit card
20   dispute with American Express regarding the NetZero
21   charges?
22      A.  I believe so.
23      Q.  Okay.  Would you give those documents to your
24   attorney and --
25      A.  Sure.
0656
 1      Q.  Okay.  Did American Express reverse all the
 2   charges?
 3      A.  No, they did not.  In fact, unfortunately, the
 4   only thing I believe I was able to do is cancel the
 5   charge for future months.  And they said it is basically
 6   my fault that I didn't notice it earlier.
 7      Q.  Do you review your credit card statements
 8   every month when they come in?
 9      A.  Unfortunately, I guess not diligently enough
10   because I have a good number of credit cards and little
11   charges, relatively little charges of 9, $10 don't stand
12   out and luckily I catch the bigger ones usually, but --
```

While Polgar denies attribution to this NetZero account, all of relevant digital forensic information identified so far is consistent with this account being used by Truong, and Polgar has not provided any documentation or information authenticating her assertion that she reported theses charges as fraudulent to American Express.

The NetZero Terms of Service indicate that Truong is responsible

According to "http://www.netzero.net/start/landing.do?page=www/legal/terms", provided in the file "NetZero-EULA.html" in the "References" directory included

with this Report, the terms of service agreement for NetZero, which I downloaded and reviewed as part of the writing of this report:

> "You must register for NetZero Services using your own name."...

> "You are responsible for all use of your NetZero Services and for the security of your login identification, your password and any security lock code that you use to protect access to your data, NetZero personal profile, your file name(s) and files, network and user access, and any information you disseminate through use of NetZero Services or through other Internet services."

These terms of service are, according to the NetZero Web site and Terms of Services, agreed to by NetZero customers as a condition of their purchase and use of NetZero accounts.

If the court should choose to accept the validity of and enforce this contract, which was apparently used and paid for by Truong and Polgar, then regardless of who may have been at the keyboard during the postings made with this account, the account holder identified in the account records as registered, Truong, is responsible for all of the activities identified with the user account with the email address "chessspammer@netzero.net" and for the use of the IP addresses associated with that account during their periods of use, including the use of these IP addresses for posting the identified FSS postings.

The same IP addresses were used by Polgar and Truong for other business

The table below shows information on the postings associated with some of Truong's known IP addresses and lists the number of posts and other common factors.

IP address	Posts	Other common factors
24.90.223.35 RGCP Used by Truong in the posting below	8	Identified as an IP address used by the user identity associated with Truong and Polgar for posting to the USCF online forums. [USCF-AccessIPs] RGCP309607 RGCP309467 RGCP309466 RGCP309465 RGCP309464 RGCP305316 RGCP296199 RGCP288144 Further details are provided under "An example tying an IP address to Truong" below.
24.90.223.35 RGCM	7	Identified as an IP address used by the user identity associated with Truong and Polgar for postings to the USCF online forums. [USCF-AccessIPs]

IP address	Posts	Other common factors
Used by Truong in the posting below		RGCM277509 RGCM277348 RGCM277347 RGCM277346 RGCM277345 RGCM271440 RGCM250317
		Further details are provided under "An example tying an IP address to Truong" below.
75.111.199.177 RGCM	3	Identified as an IP address used by the user identity associated with Truong for postings to the USCF online forums.[USCF-AccessIPs]
		RGCM282246 RGCM281824 RGCM281813
		These are listed below under "Other indicators" as part of the group having "X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2),gzip(gfe),gzip(gfe)"
75.111.199.177 RGCP	3	Identified as an IP address used by the user identity associated with Truong for postings to the USCF online forums.[USCF-AccessIPs]
		RGCP313598 RGCP313289 RGCP313285
		These are listed below under "Other indicators" as part of the group having "X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2),gzip(gfe),gzip(gfe)"
75.111.194.9 RGCM	11	Identified as an IP address used by the user identity associated with Truong for postings to the USCF online forums.[USCF-AccessIPs]
		RGCM282845 RGCM282838 RGCM282827 RGCM282826 RGCM282696 RGCM282695 RGCM282694 RGCM282644 RGCM282499 RGCM282449 RGCM282448
		These are listed below under "Other indicators" as part of the group having "X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727;

IP address	Posts	Other common factors
		Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2),gzip(gfe),gzip(gfe)"
75.111.194.9 RGCP	19	Identified as an IP address used by the user identity associated with Truong for postings to the USCF online forums.[USCF-AccessIPs] RGCP314115 RGCP314111 RGCP314110 RGCP314109 RGCP314101 RGCP314100 RGCP314098 RGCP314027 RGCP314026 RGCP314025 RGCP314022 RGCP314011 RGCP313992 RGCP313913 RGCP313846 RGCP313781 RGCP313780 RGCP313779 RGCP313778 These are listed below under "Other indicators" as part of the group having "X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2),gzip(gfe),gzip(gfe)"

Table 2 - Postings related to identified IP addresses

An example tying an IP address to Truong

Article RGCP309607, listed above under 24.90.223.35, includes in pertinent parts:

> From: Paultruong@aol.com
> Newsgroups: rec.games.chess.politics,rec.games.chess.misc
> Subject: Re: Hoainhan "Paul" Truong and the Last Helicopter out of Vietnam
> Date: 18 Apr 2007 16:54:07 -0700
> Organization: http://groups.google.com
>
> ...
> NNTP-Posting-Host: 24.90.223.35
> Mime-Version: 1.0
> Content-Type: text/plain; charset="iso-8859-1"
> X-Trace: posting.google.com 1176940448 22833 127.0.0.1 (18 Apr 2007 23:54:08 GMT)
> X-Complaints-To: groups-abuse@google.com
> NNTP-Posting-Date: Wed, 18 Apr 2007 23:54:08 +0000 (UTC)
> In-Reply-To: <lg7d23t1156dimkloqk02qtla42mchbq2v@4ax.com>
> User-Agent: G2/1.0
> X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0; .NET CLR 2.0.50727),gzip(gfe),gzip(gfe)
> Complaints-To: groups-abuse@google.com
> Injection-Info: o5g2000hsb.googlegroups.com; posting-host=24.90.223.35;

    posting-account=ByDVMwwAAAAeH-8sKmCspe9QMcbXs1Uf
Xref: number1.nntp.dca.giganews.com rec.games.chess.politics:309607
rec.games.chess.misc:277509
...
Mr. Murray,

Please do not give much credence to what SS has posted. My resume was
basically fabricated by someone for political reasons. Yes, I worked
for 4 multibillion dollar corporations. On some projects, I was their
employee. On others, I was a consultant. In either case, I was
involved with various independent projects for these companies and it
had nothing to do with running any of these companies. I have never
made this claim. This is just another lie by SS.

I have been in chess for 37 years and I have been in the US for 27
years. I doubt that even one person can claim I said that I have a
PhD. I have never made this claim to anyone. It is typical of SS
fabricate things to mislead the readers. He recently fabricated an
email from the USCF by changing the email address. I do not read this
forum nor do I care to follow the garbage by SS in any forum. I was
just alerted by this latest BS by SS.

I have no idea who made that website. I certainly did not. I would not
doubt that it came from the same person who fabricated my resume. SS
is the biggest serial liar and he has no ability to be honest. I
suggested to the USCF a number of times to require a verified resume
to run for the board. I would have been more than happy to provide
mine for verification. However, they declined.

I hope I have made this matter clear. It was a complete fabrication by
SS because he knows he has no chance to win the election. This is his
way of giving himself a chance.

Best regards,
PT

This posting is duplicated, in pertinent parts, as described in the "Xref:" headers identified above, as article RGCM277345 in rec.games.chess.misc. This again ties Truong to this IP address and the other postings related to it. The related postings identified above for this IP address all have in common, the following sequence of other header fields.

Header	RGCP	RGCM
Path:	entry 1	entry 1
From:	entry 2	entry 2
Newsgroups:	entry 3	entry 3
A "Subject:"	entry 4	entry 4

Header	RGCP	RGCM
Date:	entry 5	entry 5
Organization:	entry 6	entry 6
Lines:	entry 7	entry 7
Message-ID:	entry 8	entry 8
References:	entry 9	entry 9
NNTP-Posting-Host:	24.90.223.35	24.90.223.35
Organization:	http://groups.google.com	http://groups.google.com
Mime-Version:	1.0	1.0
Complaints-To:	groups-abuse@google.com	groups-abuse@google.com
X-Complaints-To:	groups-abuse@google.com	groups-abuse@google.com

Table 3 - Common properties of postings from this Truong's IP Address

As described earlier, postings made to news groups combine information placed in headers from different automated processes performed by different computers. As a result of variations in the different computers, processes, configurations, hardware, software, and event sequences that cause these postings to come to be, these header fields appear in particular orderings with particular values. Commonalities in these header fields indicate mechanisms that produce those common sequences. While such sequences are not necessarily unique or uniquely identifying because many different mechanisms may produce the same sequence, the same mechanism applied in the same manner, normally produces the same sorts of sequences.

The IP address in this posting has also been used to post to USCF online forums by Polgar's and Truong's user identities. [USCF-AccessIPs]

Other IP addresses associated with Paul Truong

I found other IP addresses associated with the Paultruong@aol.com "From:" header in postings [PaultruongAOL]. Starting with the user identity, I listed the postings with this in their "From:" header.

```
RGCP197361 RGCP197515 RGCP200021 RGCP200091 RGCP200191
RGCP200354 RGCP200897 RGCP200981 RGCP201082 RGCP201254
RGCP201699 RGCP201719 RGCP201789 RGCP201924 RGCP202053
RGCP202079 RGCP203451 RGCP204021 RGCP204031 RGCP204036
RGCP204099 RGCP204100 RGCP204102 RGCP204145 RGCP204149
RGCP204239 RGCP204246 RGCP204341 RGCP204347 RGCP204362
RGCP204410 RGCP204411 RGCP204418 RGCP204560 RGCP204561
```

RGCP204682 RGCP204703 RGCP204819 RGCP205621 RGCP205671
RGCP205674 RGCP205676 RGCP205712 RGCP205794 RGCP205816
RGCP205843 RGCP205902 RGCP206027 RGCP206064 RGCP208661
RGCP208773 RGCP209096 RGCP209901 RGCP212128 RGCP212174
RGCP212850 RGCP215857 RGCP309607

which all come from IP addresses:

152.163.252.163   198.81.26.103   205.188.208.170   24.90.223.35
64.12.96.106 68.237.103.74

These IP addresses are also contained in the "NNTP-Posting-Host:" headers of postings by "SusanPolgar@aol.com (GM Susan Polgar)", including:

RGCP207203 RGCP212044 RGCP212651 RGCP214552 RGCP214923
RGCP214973 RGCP216393 RGCP206661 RGCP206668 RGCP207334
RGCP212531 RGCP214127

RGCM postings with Paultruong@aol.com in their "From:" header include:

RGCM194187   RGCM194301   RGCM194491   RGCM194673
RGCM195127   RGCM195657   RGCM195692   RGCM196025
RGCM196137   RGCM196150   RGCM196849   RGCM196914
RGCM197016   RGCM197104   RGCM197327   RGCM198071
RGCM198090 RGCM198901 RGCM277509

which all come from IP addresses:

152.163.252.163   198.81.26.103   205.188.208.170   205.188.209.112
24.90.223.35 64.12.96.106

These IP addresses are also contained in the "NNTP-Posting-Host:" headers of postings by "SusanPolgar@aol.com (GM Susan Polgar)", including:

RGCM198053   RGCM198971   RGCM199094   RGCM198904
RGCM198916   RGCM198939   RGCM199199   RGCM199214
RGCM199215 RGCM199216 RGCM198795

In pertinent time frames, other postings from these IP addresses may therefore also be attributable to Truong and Polgar as well, to the extent that common IP addresses and other factors support a reasonable cause for such an attribution.

Of the IP addresses identified here, only 24.90.223.35 was used to post to the USCF online forums, and this was used, at various times, by each of the user identities associated with Truong and Polgar. [USCF-AccessIPs]

Other indicators

In examining some of the postings identified above, I noticed that quite a few had some common strings in their headers. In particular, 25 RGCM postings included the seemingly unusual "X-HTTP-UserAgent:" header:

> "X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2),gzip(gfe),gzip(gfe)"

As discussed above, this heading is consistent with a computer operating with specific software components, versions, libraries, and capabilities, and the ordering of headers is consistent with the mechanisms by which these postings were sent to the newsgroups and processed within those newsgroups.

This header is consistent with a computer using a Mozilla version 4.0 Web browser on a computer with a Windows NT 6.0 operating system, using AOL 9.0, Microsoft Internet Explorer version 7.0, and with several other specific versions of specific software packages present.

These were posts RGCM282845 RGCM282838 RGCM282827 RGCM282826 RGCM282696 RGCM282695 RGCM282694 RGCM282644 RGCM282535 RGCM282532 RGCM282531 RGCM282529 RGCM282499 RGCM282449 RGCM282448 RGCM282382 RGCM282381 RGCM282355 RGCM282354 RGCM282325 RGCM282289 RGCM282246 RGCM281824 RGCM281813 and RGCM281632.

The same header string appeared in 39 RGCP posts. These were posts RGCP314115 RGCP314111 RGCP314110 RGCP314109 RGCP314101 RGCP314100 RGCP314098 RGCP314027 RGCP314026 RGCP314025 RGCP314022 RGCP314011 RGCP313992 RGCP313913 RGCP313888 RGCP313885 RGCP313884 RGCP313882 RGCP313846 RGCP313781 RGCP313780 RGCP313779 RGCP313778 RGCP313718 RGCP313717 RGCP313698 RGCP313697 RGCP313670 RGCP313668 RGCP313657 RGCP313656 RGCP313655 RGCP313654 RGCP313621 RGCP313619 RGCP313598 RGCP313289 RGCP313285 RGCP313152.

While these individual sequences associated with specific software components, versions, libraries, and capabilities are not rare, the combination of them in sequence, and its presentation in the same news posting header, is certainly less common, being present in only 64 of more than 200,000 such postings I examined in this case. These postings also had the following commonalities:

Header	RGCM	RGCP
Path:	at entry 1	at entry 1
From:	at entry 2	at entry 2

Header	RGCM	RGCP
Newsgroups:	at entry 3	at entry 3
Subject:	at entry 4	at entry 4
Date:	at entry 5	at entry 5
Organization:	at entry 6	at entry 6
Lines:	at entry 7	at entry 7
Message-ID:	at entry 8	at entry 8
Mime-Version:	1.0	1.0
Organization:	http://groups.google.com	http://groups.google.com
User-Agent:	G2/1.0	G2/1.0
X-Complaints-To:	groups-abuse@google.com	groups-abuse@google.com

Table 4 - Commonalities of postings with identical configuration indicators

As discussed earlier, these headings provide IP addresses associated with the injection of the newsgroup posting into the newsgroup and similarity of the mechanisms used to post these messages. In particular, these are consistent with the use of the newsgroup functions of groups.google.com.

These postings all have "Injection-info:" headers indicating "posting-host=" fields, which provide the source IP addresses as identified by the systems receiving the original postings. They indicate IP addresses of [UserAgent.matches]:

IP address	RGCM	RGCP	Notes
75.111.194.9	11	19	Used in Truong USCF postings. [USCF-AccessIPs]
75.111.199.177	3	3	Used in Truong USCF postings [USCF-AccessIPs]
75.110.200.21	5	10	
64.12.116.7	2	2	
205.188.116.7	2	3	
64.12.117.133	1	1	
75.110.206.205	1	1	

Table 5 - IP addresses used for postings with this computer configuration

The IP addresses of 36 of these postings have been associated with Truong through other means, as can be seen from the IP address table above. This also

shows that this same configuration of a computer and service was used for postings across the different newsgroups.

I also found the string "Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506" in the records provided by the USCF of accesses apparently by Truong for postings made with the user identity "ChessPromotion" in 80 cases. [Joomla-Truong-String.out] included with this report.

The IP addresses and "From:" names used for posting these messages included here [Poster.matches] are from this same set of postings (**emphasis added** for items from IP address table above):

RGCM (#)	RGCP (#)	"From:" name used in postings (notes)
(11) **75.111.194.9** 75.110.200.21	(21) **75.111.194.9** 75.110.200.21	"Ray Gordon, creator of the pivot" <raygordon@seductive.com>
(7) 75.110.200.21 205.188.116.7 **75.111.199.177** 75.110.206.205	(8) 75.110.200.21 205.188.116.7 **75.111.199.177** 75.110.206.205	Jackass Lafferty <bplafferty@lawyer.com>
(5) 64.12.116.7 205.188.116.7 64.12.117.133 **75.111.194.9**	(6) **75.111.194.9** 64.12.116.7 205.188.116.7 64.12.117.133	samsloan <samsloan@usa.com> (64.12.116.7 was used for USCF postings by the user identity associated with Truong.) [USCF-AccessIPs]
(2) *75.111.194.9*	(4) **75.111.194.9**	samsloan <ismailsloan@gmail.com>

Table 6 - IP addresses and From names used in these computer configuration posts

It appears that there is a linkage between all of these postings, individuals responsible for them, and the machines and processes used to make these postings. For example, and without limit:

- At least one posting to each of RGCP and RGCM from each of the identities associated with this same complex system-specific header came from IP addresses used by Truong for other purposes.

- At least 12 features of these 64 postings were identical in terms of placement of headers within the posting, and this differs from the more than 200,000 other postings made with other configurations.

Attributes of FSS-Posts postings

I examined FSS-Posts and identified that it contains 2463 instances of what appear to be postings to newsgroup forums, identified as "Article: " followed by

the article number, in a syntax similar to that I found when I extracted articles from newsgroups using the methods described above.

Using tools and methods that are widely used on a daily basis, relied upon in the normal course of business around the world, and that have proven reliable in the past for similar purposes, I extracted and examined select data from FSS-Posts and correlated information contained therein with information I retrieved in RGCP and RGCM. I found that all of the postings appear to be postings to RGCP. Using the article numbers confirmed in this manner, I examined the headers of the postings that I downloaded for the purposes of this analysis. I have listed the identified postings in the file "FSS-Posts" in the material included ad part of this report.

I identified a set of header fields with information indicating "posting-account=" that appear to provide identifying information associated with the accounts used to post information to these groups. Of the 2463 instances of this field, I found the following number of instances of each of the 9 different posting accounts associated with these instances. In this portion of this report.

```
>grep posting-account= PostsByFakeSamSloan.txt | sed 's: ::g' |  sort | numreps
263 posting-account=-olljA0AAADP_dAsjvgsS6CBWRXesmY5
243 posting-account=18CDig0AAAAQp9KtBpimOhlDAvHePsUd
229 posting-account=PJnN4g0AAACIDMDStNEqBAzSP-8kyXrH
462 posting-account=Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F
397 posting-account=Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm
311 posting-account=orzwdQ0AAAAmuVXufoENJWdCHVkVdmrm
141 posting-account=ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0
282 posting-account=pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4
135 posting-account=rAlDGA0AAABcQDPBXQBCjuONumvMJieL
```

I then sought to identify all postings associated with each of these posting accounts in order to identify related properties and postings. there are a total of 6505 postings associated with these 9 posting-account values [FSS-Posts-Accounts-Messages] resulting in message lists containing in files identified here along with the number of postings each (emphasis added):

```
263 FSS-Posts-Accounts-Messages.posting-account=-olljA0AAADP_dAsjvgsS6CBWRXesmY5
243 FSS-Posts-Accounts-Messages.posting-account=18CDig0AAAAQp9KtBpimOhlDAvHePsUd
229 FSS-Posts-Accounts-Messages.posting-account=PJnN4g0AAACIDMDStNEqBAzSP-8kyXrH
462 FSS-Posts-Accounts-Messages.posting-account=Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F
397 FSS-Posts-Accounts-Messages.posting-account=Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm
311 FSS-Posts-Accounts-Messages.posting-account=orzwdQ0AAAAmuVXufoENJWdCHVkVdmrm
4183 FSS-Posts-Accounts-Messages.posting-account=ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0
282 FSS-Posts-Accounts-Messages.posting-account=pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4
135 FSS-Posts-Accounts-Messages.posting-account=rAlDGA0AAABcQDPBXQBCjuONumvMJieL
```

It appears that the posting-account ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0 was associated with many other messages and users. This particular posting-account

appears to have been used as a group account of some sort, involving some 170 different user names from 704 IP addresses over the period from Thu, 12 Jul 2007 14:55:36 -0700 to Thu, 15 Nov 2007 00:25:16 -0000. I have included a summary of the relevant data for this posting-account in the file [FSS-Posts-Various-Info] and colored related material yellow throughout the remainder of this portion of this report.

I identified the user names associated with the "From:" headers in these postings, saving counts of each in file named as "FSS-Posts-Usernames-$x" where $x is replaced by the posting-account identifier. The number of different identifies I found for each is listed here:

```
9 FSS-Posts-Usernames--olljA0AAADP_dAsjvgsS6CBWRXesmY5
2 FSS-Posts-Usernames-18CDig0AAAAQp9KtBpimOhlDAvHePsUd
11 FSS-Posts-Usernames-PJnN4g0AAAClDMDStNEqBAzSP-8kyXrH
4 FSS-Posts-Usernames-Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F
3 FSS-Posts-Usernames-Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm
6 FSS-Posts-Usernames-orzwdQ0AAAAmuVXufoENJWdCHVkVdmrm
170 FSS-Posts-Usernames-ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0
3 FSS-Posts-Usernames-pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4
1 FSS-Posts-Usernames-rAlDGA0AAABcQDPBXQBCjuONumvMJieL
```

With the exception of the ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0 account, the following summarizes the user names applied, all of which are from FSS-Posts.

Posting account value	Counts of user names used
-olljA0AAADP_dAsjvgsS6CBWRXesmY5	3 "ChessDaddy" <sloan@journalist.com> 3 "Dickbrain Brennan" <sloan@journalist.com> 182 "Sam Sloan" <sloan@journalist.com> 24 "SamSloan" <sloan@journalist.com> 9 "SamSloanIII" <sloan@journalist.com> 8 "SloanSam" <sloan@journalist.com> 20 "StanB" <sloan@journalist.com> 8 "The Historian" <sloan@journalist.com> 6 sloan@journalist.com
18CDig0AAAAQp9KtBpimOhlDAvHePsUd	41 "Sam Sloan" <sloan@whoever.com> 2 sloan@whoever.com

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

Posting account value	Counts of user names used
PJnN4g0AAAClDMDStNEqBAzSP-8kyXrH	143 "Andrew Zito" <andrewzito@mail.com> 24 "AndrewZito" <andrewzito@mail.com> 2 "Bill Brock" <andrewzito@mail.com> 2 "Chess One" <andrewzito@mail.com> 2 "Joel Channing" <andrewzito@mail.com> 4 "Mike Murray" <andrewzito@mail.com> 4 "Phil Innes" <andrewzito@mail.com> 2 "Ray Gordon" <andrewzito@mail.com> 42 "Sam Sloan" <andrewzito@mail.com> 2 "The Historian" <andrewzito@mail.com> 2 andrewzito@mail.com
Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F	131 "Sam Sloan" <ismailsloan@gmail.com> 313 "samsloan" <ismailsloan@gmail.com> 1 ismailsloan@gmail.com 17 samsloan <ismailsloan@gmail.com>
Y_DiAA0AAACY1rJ0q8HGgFyJlqXTrnFm	255 "Sam Sloan" <samsloan@usa.com> 103 "samsloan" <samsloan@usa.com> 39 samsloan <samsloan@usa.com>
orzwdQ0AAAAmuVXufoENJWdCHVkVdmrm	4 "Bill Brock" <raygordon@writeme.com> 4 "Mike Nolan" <raygordon@writeme.com> 257 "Ray Gordon" <raygordon@writeme.com> 12 "Sam Sloan" <raygordon@writeme.com> 29 "samsloan" <raygordon@writeme.com> 5 raygordon@writeme.com
pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4	113 "Ray Gordon" <raygordon@seductive.com> 168 "Ray Gordon, creator of the pivot" <raygordon@seductive.com> 1 raygordon@seductive.com
rAlDGA0AAABcQDPBXQBCjuONumvMJieL	135 judgementday@clerk.com

Table 7 - User names with posting-accounts identified in FSS-Posts

I identified the IP addresses associated with these postings as well:

Posting account	IP addresses using this posting account
-olljA0AAADP_dAsjvgs	152.163.100.69 205.188.116.71 207.200.116.66 208.54.94.89 216.161.190.222 216.99.245.171

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

Posting account	IP addresses using this posting account
S6CBWRXesmY5	4.236.195.139 4.237.38.100 4.237.38.115 4.237.38.188 4.237.38.234 4.237.38.250 4.237.38.59 4.237.41.112 4.237.41.136 4.237.41.219 4.237.41.41 4.237.41.81 4.237.41.82 64.12.116.5 64.12.116.69 64.12.116.6 **66.2.156.201 66.2.156.208 66.2.156.214 66.2.157.248**
18CDig0AAAAQp9Kt BpimOhlDAvHePsUd	152.163.100.5 152.163.100.69 205.188.116.71 205.188.116.71 64.12.116.69 64.12.116.6
PJnN4g0AAACIDMDS tNEqBAzSP-8kyXrH	*152.163.100.67** 152.163.100.6 205.188.116.67 205.188.117.73 207.200.116.67 207.200.116.67 64.12.116.67 64.12.116.6
Ua1dlw0AAAA1_dVRi SGiD5ejBHhRdV9F	152.163.100.65 *152.163.100.67** 152.163.100.7 152.163.101.10 *152.163.101.14** 152.163.101.6 205.188.116.132 205.188.116.144 *205.188.116.199** 205.188.116.67 205.188.117.73 24.90.223.35* 64.12.116.199 64.12.116.205 64.12.116.66 64.12.116.67 64.12.116.67 64.12.116.73 64.12.116.7
Y_DiAA0AAACY1rJ0q 8HGgFyJIqXTrnFm	152.163.100.197 152.163.100.65 *152.163.100.67** 152.163.100.6 152.163.100.7 152.163.101.10 *152.163.101.14** 152.163.101.6 205.188.116.132 205.188.116.144 *205.188.116.199** 205.188.116.205 205.188.116.67 205.188.117.73 207.200.116.66 207.200.116.67 24.90.223.35* 64.12.113.184 64.12.116.199 64.12.116.205 64.12.116.66 64.12.116.67 64.12.116.6 64.12.116.73 64.12.116.7
orzwdQ0AAAAmuVXu foENJWdCHVkVdmr m	*152.163.100.67** 152.163.100.69 152.163.100.6 205.188.116.67 205.188.116.71 205.188.117.73 64.12.116.67 64.12.116.6 **66.2.156.114**
pzt0Dg0AAABJOWkhI GYqJEkINXRErvy4	152.163.100.197 152.163.100.65 *152.163.100.67** 152.163.100.6 152.163.100.7 152.163.101.10 *152.163.101.14** 205.188.116.132 205.188.116.144 *205.188.116.199** 205.188.116.67 205.188.117.73 207.200.116.67 24.90.223.35* 64.12.116.199 64.12.116.205 64.12.116.67 64.12.116.6 64.12.116.73 64.12.116.7
rAlDGA0AAABcQDPB XQBCjuONumvMJieL	152.163.100.11 152.163.100.11 152.163.100.65 152.163.100.7 152.163.101.10 *152.163.101.14** 205.188.113.64 205.188.116.132 205.188.116.144 *205.188.116.199** 205.188.116.205 205.188.116.67

Posting account	*IP addresses using this posting account*
	205.188.116.7 64.12.116.199 64.12.116.205 64.12.116.73 64.12.116.7

Table 8 - IP addresses associated with posting-accounts

The IP addresses marked with a trailing "*" are IP addresses also used by the user identity associated with Truong to make postings at USCF online forums.

I checked the IP addresses associated with the posting-accounts identified above and found that the following posting accounts were used from IP addresses authenticated as associated with Truong through XO Communications. These are also highlighted in the IP address table above.

Posting account	Number	IP address
orzwdQ0AAAAmuVXufoENJWdCHVkVdmrm	5	66.2.156.114
-olljA0AAADP_dAsjvgsS6CBWRXesmY5	7	66.2.156.201
-olljA0AAADP_dAsjvgsS6CBWRXesmY5	5	66.2.156.208
-olljA0AAADP_dAsjvgsS6CBWRXesmY5	4	66.2.156.214
-olljA0AAADP_dAsjvgsS6CBWRXesmY5	11	66.2.157.248
ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0	3	201.134.236.150

Table 9 - FSS-Posts posting-accounts with Truong XO Communications IPs

Note that the last account listed is associated with the "group account" identified earlier, and is therefore less reliable as an indicator without the additional information of the IP address.

The following table lists the specific postings associated with these IP addresses, and they cover all of the postings authenticated as associate with Truong through the use of XO Communications as discussed above.

IP address	Matching posts with Truong XO Communications IPs
66.2.156.114	RGCP280453 RGCP280454 RGCP280455 RGCP280456 RGCP280457
66.2.156.201	RGCP273611 RGCP273612 RGCP273613 RGCP273615 RGCP273616 RGCP273617 RGCP273619
66.2.156.208	RGCP278953 RGCP278955 RGCP278956 RGCP278958 RGCP278960
66.2.156.214	RGCP273230 RGCP273231 RGCP273232 RGCP273233

IP address	Matching posts with Truong XO Communications IPs
66.2.157.248	RGCP273724 RGCP273725 RGCP273726 RGCP273727 RGCP273739 RGCP273740 RGCP273742 RGCP273743 RGCP273744 RGCP273745 RGCP273746
201.134.236.150	RGCP314435 RGCP314436 RGCP314456

Table 10 - FSS-Posts postings with Truong XO Communications IPs

As indicated earlier, the last entry indicates that this is the case where the IP addresses and postings were linked to Truong earlier, but in which the posting-account appears to have been used by many other identities and from many other IP addresses.

I also examined the FSS-Posts for the presence of the IP addresses associated with the AOL account Paultruong@aol.com [PaultruongAOL] identified above (152.163.252.163 198.81.26.103 205.188.208.170 24.90.223.35 64.12.96.106 68.237.103.74) and found that these addresses are also used in postings identified in FSS-Posts. In particular, I found:

posting account	#	posting host
Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F	1	24.90.223.35
Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm	1	24.90.223.35
pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4	5	24.90.223.35

Table 11 - FSS-Posts with an IP address used by Paultruong@aol.com

The IP address 24.90.223.35 is also an IP address used by the user identities used by Truong and Polgar to make postings to the USCF online forum.

Attribution by way of USCF usage patterns

Polgar and Truong are and have long been members of the United States Chess Federation (USCF). As such, they are active members of the chess community and often use the online facilities of the USCF for various chess-related purposes. Their usage of these online facilities and the related business records, asserted by USCF to be kept and relied upon by the Federation in the normal course of business to support its day-to-day operations, also provide traces of what took place over time.

I extracted the IP addresses from USCF-Logs identified as "IP addresses of the 668 ChessPromotion posts in the USCF Forums", with ChessPromotion identified in IL-C as the identifying name used by Truong in his use of that forum over a substantial period of time. Using those IP addresses, I searched for posting with the FSS-Posts posting-name fields and found the following results:

Posting-account	Count	IP Address
PJnN4g0AAAClDMDStNEqBAzSP-8kyXrH	20	152.163.100.67
Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F	1	205.188.116.199
Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F	1	**24.90.223.35**
Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F	159	152.163.100.67
Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F	6	152.163.101.14
Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm	1	**24.90.223.35**
Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm	5	152.163.101.14
Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm	6	205.188.116.199
Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm	78	152.163.100.67
orzwdQ0AAAAmuVXufoENJWdCHVkVdmrm	1	152.163.100.67
ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0	12	205.188.116.199
ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0	19	**75.111.194.9**
ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0	2	205.188.116.136
ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0	3	152.163.100.132
ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0	3	**75.111.199.177**
pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4	1	152.163.101.14
pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4	10	205.188.116.199
pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4	37	152.163.100.67
pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4	5	**24.90.223.35**
rAlDGA0AAABcQDPBXQBCjuONumvMJieL	6	152.163.101.14
rAlDGA0AAABcQDPBXQBCjuONumvMJieL	6	205.188.116.199

Table 12 Posting accounts linked to IP addresses through the USCF logs

The boldface underlined IP addresses are also identified earlier in this report as associated with the posts at issue in IL-B and/or IP addresses used by Truong to make postings under the "Paultruong@aol.com" account.

Summary of FSS attribution factors

There are several different ways in which attributions of different factors have been made between FSS postings and Truong. I have summarized these results in the following table. The counts identified are conservative in that the total number of instances of each in the FSS postings may exceed the identified counts in this table.

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

Factor	*Basis*
IP address traced to Truong Netzero account: 66.2.156.114 66.2.156.201 66.2.156.208 66.2.156.214 66.2.157.248	This was identified in 36 FSS instances - Posting was made from an IP address logged in as "chessspammer@netzero.net". - Login account active at the times at issue. - Paid for regularly and included Internet and email services. - Had a member name of "Paul Truong" - Was originally started on March 13, 2005 - Had an address of 67-15 102nd St. 7U, Forest Hills, NY, 11375, USA that Tax records show as an address of Truong and Polgar. - Had a home phone of 212-748-9587 linked to Truong by advertising and promotions for Polgar's Chess Center and E-mail address "PaulTruong@aol.com" - Paid for monthly for more than 3 years by Polgar / Truong's American Express Optima card. - NetZero terms of service state registered user is "responsible" for use and protection of user ID, password, and security codes.
IP address used by Truong for other posting: 24.90.223.35	This was identified in at least 15 FSS instances. - RGCP309607 was posted from AOL account "Paultruong@aol.com" and used this same IP address. - Truong does not deny having posted RGCP309607. - Truong also posted to the USCF database using the same IP address under the identity "ChessPromotion" - Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm posting account used this IP address. (1) - Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F posting account used this IP address. (1) - pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4 posting account used this iP address. (5)

Factor	*Basis*
	- All FSS postings containing this IP address also share 13 other header characteristics .
From: Paultruong@aol.com postings indicated IP addresses: 152.163.252.163 198.81.26.103 205.188.208.170 205.188.209.112 24.90.223.35 64.12.96.106 68.237.103.74	- These same IP addresses also had postings "From: SusanPolgar@aol.com (GM Susan Polgar)" (23) [152.163.252.163, 205.188.208.170, 205.188.209.112, and 64.12.96.106] - IP addresses 24.90.223.35 was also used to post to the USCF database and FSS postings as shown above.
IP addresses Truong used for postings to the USCF database. 152.163.100.67 205.188.116.199 24.90.223.35 152.163.101.14 75.111.194.9 205.188.116.136 152.163.100.132 75.111.199.177 152.163.101.14	This was identified in at least 37 instances. - IP address 24.90.223.35 was also used in postings "From: Paultruong@aol.com". - IP address 24.90.223.35 was also used for postings with 3 different FSS posting accounts. - IP addresses 75.111.199.177 and 75.111.194.9 are also linked to the "X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2),gzip(gfe),gzip(gfe)" entry below. - IP address 205.188.116.199 was used for 4 (samsloan <samsloan@usa.com>) and 7 (Jackass Lafferty <bplafferty@lawyer.com>) posts. - IP address 205.188.116.199 was used for posting with 5 FSS posting accounts. - IP address 152.163.100.132 was used for 1 (Jackass Lafferty <bplafferty@lawyer.com>) and 2 (blafferty@lawyer.com) posts. - IP address 152.163.100.132 was also used for postings with one FSS posting account.

Factor	Basis
	- IP address 152.163.100.67 was also used for postings used 5 FSS posting accounts.
	- IP address 152.163.101.14 was used for posting with 4 FSS posting accounts.
	- IP address 205.188.116.136 was used for posting with one FSS posting accounts.
Postings containing the "X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2),gzip(gfe),gzip(gfe)" header entry	- This header is found 64 times in FSS
	- This header is consistent with a computer using a Mozilla version 4.0 Web browser on a computer with a Windows NT 6.0 operating system, using AOL 9.0, Microsoft Internet Explorer version 7.0, and with a variety of other quite specific versions of different related software packages present.
	- Present in only 64 of more than 200,000 such postings I examined in this case.
	- All also have 12 other commonalities in headers.
	- 36 have IP addresses used in Truong's USCF postings.
	- All 64 postings are identified as part of FSS.
	These are divided into:
	- 33 have "From: Ray Gordon, creator of the pivot" <raygordon@seductive.com>"
	- 15 have "From: Jackass Lafferty <bplafferty@lawyer.com>"
	- 11 have "From: samsloan <samsloan@usa.com>"
	- 6 have "From: samsloan <ismailsloan@gmail.com>"
	- Each of these 4 "From:" addresses includes postings with this header that have IP addresses 75.111.194.9 or 75.111.199.77
	- 75.111.194.9 was used in 19 Truong USCF postings.
	- 75.111.199.77 was used in 3 Truong USCF

Factor	*Basis*
	postings.
	- The substring "Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506" was also present in the records of USCF forum postings by Truong [Joomla]
Posting account -olljA0AAADP_dAsjvgsS6CBWRXesmY5	- Only used in FSS postings. - 7 from IP address 66.2.156.201 (Truong's NetZero account). - 5 from IP address 66.2.156.208 (Truong's NetZero account). - 4 from IP address 66.2.156.214 (Truong's NetZero account). - 11 from IP address 66.2.157.248 (Truong's NetZero account).
Posting account orzwdQ0AAAAmuVXufoENJWdCHVkVdmrm	- Only used in FSS postings. - Used from 66.2.156.114 (Truong's NetZero account). - Also used from 152.163.100.67 (a USCF posting IP address used by Truong)
Posting account Ua1dlw0AAAA1_dVRiSGiD5ejBHhRdV9F	1 with IP address 205.188.116.199 (Used in Truong USCF postings) 1 with IP address 24.90.223.35 (Truong links discussed above) 159 with IP address 152.163.100.67 (Used in Truong USCF postings) 6 with IP address 152.163.101.14 (Used in Truong USCF postings)
Posting account Y_DiAA0AAACY1rJ0q8HGgFyJIqXTrnFm	1 with IP address 24.90.223.35 (Truong links discussed above) 5 with IP address 152.163.101.14 (Used in Truong USCF postings) 6 with IP address 205.188.116.199 (Used in Truong USCF postings)

Factor	*Basis*
	78 with IP address 152.163.100.67 (Used in Truong USCF postings)
Posting account pzt0Dg0AAABJOWkhIGYqJEkINXRErvy4	1 with IP address 152.163.101.14 (Used in Truong USCF postings)
	10 with IP address 205.188.116.199 (Used in Truong USCF postings)
	37 with IP address 152.163.100.67 (Used in Truong USCF postings)
	5 with IP address 24.90.223.35 (Truong links discussed above)
Posting account ps2QrAMAAAA6_jCuRt2JEIpn5Otqf_w0	12 with IP address 205.188.116.199 (Used in Truong USCF postings)
	19 with IP address 75.111.194.9 (Used in Truong USCF postings and shows uncommon header discussed earlier)
	2 with IP address 205.188.116.136 (Used in Truong USCF postings)
	3 with IP address 152.163.100.132 (Used in Truong USCF postings)
	3 with IP address 75.111.199.177 (Used in Truong USCF postings and shows uncommon header discussed earlier)
Posting account PJnN4g0AAACIDMDStNEqBAzSP-8kyXrH	2 with IP address 152.163.100.67 (Used in Truong USCF postings)
Posting account rAlDGA0AAABcQDPBXQBCjuONumvMJieL	3 with IP address 152.163.101.14 (Used in Truong USCF postings)
	3 with IP address 205.188.116.199 (Used in Truong USCF postings)

Table 13 - Summary of links I found between FSS and Truong

Given the many different links between the postings identified with FSS and Truong, it seems apparent that there are many different and largely independent reasons to attribute FSS postings to Truong, many involving a range of different combinations of factors.

Everything I have reviewed related to this matter from a standpoint of digital forensic evidence and in the context of the relevant records provided to me, is consistent with identified FSS postings being initiated and sourced by Truong, and I have found no basis in the digital forensic evidence to refute such a claim.

Attribution of access to privileged communications

The USCF and their related parties assert that privileged emails at issue were taken by an unauthorized party, Alexander, then disclosed to a second unauthorized party, Polgar, and then disclosed to others. The basis for this claim is the presence of specific sequences of words at different times in different messages and postings, and other related records.

The color codes for this section of this report

The color coding in this section is used to demonstrate how different elements are linked together. In particular:

The red coloring is used to indicate the IP address 76.121.230.165 and information linked to that specific IP addresses apparently used by Alexander for unauthorized access to Mr. Hough's email account, for access to an anonymizing service used to access that account, for postings to newsgroups, and for postings to the USCF online forum, and as an IP address apparently assigned to him by Comcast Communications.

The yellow coloring is associated with unauthorized accesses to an email account containing confidential and/or privileged information at particular times between when the information first came to be realized in digital form and when it was subsequently first released by Polgar.

The green coloring is used to indicate the IP address 71.197.185.76 and information linked to that specific IP addresses apparently used by Alexander for unauthorized access to Mr. Hough's email account, for access to an anonymizing service used to access that account, for postings to newsgroups, and for postings to the USCF online forum, as an IP address apparently assigned to him by Comcast Communications, for postings and administration of the "USCF-SAID.BLOGSPOT.COM" blog, and for use of the "uscf_said@yahoo.com" Yahoo! account used to create and support that blog.

The light blue coloring is used to indicate the IP address 76.104.213.144 and information linked to that specific IP addresses apparently used by Alexander for unauthorized access to Mr. Hough's email account, access to an anonymizing service used to access that account, for postings to newsgroups, and for postings to the USCF online forum, as an IP address

apparently assigned to him by Comcast Communications, and for postings and administration of the "USCF-SAID.BLOGSPOT.COM" blog.

The darker blue coloring is used to indicate IP address 128.241.108.179 and information linked to that specific IP address apparently used by Alexander for unauthorized access to Mr. Hough's email account and subsequent use of the "uscf_said@yahoo.com" Yahoo! account used to create and support that blog.

The gold coloring is used to indicate IP address 207.195.241.249 and information linked to that specific IP address apparently used by Alexander for unauthorized access to Mr. Hough's email account and subsequent use of the "uscf_said@yahoo.com" Yahoo! account used to create and support that blog and for postings and administration of the "USCF-SAID.BLOGSPOT.COM" blog.

The orange coloring is used to indicate IP address 207.67.148.229 and information linked to that specific IP address apparently used by Alexander for unauthorized access to Mr. Hough's email account and for subsequent access to postings and administration of the "USCF-SAID.BLOGSPOT.COM" blog.

The gray coloring is used to indicate an unauthorized access made to Mr. Hough's email account between the time of the first creation of a sequence of words and its subsequent disclosure less than 24 hours later by Polgar.

The emails are asserted to be privileged and taken

According to [HOUGH]:

- He is the authorized user of the email address randallhough@yahoo.com.

- He does use and has, over the period at issue in this case, used this account for confidential communications with USCF board members and attorneys relative to legal matters and business matters, as well as personal emails, and including, without limit, confidential and privileged communications regarding legal matters underway between USCF, Truong, and Polgar.

- He indicates that the specifics of the claimed unauthorized accesses to the email address randallhough@yahoo.com relating to this matter, and specifically with regard to the fact that these identified accesses were not by him and not authorized by him, are true.

Access to the randallhough account from Alexander's Comcast addresses

According to [POAMD-A], access to the Yahoo! account associated with the email address randallhough@yahoo.com was attempted from various IP addresses on various dates and at various times. In particular, and without limit, these include:

User name	IP address	Date and time of login attempts
randallhough	76.121.230.165	Fri 06:56:55 (GMT) 18-Apr-2008
randallhough	76.121.230.165	Wed 06:34:24 (GMT) 16-Apr-2008
randallhough	76.121.230.165	Mon 07:22:59 (GMT) 14-Apr-2008
randallhough	76.121.230.165	Sun 08:14:05 (GMT) 13-Apr-2008
randallhough	76.121.230.165	Sat 08:22:24 (GMT) 12-Apr-2008
randallhough	76.121.230.165	Wed 08:49:09 (GMT) 12-Mar-2008
randallhough	76.121.230.165	Sun 11:02:28 (GMT) 09-Mar-2008
randallhough	76.121.230.165	Sat 09:06:32 (GMT) 08-Mar-2008
randallhough	76.121.230.165	Wed 08:02:06 (GMT) 05-Mar-2008
randallhough	76.121.230.165	Tue 08:33:27 (GMT) 04-Mar-2008
randallhough	76.121.230.165	Sun 08:53:12 (GMT) 02-Mar-2008
randallhough	76.121.230.165	Sat 08:50:33 (GMT) 01-Mar-2008
randallhough	76.121.230.165	Tue 09:24:49 (GMT) 26-Feb-2008
randallhough	71.197.185.76	Wed 08:04:02 (GMT) 28-Nov-2007
randallhough	71.197.185.76	Tue 08:03:31 (GMT) 27-Nov-2007
randallhough	71.197.185.76	Mon 09:00:49 (GMT) 26-Nov-2007
randallhough	76.104.213.144	Sun 09:38:17 (GMT) 17-Feb-2008
randallhough	76.104.213.144	Sun 09:30:06 (GMT) 17-Feb-2008
randallhough	76.104.213.144	Sun 08:54:02 (GMT) 20-Jan-2008
randallhough	76.104.213.144	Fri 07:59:00 (GMT) 18-Jan-2008
randallhough	76.104.213.144	Thu 06:49:03 (GMT) 17-Jan-2008
randallhough	76.104.213.144	Wed 09:34:00 (GMT) 02-Jan-2008
randallhough	76.104.213.144	Wed 08:41:19 (GMT) 05-Dec-2007

Table 14 - Unauthorized accesses to randallhough@yahoo.com

According to lookups undertaken, [POAMD-B] "Comcast Cable Communications, Inc." was, at the time, the company that controlled the IP addresses identified above, with the IP address range "71.192.0.0 - 71.207.255.255" was handled by "Comcast Cable Communications, IP Services WASHINGTON-16," "76.104.128.0 - 76.104.255.255" by "Comcast Cable Communications, IP Services WASHINGTON-19," and "76.121.0.0 - 76.121.255.255" handled by "Comcast Cable Communications, IP Services WASHINGTON-22".

I am informed that, based on that information, a subpoena was issued to Comcast to attain the information on the account holder associated with the use of those IP addresses in those time frames.

According to [POAMD-D], a letter from Comcast to Alexander, the response to a subpoena of records regarding the IP addresses identified above indicating its upcoming release of this data. This is confirmed by "Letter dated 12.1.08 from G. Alexander re. Subpoenas - filed w_court (DATED 12.5.08).PDF", a letter with attachments, written to and filed with the US District Court, Northern District of California, that declares that the letter from Comcast was to him and includes the letter from Comcast in this regard.

According to [JMR-Dec], Alexander admitted in open court that the IP address 76.121.230.165 identified by Comcast, the company providing that IP address as a service to its customers, was assigned to Alexander over the period in question.

According to [MN-Dec], the IP addresses 76.121.230.165, 71.197.185.76, and 76.104.213.144 were all used to access the United States Chess Federation's online facilities by a user identified as "gregory" (internal identity # 793), an identity associated with Alexander in various postings that I found in RGCM as well as in [MN-Dec].

- 76.121.230.165 was used by "gregory" on 2008-03-11 at 03:05:05 (no time zone is identified), a time period during which the same IP address was used for unauthorized access to randallhough@yahoo.com.

- 76.104.213.144 was used by "gregory" on 2008-02-16 at 03:11:52 (no time zone is identified), a time period during which the same IP address was used for unauthorized access to randallhough@yahoo.com.

- 71.197.185.76 was used by "gregory" on 2007-11-25 at 14:52:30 (no time zone is identified), a time period during which the same IP address was used for unauthorized access to randallhough@yahoo.com. I also found this IP address identified as the "NNTP-Posting-Host:" for newsgroup postings RGCM282792, RGCM282836, RGCP314083, RGCP314105, RGCP315200, RGCP316187, RGCP325916, RGCP325918, RGCP325927, RGCP325958, RGCP325962, RGCP325964,

RGCP325965, RGCP325968, RGCP325970, RGCP326062, RGCP326063, RGCP326065, RGCP326066, RGCP326067, RGCP326068, RGCP326262, RGCP326263, RGCP326269, and RGCP325466, all also indicated as "From: Gregory <gregory@tatiana.net>".

The Yahoo! address records in combination with either of the USCF records or the Comcast records provide the means to attribute identified unauthorized uses of the email account randallhough@yahoo.com to Alexander. In combination, these records are independently confirmative and consistent with Alexander gaining access to randallhough@yahoo.com on at least 26 occasions over the period from December 5, 2007 through April 18, 2008.

In addition, all of these IP addresses are IP addresses used by the user identity associated with Alexander to make postings to USCF online forums. [USCF-AccessIPs]

Access to the randallhough account from Other IP Addresses

According to [POAMD-E], access to the Yahoo! account associated with the email address randallhough@yahoo.com was attempted from various IP addresses on various dates and at various times. In particular, and without limit, these include:

User name	IP address	Date and time of login attempts
randallhough	128.241.108.179	Fri 09:13:10 (GMT) 08-Aug-2008
randallhough	198.172.202.2	Thu 08:40:44 (GMT) 07-Aug-2008
randallhough	207.67.148.229	Wed 08:59:40 (GMT) 06-Aug-2008
randallhough	130.94.133.28	Tue 08:07:48 (GMT) 05-Aug-2008
randallhough	198.65.166.218	Fri 10:37:30 (GMT) 01-Aug-2008
randallhough	198.65.166.218	Fri 10:16:20 (GMT) 01-Aug-2008
randallhough	207.67.145.169	Mon 09:27:09 (GMT) 21-Jul-2008
randallhough	207.67.145.169	Mon 09:24:04 (GMT) 21-Jul-2008
randallhough	207.67.145.222	Sun 09:28:28 (GMT) 20-Jul-2008
randallhough	130.94.123.71	Wed 09:24:07 (GMT) 16-Jul-2008
randallhough	128.241.108.41	Fri 07:23:58 (GMT) 11-Jul-2008
randallhough	128.241.46.94	Mon 08:39:02 (GMT) 07-Jul-2008
randallhough	205.212.79.15	Sun 08:24:00 (GMT) 06-Jul-2008
randallhough	128.241.104.124	Sat 09:07:27 (GMT) 05-Jul-2008

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

User name	IP address	Date and time of login attempts
randallhough	207.67.145.132	Fri 07:10:16 (GMT) 04-Jul-2008
randallhough	198.172.206.109	Sat 06:48:54 (GMT) 28-Jun-2008
randallhough	207.67.144.247	Thu 07:22:14 (GMT) 26-Jun-2008
randallhough	128.241.41.136	Tue 06:49:44 (GMT) 24-Jun-2008
randallhough	198.172.207.87	Mon 07:17:27 (GMT) 23-Jun-2008
randallhough	128.241.45.210	Sat 07:54:31 (GMT) 21-Jun-2008
randallhough	128.241.110.86	Fri 07:16:49 (GMT) 20-Jun-2008
randallhough	128.241.109.234	Thu 07:40:17 (GMT) 19-Jun-2008
randallhough	130.94.107.233	Mon 07:56:03 (GMT) 16-Jun-2008
randallhough	205.212.78.19	Thu 07:00:06 (GMT) 12-Jun-2008
randallhough	128.241.105.151	Tue 06:27:17 (GMT) 10-Jun-2008
randallhough	207.67.145.144	Mon 07:44:35 (GMT) 09-Jun-2008
randallhough	198.172.203.227	Sat 07:54:47 (GMT) 07-Jun-2008
randallhough	128.241.104.14	Fri 07:41:36 (GMT) 06-Jun-2008
randallhough	205.212.78.20	Thu 06:57:33 (GMT) 05-Jun-2008
randallhough	207.67.146.76	Tue 07:24:22 (GMT) 03-Jun-2008
randallhough	128.241.109.75	Fri 06:36:53 (GMT) 30-May-2008
randallhough	128.241.43.144	Thu 07:38:53 (GMT) 22-May-2008
randallhough	205.212.73.144	Thu 07:26:07 (GMT) 15-May-2008
randallhough	205.212.73.176	Tue 07:51:55 (GMT) 13-May-2008
randallhough	205.212.75.144	Sun 08:47:27 (GMT) 11-May-2008
randallhough	128.241.105.0	Sat 08:35:30 (GMT) 03-May-2008
randallhough	130.94.134.192	Fri 07:53:53 (GMT) 02-May-2008
randallhough	128.241.107.235	Thu 08:36:45 (GMT) 01-May-2008
randallhough	130.94.133.64	Wed 08:12:04 (GMT) 30-Apr-2008
randallhough	128.241.107.235	Tue 07:05:49 (GMT) 29-Apr-2008
randallhough	205.212.72.97	Mon 08:46:41 (GMT) 28-Apr-200
randallhough	168.143.120.64	Mon 07:37:33 (GMT) 21-Apr-2008
randallhough	128.241.111.27	Tue 07:43:49 (GMT) 15-Apr-2008

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

User name	IP address	Date and time of login attempts
randallhough	205.212.73.144	Sat 03:36:58 (GMT) 05-Apr-2008
randallhough	207.67.151.112	Wed 13:20:45 (GMT) 02-Apr-2008
randallhough	207.67.151.112	Thu 12:50:01 (GMT) 27-Mar-2008
randallhough	128.241.107.27	Wed 12:28:32 (GMT) 26-Mar-2008
randallhough	205.212.74.112	Wed 06:55:34 (GMT) 27-Feb-2008
randallhough	128.241.109.241	Mon 08:09:52 (GMT) 25-Feb-2008
randallhough	207.67.148.224	Sun 08:52:45 (GMT) 24-Feb-2008
randallhough	128.241.45.5	Wed 08:26:32 (GMT) 20-Feb-2008
randallhough	198.172.206.84	Tue 09:07:58 (GMT) 19-Feb-2008
randallhough	198.172.207.125	Thu 07:47:12 (GMT) 14-Feb-2008
randallhough	198.172.201.226	Wed 08:37:30 (GMT) 13-Feb-2008
randallhough	130.94.107.215	Tue 07:58:59 (GMT) 12-Feb-2008
randallhough	128.241.40.25	Sun 09:19:12 (GMT) 10-Feb-2008
randallhough	207.67.148.160	Fri 08:05:37 (GMT) 08-Feb-2008
randallhough	128.241.40.167	Wed 08:41:19 (GMT) 06-Feb-2008
randallhough	198.172.206.24	Tue 08:04:32 (GMT) 05-Feb-2008
randallhough	198.172.206.24	Tue 07:35:09 (GMT) 05-Feb-2008
randallhough	128.241.41.212	Mon 08:00:44 (GMT) 04-Feb-2008
randallhough	128.241.108.255	Sun 08:08:34 (GMT) 03-Feb-2008
randallhough	130.94.121.246	Sat 08:56:44 (GMT) 02-Feb-2008
randallhough	128.241.104.188	Fri 08:27:37 (GMT) 01-Feb-2008
randallhough	128.241.105.195	Wed 08:12:29 (GMT) 30-Jan-2008
randallhough	128.241.46.246	Mon 08:32:17 (GMT) 28-Jan-2008
randallhough	198.172.207.108	Sun 08:51:51 (GMT) 27-Jan-2008
randallhough	128.241.46.163	Sat 07:50:22 (GMT) 26-Jan-2008
randallhough	198.172.207.31	Fri 07:49:24 (GMT) 25-Jan-2008
randallhough	198.172.206.168	Thu 08:18:14 (GMT) 24-Jan-2008
randallhough	130.94.107.155	Wed 08:17:21 (GMT) 23-Jan-2008
randallhough	128.241.105.253	Wed 04:59:51 (GMT) 23-Jan-2008

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

User name	IP address	Date and time of login attempts
randallhough	128.241.40.146	Mon 07:50:54 (GMT) 21-Jan-2008
randallhough	128.241.105.37	Mon 06:17:29 (GMT) 21-Jan-2008
randallhough	128.241.46.162	Sat 06:03:12 (GMT) 19-Jan-2008
randallhough	128.241.110.140	Fri 04:14:36 (GMT) 18-Jan-2008
randallhough	128.241.110.173	Wed 05:40:20 (GMT) 16-Jan-2008
randallhough	128.241.110.173	Tue 07:27:23 (GMT) 15-Jan-2008
randallhough	128.241.40.69	Mon 06:54:01 (GMT) 14-Jan-2008
randallhough	128.241.40.69	Sun 07:58:40 (GMT) 13-Jan-2008
randallhough	128.241.104.112	Thu 08:27:13 (GMT) 10-Jan-2008
randallhough	198.172.206.129	Tue 08:45:43 (GMT) 08-Jan-2008
randallhough	198.172.207.93	Mon 08:02:22 (GMT) 07-Jan-2008
randallhough	207.67.151.112	Sun 09:30:20 (GMT) 06-Jan-200
randallhough	128.241.111.22	Sat 10:24:53 (GMT) 05-Jan-2008
randallhough	128.241.109.157	Fri 09:15:07 (GMT) 04-Jan-2008
randallhough	128.241.46.108	Thu 08:54:35 (GMT) 27-Dec-2007
randallhough	130.94.107.179	Sat 09:23:52 (GMT) 22-Dec-2007
randallhough	207.67.148.48	Sun 09:27:23 (GMT) 16-Dec-2007
randallhough	198.172.206.72	Sat 08:32:36 (GMT) 15-Dec-2007
randallhough	198.172.206.67	Sun 10:28:16 (GMT) 09-Dec-2007
randallhough	207.67.148.160	Sat 09:02:48 (GMT) 08-Dec-2007
randallhough	128.241.45.221	Fri 06:20:59 (GMT) 07-Dec-2007
randallhough	128.241.45.221	Thu 07:18:09 (GMT) 06-Dec-2007
randallhough	128.241.40.146	Tue 07:22:00 (GMT) 04-Dec-2007
randallhough	128.241.109.240	Mon 08:04:55 (GMT) 03-Dec-2007
randallhough	128.241.110.113	Sun 08:09:13 (GMT) 02-Dec-2007
randallhough	128.241.111.116	Fri 07:57:25 (GMT) 30-Nov-2007

Table 15 - Records of unauthorized accesses to randallhough@yahoo.com

Records subpoenaed from anonymizer.com

IP addresses listed above were identified by NCT America [NTT-Resp][NTT-Resp2] as used by Anonymizer Inc.

Anonymizer Inc., in response to subpoena, indicated [Anon] that the IP address used by the Anonymizer user identified by the user name "gregoryalexander", included 71.197.185.76, 76.104.213.144, 76.121.230.165, 202.137.100.203, 202.137.100.239, and 202.137.103.184.

According to [POAMD-G], an account holder named "Gregory Alexander", had the username "gregoryalexander", a contact email gregory@tatiana.net, and a billing address of 8416 Monte Cristo Dr., Everett, WA 98202, created an Anonymizer account on September 28, 2007 for "Anonymous Surfing, Digital Shredder Lite, ...", and created that account from originating IP address 76.121.230.165.

Of these IP addresses, 71.197.185.76, 76.104.213.144, 76.121.230.165, and 202.137.100.239 were all used by the user identity associated with Alexander to post information at the USCF online forums. [USCF-AccessIPs]

The content of confidential emails was first disclosed by Polgar

At lease two privileged emails that were kept in Mr. Hough's email account "randallhough@yahoo.com" came to be in the unauthorized possession of Polgar and came to be first publicly released by Polgar after that account was accessed without authorization by Alexander.

Polgar first publicly released portions from a 2007-11-27 privileged email

According to [Affit], an attorney-client privileged email from Karl Kronenberger to the Legal Subcommittee of the USCF, which included Mr. Hough and as received at his email address "randallhough@yahoo.com", was sent on November 27, 2007, at 10:37 PST, with the subject line, "Next Steps re: Truong and Polgar." I will identify this message as [Priv1]

According to the records shown above, unauthorized access to the account "randallhough@yahoo.com" was made by accounts and addresses under the control of Alexander between the date and time of the identified email and 2008-01-13, including, without limit, on Wed 08:04:02 (GMT) 28-Nov-2007, Wed 09:34:00 (GMT) 02-Jan-2008, Wed 08:41:19 (GMT) 05-Dec-2007 from Comcast addresses assigned to and used by Alexander and Sun 07:58:40 (GMT) 13-Jan-2008, Thu 08:27:13 (GMT) 10-Jan-2008, Tue 08:45:43 (GMT) 08-Jan-2008, Mon 08:02:22 (GMT) 07-Jan-2008, Sun 09:30:20 (GMT) 06-Jan-200, Sat 10:24:53 (GMT) 05-Jan-2008, Fri 09:15:07 (GMT) 04-Jan-2008, Thu 08:54:35 (GMT) 27-Dec-2007, Sat 09:23:52 (GMT) 22-Dec-2007, Sun 09:27:23 (GMT)

16-Dec-2007, Sat 08:32:36 (GMT) 15-Dec-2007, Sun 10:28:16 (GMT) 09-Dec-2007, Sat 09:02:48 (GMT) 08-Dec-2007, Fri 06:20:59 (GMT) 07-Dec-2007, Thu 07:18:09 (GMT) 06-Dec-2007, Tue 07:22:00 (GMT) 04-Dec-2007, Mon 08:04:55 (GMT) 03-Dec-2007, Sun 08:09:13 (GMT) 02-Dec-2007, and , Fri 07:57:25 (GMT) 30-Nov-2007 from IP addresses associated with Alexander's Anonymizer account.

The email depicted in and identified as [PE1] was received by USCF attorney Jeremy Brown on or about 2008-01-13 at 16:51:53 EST. This email reflects a message sent from Polgar's AOL email address (susanpolgar@aol.com) and that Polgar has not denied sending, which, as depicted, contains paragraphs identified to me by counsel as excepts from [Priv1] In addition, the AOL Terms of Service agreement for registered users [AOLTOS] states:

> "You are responsible for all activities under your account, including the use of your account and Screen Name by others."

I searched RGCP and RGCM for partial sequences from these paragraphs and have found no evidence that shows that these sequences appeared in any other venue at any earlier time.

All of the original recipients and the original sender of [Priv1] have sworn under oath that they did not disclose this information to any other party over this period [Afit] with the exception of one ex-board member who provided a signed letter so stating.

Alexander worked, over the period in question, on a volunteer basis, and with minimal remuneration, managing Polgar's Web site, and performs other tasks for Polgar at her request. [Polgar-Dec] [Polgar-Request]

In summary, based on the evidence and analysis above, it appears that:

- A privileged email was sent on November 27, 2007, 10:37 a.m. PST and stored in Mr. Hough's "randallhough@yahoo.com" email account.
- That account was accessed by Alexander between the time of that email and the time of the first release of its content.
- Alexander worked for Polgar on a volunteer basis at that time.
- Polgar first publicly released exact content from that email on or about January 12, 2008.

  Polgar first released the confidential information from [Priv1] after it was accessible to Alexander through his unauthorized access to Mr. Hough's "randallhough@yahoo.com" email account and before it was otherwise available through any other means.

Polgar first publicly released portions from a 2008-06-23 private email

A confidential but not privileged email from Bill Goichberg to Randy Hough and Jim Berry was received by Randy Hough at his "randallhough@yahoo.com" email account on or about June 22, 2008 at 17:48:24 CDT, with the subject line, "Military liaison." This email, which is not asserted as attorney-client privileged, is included with this report in the "Referenced" directory [PE2]. All parties involved with this email indicate that they did not disclose this email over the period in question. [NotDisclosed]

According to the records shown above, unauthorized access to the account "randallhough@yahoo.com" was made by one address under the control of Alexander at Mon 07:17:27 (GMT) 23-Jun-2008. This corresponds to an offset of 5 hours from CDT, or 02:17:27 CDT on June 23, 2008.

On June 23, 2008 at or about 13:57:15 CDT, Susan Polgar sent an email [PE3], to board member Jim Berry, quoting verbatim from Bill Goichberg's confidential email of the previous day. This email contains traces demonstrating a discussion between Bill Goichberg and Jim Berry.

I have found no evidence that shows that this email or its contents appeared in any other venue at any earlier time, and all of the original recipients and the original sender of [PE2] have indicated that they did not disclose this information to any other party over this period. [NotDisclosed]

Alexander worked, over the period in question, on a volunteer basis, and with minimal remuneration, managing Polgar's Web site, and performs other tasks for Polgar at her request. [Polgar-Dec] [Polgar-Request]

In summary, based on the evidence and analysis above, it appears that:

- A confidential but not privileged email was sent on June 22, 2008 at 17:48:24 CDT and stored in Mr. Hough's "randallhough@yahoo.com" email account.

- That account was accessed by Alexander between the time of that email and the time of the first release of its content.

- Alexander worked for Polgar on a volunteer basis at that time.

- Polgar first publicly released exact content from that email on or about June 23, 2008 at or about 13:57:15 CDT.

  Polgar first released the confidential information from [PE2] after it was accessible to Alexander through his unauthorized access to Mr. Hough's "randallhough@yahoo.com" email account and before it was otherwise available through any other means.

Alexander subsequently publicly released privileged emails

According to [POPP], on or about July 31, 2008, the contents of the two emails identified above and of other privileged and/or confidential emails that were, over the period in question, stored in and/or sent to or from Mr. Hough's "randallhough@yahoo.com" email account, were published on an Internet site identified as "uscf-said.blogspot.com". [POPP] also indicates that at least 6 confidential emails (redacted in POPP) were placed on that site.

According to [POPP-A], a log provided under subpoena from Google, the subscriber and recent IP address information for the Blogger account "uscf-said.blogspot.com" indicates as follows:

- The Blog Owner is the user name "uscf_said@yahoo.com".

- The email address of the owner is "uscf_said@yahoo.com".

- The blog was created 2008-07-31 at 02:00:33.739 GMT (Zulu time)

- The blog was accessed at times indicated as 2008-07-30 starting at 19:02 PDT (7 hours offset from GMT) and repeating until 21:57 PDT, which corresponds to 2008-07-31 from 02:02 to 03:57 GMT, and those accesses came from IP address 207.195.241.249.

- The blog was accessed two times indicated as at 2008-07-31 at 01:02:00 PDT (2008-07-31 at 08:02:00 GMT) from IP address 198.172.201.50

- The blog was accessed one time on 2008-08-06 at 21:43:00 PDT from IP address 207.67.148.229. This IP address was also used, according to the Anonymizer logs discussed above, to obtain unauthorized access to the email account randallhough@yahoo.com on or about 2008-08-06 at or about 08:59:40 GMT, or 01:59:40 PDT, apparently by Alexander.

According to [POPP-B], a Yahoo! account management tool output describing the account associated with the email address "uscf_said@yahoo.com", which was provided under subpoena, indicates as follows:

- The Yahoo! mail name used to create the account at issue was uscf_said@yahoo.com.

- The IP address used to create this account was 128.241.107.234.

- The account was created on 2008-07-30 at 04:10:13 GMT.

- A total of 5 accesses were identified in the date range from 2007-11-21 to 2008-10-20. They include accesses from IP addresses at dates:

  ○ 207.195.241.249 on 2008-07-31 at 01:54:04 GMT, the date and time at which the blog was created.

- ○ 128.241.108.179 (2008-08-08 at 21:52:39, 22:26:08, and 23:53:19 GMT) This IP address was also used, according to the Anonymizer logs discussed above, to obtain unauthorized access to the email account randallhough@yahoo.com on or about 2008-08-08 at or about 09:13:10 GMT, or 02:13:10 PDT, apparently by Alexander.

- ○ 128.95.225.11 (2008-08-31 at 13:22:48 GMT), an IP address used by the user identity associated with Alexander and used to post to USCF online forums. [USCF-AccessIPs]

A summary of the time sequence of events

The sequence of events with respect to the "uscf-said.blogspot.com" Web site is then summarized as follows:

- **2008-07-30 at 04:10:13 GMT**: The account "uscf_said@yahoo.com" was created on or about 2008-07-30 at 04:10:13 GMT from an IP address 128.241.107.234. [POPP-A] This is in the IP address range of other addresses associated with Anonymizer and under the control of NTT America. [NTT-Resp]

- **2008-07-31 at 02:00:33.739 GMT**: The "uscf-said.blogspot.com" blog was created using the "uscf_said@yahoo.com" Yahoo! account for ownership identification, and accessed at that time from Anonymizer IP address 207.195.241.249.[POPP-B] Access through Anonymizer at this time was undertaken by the user identified as Alexander from IP address 76.121.230.165. [Anon] This 76.121.230.165 IP address was also used by the user identity associated with Alexander to post to USCF online forums. [USCF-AccessIPs]

- **2008-07-31 from 02:02 to 03:57 GMT**: The "uscf-said.blogspot.com" blog was accessed repeatedly from IP address 207.195.241.249. Access through Anonymizer at this time was undertaken by the user identified as Alexander from IP address 76.121.230.165. [Anon] This 76.121.230.165 IP address was also used by the user identity associated with Alexander to post to USCF online forums. [USCF-AccessIPs]

- **2008-07-31 at 08:02:00 GMT**: The "uscf-said.blogspot.com" blog is accessed two times from IP address 198.172.201.50 [POPP-B].

- **2008-08-06 at 08:59:40 GMT**: IP address 207.67.148.229 is used, to obtain unauthorized access to the randallhough@yahoo.com email account, by an individual identified as Alexander according to the Anonymizer logs and analysis discussed above.

- **2008-08-07 at 04:43:00 GMT**: The same IP address 207.67.148.229 is used to access the blog "uscf-said.blogspot.com" [POPP-A]

- **2008-08-08 at 09:13:10 GMT**: The IP address 128.241.108.179 is used to obtain unauthorized access to the randallhough@yahoo.com email account, by an individual identified as Alexander according to the Anonymizer logs and analysis discussed above.

- **2008-08-08 at 21:52:39, 22:26:08, and 23:53:19 GMT**: The same IP address 128.241.108.179 is used to access the "uscf_said@yahoo.com" Yahoo! account.

- **2008-08-31 at 13:22:48 GMT**: The IP address 128.95.225.11 is used to access the blog "uscf-said.blogspot.com" [POPP-A] This is also an IP address used by Alexander for postings to RGCP and RGCM, and an IP address used by the user identity associated with Alexander to post to USCF online forums. [USCF-AccessIPs]. According to [POPP-C], the IP address 128.95.225.11 was associated with MAC address 001279ACAC73 on 2008-08-31 at 13:32:48 GMT at the University of Washington, in an area of that University where Alexander worked.

Other links to Alexander

I searched RGCM and RGCP for postings using the IP addresses associated with the creation and operation of the "uscf_said@yahoo.com" email address and "uscf-said.blogspot.com" and found that IP address 128.95.225.11 was also identified as a posting-host for postings including, without limit:

> RGCP314974 RGCP320817 RGCP320823 RGCP326048 RGCP326049
> RGCP326050 RGCP326215 RGCP326216 RGCP326224 RGCP326232
> RGCP326235 RGCP326237 RGCP326242 RGCP326244 RGCP326247
> RGCP326251 RGCM283837 RGCM289090 RGCM289101

> **Each of these postings is "From: Gregory <gregory@tatiana.net>", the user identity associated with Alexander from the domain operated by Alexander, as described in [POAMD-G]. This IP address was also used by the user identity associated with Alexander to post to USCF online forums. [USCF-AccessIPs]**

I searched RGCM and RGCP for postings using the IP addresses associated with the creation and use of Anonymizer Inc. and found that the IP address 76.121.230.165 was also identified as a posting-host for postings including, without limit:

RGCP325916 RGCP325918 RGCP325927 RGCP325958 RGCP325962
RGCP325964 RGCP325965 RGCP325968 RGCP325970 RGCP326062
RGCP326063 RGCP326065 RGCP326066 RGCP326067 RGCP326068
RGCP326262 RGCP326263 RGCP326269

Each of these postings is "From: Gregory <gregory@tatiana.net>", the user identity associated with Alexander from the domain operated by Alexander, as described in [POAMD-G]. This IP address was also used by the user identity associated with Alexander to post to USCF online forums. [USCF-AccessIPs]

Only Alexander could have contributed the identified content

These comprise all of the sessions where postings and activities to control the "uscf-said.blogspot.com" blog were identified as recorded by Google, the operator of this site. Polgar's attorney identified that this is the site where she came to first possess the identified confidential information, providing the printout of the Web page prior to the deletion of all of the information from that site. [POPP] This printout appears to demonstrate that this site had this information, but postdates Polgar's prior release of the same information.

Because the details of the postings at this site are redacted, and because the site itself and its content are not now available for examination, I am unable to perform additional analysis that might provide additional attribution and timing information.

Limits of the methods and technologies used

The National Research Council ["Strengthening Forensic Science in the United States: A Path Forward", 2009, ISBN: 978-0-309-13130-8] recommends that "As a general matter, laboratory reports generated as the result of a scientific analysis should be complete and thorough. They should contain, at minimum, "methods and materials," "procedures," "results," "conclusions," and, as appropriate, sources and magnitudes of uncertainty in the procedures and conclusions (e.g., levels of confidence)... Forensic reports, and any courtroom testimony stemming from them, must include clear characterizations of the limitations of the analyses, including measures of uncertainty in reported results and associated estimated probabilities where possible." The Reference Manual on Scientific Evidence states "the theory's testability, whether it was the subject of peer review or publication, its known or potential rate of error, and its general acceptance within the relevant scientific community" [Reference Manual on Scientific Evidence - Second Edition - Federal Judicial Center, 2000]

Tool usage and processing

In carrying out all of these examination, I used an Apple MacBook computer running the OS-X operating system, the Unix "bash" command interpreter, the "Perl" and "Lisp" computer languages, and the programs and mechanisms described herein.

I have found all of these tools and the methods by which they were applied to be reliable for the purposes discussed herein and have used and tested these systems, tools, and methods over a period of years to verify that they operate reliably as applied herein. Many of these tools are used on a daily basis in commercial businesses, in government, in educational institutions, and in other settings, by people from all over the world, and they are generally relied upon for the purposes for which they are used in those contexts, many of which are very similar to the uses I made of those tools as described herein.

Many of the specific techniques described herein have been published in scientific conferences which included peer review processes, and those processes have been accepted within the scientific community to the extent that appearance in peer reviewed publications so indicates.

From a standpoint of identifying possible sources of error and reliability of these tools in this context, I have found that computer programs sometimes produce results that are off by one or otherwise different than what might be attained by hand counts, either because of programming errors that are not detected even after a long period of use, or because of differences in interpretation of what constitutes things like "words", "lines", and so forth.

I have verified each of these results so as to reduce or eliminate such potential errors, and I believe that all of the results herein are accurate as stated.

Methodologies applied and specific reliability factors

The methodologies applied herein for attribution are based on techniques with differing reliability. While I have tried to detail the relevant factors and basis for attributions where applicable, I will briefly summarize here.

- In general, stored data may be altered by those who possess and control it, and data in motion may be sourced falsely, intercepted, or replaced en route. No special mechanisms are identified for this matter that would tend to alter the nature of digital systems in this regard and I did not identify any information that would indicate any such tampering.

- The attributions associated with news postings are based on my retrieval of data from widely used and widely available data sources in the form of postings in news forums that are independently and redundantly kept in the possession and control of a wide array of different providers, none of whom are directly related to the matter at hand. As such, as far as I am aware, no party to this case has had access to the stored form of this data or the transmission path between these providers and my systems. Further, all parties may gain access to the same data I used and verify its accuracy independently from the various sources available for news group content.

- I have found that the information stored in systems that work as part of the open news systems supporting network news transport protocol (NNTP) and the related mechanisms associated with this matter, is generally reliable as to faithfully recording the IP addresses of sending computers upon reception, and doing so independently of the data sent within the news posting, including the originating header information. Thus these specific fields within headers may be considered to accurately reflect the IP addresses in the datagrams sent to the servers that accepted these news postings and made them widely available.

- The data gained by subpoena was, as far as I am aware and as has been so indicated in the responses to these subpoenas, constituted of business records in daily use that are generally relied upon for their accuracy and faithfully recorded.

- The analytical processes used all result in things that were described in terms of how specific information related to other specific information, and the basis for making claims with regard to specifics about those relationships. These may be verified by any party to the case based on the information available to them and provided herein and in the included information with this report.

- No attribution based entirely on digital traces can be relied upon in a vacuum. It is the consistency of the digital traces that brings reliability to it. In this case, all of the digital data I was able to examine appears to be consistent with the attribution results I have presented.

In addition, as to the USCF systems:

- I have no special knowledge of the operation of the USCF systems or mechanisms in place, and my results with regard to these systems and mechanisms rely on the information, reports, and records provided by them.

- The results of my analysis of the USCF data, reports, and information indicates that is that it is consistent with and redundant to my attributions through other independent means. As such, it is confirmatory as to results, but not necessary in order to attribution to be made.

Compensation for this case

My compensation for this case is at the rate of $500 per hour, however, the effort associated with this report was performed at a firm fixed cost of $10,000.

Other cases in the last 4 years

The following is a listing of all other cases in which I have testified as an expert at trial or by deposition within the preceding four years.

In court:

Rose v. Albritton, Superior Court of the County of San Francisco, Case No.: FDV-09-806677, July 14, 2009 (qualified as an expert)

Depositions:

ASIS Internet Services, v. Optin Global, Inc., et. al., - UNITED STATES DISTRICT COURT - NORTHERN DISTRICT OF CALIFORNIA Case No. C-05-5124 JCS, 2008-01-07

Paul Cozza v. McAffee, Inc. United States District Court for the District of Massachusetts, case no. 02-11135RGS, 2006-07-13

Ongoing analysis

Analysis and examination is ongoing and will be supplemented in accordance with applicable court orders and rules.

Signature

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 15th day of September, 2009, in Livermore, California.

_____

Dr. Frederick B. Cohen

Appendix A - My Curriculum Vitae and background

Dr. Fred Cohen
572 Leona Drive
Livermore, CA 94550
http://all.net/
925-454-0171

Education:
Ph.D. Electrical Engineering - University of Southern California, 1986
M.S. Information Science - University of Pittsburgh, 1980
B.S. Electrical Engineering - Carnegie-Mellon University, 1977

Positions (* current):
* President, California Sciences Institute, 11/07 - present
* CEO, Fred Cohen & Associates, 03/86-present
Community Faculty Member, Metropolitan State University, 04/08-01/09
Adjunct Professor, University of San Francisco, 08/07-08/08
Research Professor, University of New Haven, 09/02-08/08
Chairman, Security Posture, 10/02-09/06
Principal Analyst, Burton Group, 4/03-4/06
Principal Member of Technical Staff, Sandia National Laboratories, 10/97-11/02
Chief Computer Forensic Scientist/Investigator, TAL Global, 09/01-11/02
Senior Member Technical Staff, Sandia National Laboratories, 7/96-9/97
Practitioner in Residence, University of New Haven, 06/98-09/02
Senior Scientist, SAIC, Inc., 7/93-6/95
Chairman, AllThings Incorporated, 1/95-1/96
Board Member, AllThings Incorporated, 6/94-1/96
Professor, Queensland University of Technology (visiting), 7/92-12/92
President, The Radon Project, Inc. 3/87-10/89
Asst. Professor, University of Cincinnati, 9/87-12/88
Asst. Professor, Lehigh University, 1/86-8/87
Lecturer, Lehigh University, 1/85-12/85

Editorial Boards:
2007-present, EDP Audit, Control, and Security (EDPACS)
2005-present, "Journal in Computer Virology"
2000-present, "Journal on Computer Crime"
1987-present, IFIP TC-11 Journal "Computers and Security"
1995-2002, "Network Security Magazine"
1990-1993, ACM/SigSAC Annual Student Paper Review Board
1989-1991, DPMA, IEEE, and ACM "Computer Virus and Security Conference"

1989-1991, "Computer Virus Bulletin"
Honors and Awards:
2004: Burton Group Best Award
2002: Sandia Certificate of Appreciation (CCD Program)
2002: Techno-Security Industry Professional of the Year
2001: Sandia Employee Recognition Award (College Cyber Defenders)
2000: Sandia Meritorious Achievement Award (Security Immersion Program)
2000: Sandia Award for Excellence (Cyber Security / Surety)
1999: Sandia Exceptional Service Award (Security Awareness Work)
1998: Sandia Exceptional Service Award (Red Team Work)
1989: UK IT Auditors: Information Technology Award

Books and Book Chapters:
F. Cohen, ""Digital Forensic Evidence Examination" ASP Press, 2009
F. Cohen, ""Enterprise Information Protection Architecture" ASP Press, 2008
F. Cohen, "Challenges to Digital Forensic Evidence" ASP Press, 2008
F. Cohen, "A Framework for Deception", (one chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007. (in press).
F. Cohen, ""Critical Infrastructure Protection: Issues and Answers", (one chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007. (in press).
F. Cohen, "Information Warfare, Netwar, and Cyber Intelligence.", (1 chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007. (in press).
F. Cohen, "Challenges to Digital Forensic Evidence", (one chapter in "Forensic Computer Crime Investigation", Thomas A. Johnson, Ed. Taylor & Francis, 2006
F. Cohen, "IT Security Governance Guidebook with Security Program Metrics on CD-ROM." , Taylor & Francis/CRC Press, 2006
World War 3 ... Information Warfare Basics , ASP Press, 2006
Information Security Awareness Basics , ASP Press, 2006
Frauds, Spies, and Lies - and how to defeat them , ASP Press, 2005
The CISO ToolKit: Security Checklists - Governance , ASP Press, 2005
The CISO ToolKit: Security Metrics , ASP Press, 2005
The CISO ToolKit: Governance Guidebook , ASP Press, 2005
Protection and Security on the Information Superhighway , John Wiley and Sons (1995)
F. Cohen, "It's Alive!!!", John Wiley and Sons (1994)
F. Cohen, "A Short Course in Computer Viruses (2nd edition)", John Wiley and Sons (1994)
F. Cohen, "A Short Course on Systems Administration and Security Under Unix", ASP Press, (1992)

F. Cohen, "Payback - Automated Bill Collection System", ASP Press (1992)
F. Cohen, "A Short Course in Computer Viruses", ASP Press (1991)
F. Cohen, "The ASP Integrity Toolkit", ASP Press (1990)
F. Cohen, "Introductory Information Protection", ASP Press (1987)
F. Cohen, "Computer Viruses", ASP Press, (1985)

Patents:

F. Cohen, *"Method and Apparatus for Network Deception/Emulation"*, US Pat. 7,107,347.

F. Cohen, *"Method and Apparatus for Providing Deception and/or Altered Execution of Logic in an Information System* US Pat. 7,296,274.

F. Cohen, D Koike, V. Nagaeu, "Method and Apparatus Providing Deception and/or Altered Operation in an Information System Operating System", US Pat. 7,437,766 10/679,186

F. Cohen, *"Method and Apparatus for Configurable Communication Network Defenses"* 20040162994 (pending)

F. Cohen, *"Method and Apparatus for Specifying Communication Indication Matching and/or Responses"* 20040153574 (pending)

F. Cohen, *"Method and Apparatus for Invisible Network Responder"* 20040148521 (pending)

F. Cohen, *"Method and/or System for Providing and/or Analyzing Influence Strategies",* (pending)

F. Cohen, *"Method and/or System for Providing and/or Analyzing and/or Presenting Decision Strategies",* 60957455 (pending)

Refereed journal articles

F. Cohen, "Red Teaming Experiments with Deception Technologies", Computers and Security (submitted, Mar. 2007)

F. Cohen and C. Preston, "A Method for Recovering Data From Failing Floppy Disk Drives", Journal of Computer Crime, (Submitted 2006)

F. Cohen, et. al. "Leading Attackers Through Attack Graphs with Deceptions", IFIP-TC11, `Computers and Security', V22#5, July 2003, pp. 402-411(10)

F. Cohen, et. al. "A Mathematical Structure of Simple Defensive Network Deceptions", IFIP-TC11, `Computers and Security', Volume 19, Number 6, 1 October 2000, pp. 520-528(9)

Cohen F.; Phillips C.; Swiler L.P.; Gaylor T.; Leary P.; Rupley F.; Isler R., "A Cause and Effect Model of Attacks on Information Systems. Some Analysis Based on That Model, and The Application of that Model for CyberWarfare in CID", IFIP-TC11 Computers and Security, V17#3, 1998 pp. 211-221 (11)

F. Cohen, "Providing for Responsibility in a Global Information Infrastructure ", IFIP-TC11, `Computers and Security', 1997.

F. Cohen, "Simulating Cyber Attacks, Defenses, and Consequences", IFIP-TC11,

`Computers and Security', 1999, vol. 18, no. 6, pp. 479-518(40)

F. Cohen, et. al. "Intrusion Detection and Response", IFIP-TC11, `Computers and Security', V16,#6, 1997, pp. 516-516(1) (also appearing below under National Info-Sec Technical Baseline studies from Dec, 1996)

F. Cohen, "A Note on the Role of Deception in Information Protection", IFIP-TC11, Computers and Security, 1998, vol. 17, no. 6, pp. 483-506(24)

F. Cohen, "Information System Defences: A Preliminary Classification Scheme", IFIP TC-11, Computers and Security, V16,#2, 1997, pp. 94-114(21)

F. Cohen, "A Note on Distributed Coordinated Attacks", IFIP-TC11, `Computers and Security', Volume 15, Number 2, 1996, pp. 103-121(19), also appearing as an invited paper in *4th Computer Misuse and Anomaly Detection Workshop*, Monterey, 1996 (referenced below).

F. Cohen, "A Secure World-Wide-Web daemon", IFIP-TC11, `Computers and Security', V15#8, 1996, pp. 707-724(18)

F. Cohen, "Operating Systems Protection Through Program Evolution", IFIP-TC11 `Computers and Security' (1993) V12#6 (Oct. 1993) pp.565 - 584

J. Voas, J. Payne, F. Cohen "A Model for Detecting the Existence of Software Corruption in Real-Time", IFIP-TC11 "Computers and Security", V12#3 May, 1993 pp. 275-283.

F. Cohen, "A Formal Definition of Computer Worms and Some Related Results", IFIP-TC11 "Computers and Security" V11#7, November, 1992, pp. 641-652.

F. Cohen, "Defense-In-Depth Against Computer Viruses", IFIP-TC11 "Computers and Security", V11#6, 1992 pp. 563-579.

F. Cohen, "A DOS Based POset Implementation", IFIP-TC11 "Computers and Security", V10#6, October 1991.

F. Cohen, "A Note On High Integrity PC Bootstrapping", IFIP-TC11 "Computers and Security", V10#6, October 1991.

F. Cohen, "A Cost Analysis of Typical Computer Viruses and Defenses", IFIP-TC11 "Computers and Security", V10#3, May, 1991 (also appearing in 4th DPMA, IEEE, ACM Computer Virus and Security Conference, 1991)

F. Cohen, "Automated Integrity Maintenance for Viral Defense", IFIP-TC11 "Computers and Security", 1990

F. Cohen, "Computational Aspects of Computer Viruses", IFIP-TC11, "Computers and Security", V8 pp325-344, 1989.

Y. J. Huang and F. Cohen, "Some Weak Points of One Fast Cryptographic Checksum Algorithm and its Improvement", IFIP-TC11 "Computers and Security", V8#1, February, 1989

B. Cohen and F. Cohen, "Error Prevention at a Radon Measurement Service Laboratory", Radiation Protection Management, V6#1, pp43-47, Jan. 1989

F. Cohen, "Models of Practical Defenses Against Computer Viruses", IFIP-TC11, "Computers and Security", V8#2, April, 1989 pp149-160.

F. Cohen, "Two Secure Network File Servers", IFIP-TC11, "Computers and

Security", V7#4, August, 1988.

F. Cohen, "Designing Provably Correct Information Networks with Digital Diodes", IFIP-TC11, "Computers and Security", V7#3, June, 1988.

F. Cohen, "On the Implications of Computer Viruses and Methods of Defense", Invited Paper, IFIP-TC11, "Computers and Security", V7#2, April, 1988,

F. Cohen, "Maintaining a Poor Person's Information Integrity", IFIP-TC11, "Computers and Security", V7#1, Feb 1988.

F. Cohen, "A Cryptographic Checksum for Integrity Protection", IFIP-TC11 "Computers and Security", V6#6 (Dec. 1987), pp 505-810.

F. Cohen, "Design and Protection of an Information Network Under a Partial Ordering: A Case Study", IFIP-TC11, "Computers and Security", V6#4 (Aug. 1987) pp 332-338.

F. Cohen, "Design and Administration of Distributed and Hierarchical Information Networks Under Partial Orderings", IFIP-TC11, "Computers and Security", V6#3 (June 1987), pp 219-228.

F. Cohen, "Protection and Administration of Information Networks with Partial Orderings", IFIP-TC11, "Computers and Security", V6#2 (April 1987) pp 118-128.

F. Cohen, "Computer Viruses - Theory and Experiments", DOD/NBS 7th Conference on Computer Security, originally appearing in IFIP-sec 84, also appearing as invited paper in IFIP-TC11, "Computers and Security", V6#1 (Jan. 1987), pp 22-35 and other publications in several languages.

F. Cohen, "A Secure Computer Network Design", IFIP-TC11, "Computers and Security", V4#3, (Sept. 1985), pp 189-205, also appearing in AFCEA Symp. and Expo. on Physical and Electronic Security, Aug. 1985.

F. Cohen, "Algorithmic Authentication of Identification", Information Age, V7#1 (Jan. 1985), pp 35-41.

Burton Group Reports:

F. Cohen, "Outsourcing, Offshoring, and Security: What's the Difference?" 28 Jun 2006

F. Cohen, "IT Risk Management and COSO" 24 May 2006

F. Cohen, "Defending Against the Evil Insider" 16 Nov 2005

F. Cohen, "Raising the Bar: Solving Medium-Risk Problems with Medium-Surety Solutions" 27 Sep 2005

P. Schacter and F. Cohen, "Enterprise Strategies for Defending Against Spyware" 23 Aug 2005

F. Cohen, "Security Metrics: Horses for Courses" 24 Jun 2005

F. Cohen, "Security Governance for the Enterprise" 31 Mar 2005

F. Cohen, "Business Continuity Planning for IT" 24 Mar 2005

D. Blum and F. Cohen, "A Systematic, Comprehensive Approach to Information Security" 24 Feb 2005

F. Cohen, "Security Awareness, Training, and Education Programs for the

Enterprise" 17 Jan 2005

F. Cohen, "Change Management for the Enterprise" 17 Jan 2005

D. Blum and F. Cohen, "Concepts and Definitions" 17 Jan 2005

F. Cohen, "Database Security: Protecting the Critical Content of the Enterprise" 28 Oct 2004

F. Cohen, "Building Secure Applications: How secure do you want to be today?" 09 Sep 2004

F. Cohen, "Risk Aggregation: The Unintended Consequence", 27 Apr 2004

F. Cohen, "Auditing and Audit Trails", 18 Mar 2004

F. Cohen, "Patch Management", 2003

F. Cohen, "The Evolving Role of Firewalls", 2003

F. Cohen, "Linux Security Features", 2003 (unpublished)

F. Cohen, "Intrusion Detection and Response Systems", October, 2003

F. Cohen, "Analysis of Information-Related Threats to Enterprises", 18 Sep 2003

F. Cohen, "Risk Management: Concepts and Frameworks", 18 July, 2003

F. Cohen, "Policy-Based Security and Enterprise Policy Management", 9 Dec 2003

Invited Papers and Keynotes:

F. Cohen, "The past and future history of computer viruses", EICAR annual conference, Berlin, Germany, May 11-12, 2009.

F. Cohen, "30 Lies About Secure Electronic Commerce: The Truth Exposed", Institute for International Research Electronic Commerce Conference, Feb. 1999.

F. Cohen, Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, Richard Isler, and Eli Dart "A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model", Encyclopedia of Computer Science, 1999.

F. Cohen, "National Info-Sec Technical Baseline - Intrusion Detection and Response" National InfoSec Research Council, Dec, 1996. (also appearing above in Computers and Security, 1997).

F. Cohen, "A Note on Distributed Coordinated Attacks", *4th Computer Misuse and Anomaly Detection Workshop*, Monterey, 1996 (also appearing above in Computers and Security, 1996).

F. Cohen, "The Internet, ..., and Information Security", Computer Society of South Africa, 7th Annual Conference, August, 1995, South Africa.

F. Cohen, "The Internet, Corporate Networks, and Firewalls", Computer Society of South Africa, 7th Annual Conference, August, 1995, South Africa.

F. Cohen, "Information Assurance", IFIP TC-11 World Congress, May, 1995, Cape Town, South Africa.

F. Cohen, "`Information Warfare Considerations", Norwegian Academy of

Sciences, September, 1993.

F. Cohen, "Computer Viruses", (one chapter in "The Computer Security Reference Book", Butterworth/Heinemann, Oxford, England, 2004.

F. Cohen, "Fault Tolerant Software for Computer Virus Defense", November, 1991.

F. Cohen, "Some Applications of Benevolent Viruses in Networked Computing Environments", `DPMA, IEEE, ACM Computer Virus and Security Conference', March 1993

F. Cohen and S. Mishra, "Some Initial Results From the QUT Virus Research Network", `The Virus Bulletin Conference', Edinburgh, Scotland, July, 1992 (keynote).

F. Cohen, "Computer Viruses", (one chapter in "The Computer Security Reference Book" Butterworth/Heinemann (1992), Oxford, England

F. Cohen, "Current Trends in Computer Viruses", Invited Paper, International Symposium on Information Security, Oct. 17-18, 1991, Tokyo, Japan

F. Cohen, "Current Best Practice Against Computer Viruses", Invited Paper, 1991, 25th IEEE International Carnahan Conference on Security Technology, Oct. 1-3, 1991, Taiwan ROC.

F. Cohen, "Exploiting Defense-In-Depth Against Computer Viruses", Invited Paper, The Oxbridge Sessions, Sept. 3-5, 1991, The Netherlands.

F. Cohen, "Computers Under Attack" (one paper), ACM/Addison Wesley (1990)

F. Cohen, "A Summary of Results on Computer Viruses and Defenses", Invited Paper, 1990 NIST/DOD Conference on Computer Security.

F. Cohen, "Integrity Maintenance in Untrusted Computing Environments", Invited Paper, IBC Computer Virus Conference, London, 1990.

F. Cohen, "Information Systems as a Competitive Weapon", Keynote Address, Utah State School of Business, Annual Computer Conference, March 1-2, 1990.

F. Cohen, "Recent Advances in Integrity Maintenance in Untrusted Systems", Invited Paper, The Netherlands Computer Security Seminar, April 10-12, 1990.

F. Cohen, "A Note on the use of Pattern Matching in Computer Virus Detection", Invited Paper, Computer Security Conference, London, England, Oct 11-13, 1989, also appearing in DPMA, IEEE, ACM Computer Virus Clinic, 1990.

F. Cohen, "Computer Viruses - Attacks and Defensive Measures", London Corporate Computer Security Conference - Keynote Address, London, England, Feb. 14, 1989.

F. Cohen, "Current Trends in Computer Virus Research", 2nd Annual Invited Symposium on Computer Viruses - Keynote Address, Oct. 10, 1988. New York, NY

F. Cohen, "Recovery Techniques in Computer Virus Attack", Invited Paper, Invitational Conference on Computer Viruses, 1988.

Special Cyber Terrorism Studies:

The Provisional Irish Republican Army - 2000
The Animal Liberation Front (ALF) - 2000
Revolutionary Armed Forces of Colombia (FARC) - 2000
National Liberation Army (ELN)--Colombia - 2000
Issues in Cyber-Terrorism - 2000

Short Analyst Reports
2009-09 - Forensics: The limits of my tools, my techniques, and myself
2009-08 - Virtualization and the cloud - Risks and Rewards
2009-07 - The speed of light, it's easy to forge, email is always fast, and more
2009-06 - Security Decisions: Deception - When and where to use it
2009-05-B - Culture clash: Cloud computing and digital forensics
2009-05 - Protection testing: What protection testing should we do?
2009-04-B - Proposed Cyber-Security Law: What's the problem?
2009-04 - Risk management: There are no black swans
2009-03 - How spam vigilantes are wrecking email and encourage violations of law
2009-02-B Digital forensics must come of age
2009-02 - A structure for addressing digital forensics
2009-01 - Change management: How should I handle it?
2008-12-B - Short Note: Twittering away your privacy
2008-12 - Digital Forensic Evidence: A Wave Starting to Break
2008-11 - Security Decision: Zoning your network
2008-10 - Social tension and separation of duties
2008-09 - Default deny is best practice? Not anymore!
2008-08 - Control architecture: Access controls
2008-07 - Fault modeling, the scientific method, and thinking out of the box
2008-06 - Inventory Revisited - How to reduce security losses by 70%?
2008-05 - Control Requirements for Control Systems... Matching Surety to Risk
2008-04 - The Botnets have come - The Botnets have come...
2008-03 - Enterprise Information Protection - It's About the Business
2008-02 - The Digital Forensics World
2008-02 - Who Should Do Your Digital Forensics?
2008-01 - Unintended Consequences
2008-01 - Accidental Security
2007-12 - Security, justice, and the future
2007-12 - Security End-of-year
2007-11 - Security by Psychology
2007-11 - Covert Awareness
2007-10 - Making compliance simple - not
2007-10 - Measuring Compliance
2007-09 - Identity Assurance and Risk Aggregation

2007-09 - Identity Assurance
2007-08 - The ethical challenge
2007-08 - Conflicts of Interest
2007-07 - Security Decision Support
2007-07 - Making Better Security Decisions
2007-06 - User platform selection
2007-06 - Which User Platform
2007-05 - Risk Management
2007-05 - Managing Risks
2007-04 - Security Ethics and the Professional Societies
2007-04 - Information Content Inventory
2007-03 - Emerging Risk Management Space
2007-03 - Sensible Security - You Wouldn't?
2007-02 - Emerging Market Presence
2007-02 - Measuring Security
2007-01 - Market Maturity and Adoption Analysis Summary
2007-01 - Closing the Gap
2007-00 - Analysis Framework
2006-12 - The Security Schedule
2006-11 - The Holidays Bring the Fraudsters
2006-10 - Physical/Logical Convergence??
2006-09 - How can I Show I am Me in Email?
2006-08 - Service Oriented Architecture Security Elements
2006-07 - The Life Expectancy of Defenses
2006-07 - BONUS ISSUE: The End of the World as we Know it
2006-06 - Why the CISO should work for the CEO - Three Case Studies

Conference Papers and Other Publications:

F. Cohen, "Attribution of messages to sources in digital forensics cases", HICSS-43, Jan 7, 2010 (accepted)

F. Cohen, "Analysis of redundant traces for consistency", IEEE International Workshop on Computer Forensics in Software Engineering (CFSE 09), Seattle, Washington, USA, July 20-24, 2009

F. Cohen, "Two models of digital forensics examination with application examples in bulk message analysis", IEEE SADFE (in conjunction with the IEEE Oakland Conference), 2009-05-21, Oakland, CA

F. Cohen, "Issues and a case study in bulk email forensics", Fifth annual IFIP WG 11.9 International Conference on Digital Forensics, 2009/01/27, published as "Bulk Email Forensics" in the conference publication.

F. Cohen and T. Johnson, "A Ph.D. Curriculum for Digital Forensics", HICSS-42, Jan 7, 2009

F. Cohen, "Information Assurance Architectural Models", HICSS-42 Product and

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

Process Assurance Symposium Position Paper, Jan 5, 2009

F. Cohen, "Social tension and separation of duties", EDPACS 38(5) (2009).

F. Cohen, "Control Requirements for Control Systems... Matching Surety to Risk", EDPACS, 2008

F. Cohen, "Making Compliance Simple – Not", EDPACS, March 2008, V37#3.

F. Cohen and C. Preston, "A Method for Recovering Data From Failing Floppy Disks with a Practical Example", Fourth annual IFIP WG 11.9 International Conference on Digital Forensics, 2008/01/27 to 30.

F. Cohen, "Fault Modeling and Root Cause Analysis for Information Security Governance", Computers and Security, 2007.

F. Cohen and D. Koike, "Misleading attackers with deception", Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC Publication Date: 10-11 June 2004: pp. 30- 37

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) " Nov. 2002, Breaking In... to test security?

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) " Oct., 2002 - Reworking Your Firewalls

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) " Sept, 2002 - Deception Rising

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) " Aug, 2002 - You're in a Bind!

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) " July, 2002 - Smashed Again by Stupid Security (appears in Computer Frauds and Security Bulletin)

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) " July, 2002 - Is Open Source More or Less Secure?

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) June, 2002 - Academia's Vital Role in Information Protection

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) May, 2002 - Terrorism and Cyberspace

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) April, 2002 - Misimpressions We Need to Extinguish

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) March, 2002 - Embedded Security

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) February, 2002 - How to Get Around Your ISP

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) January, 2002 - The End of the Internet as we Know it

F. Cohen, "2001: Red Teaming Experiments with Deception Technologies"

F. Cohen, "2001: A Framework for Deception"

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The World Doesn't Want to be Fixed", Network Security, Dec.,

2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Deception Defense", Network Security, Nov., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The DMCA ", Network Security, Oct., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Best Security Book Ever Written ", Network Security, Sep., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Special Issue - The Balancing Act ", Network Security, Sep., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Bootable CDs", Network Security, Aug., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - A Matter of Power", Network Security, Jul., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Wireless Revolution", Network Security, Jun., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The New Cyber Gang - A Real Threat Profile ", Network Security, May., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - To Prosecute or Not to Prosecute", Network Security, Apr., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Corporate Security Intelligence", Network Security, Mar., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Testing Your Security by Breaking In - NOT ", Network Security, Feb., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Marketing Hyperbole at its Finest", Network Security, Jan., 2001.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Millennium Article - Yet Again! - The Bots are Coming!!! The Bots are Coming!!!", Network Security, Dec., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Why Everything Keeps Failing", Network Security, Nov., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Threat", Network Security, Oct., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Chipping ", Network Security, Sep., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Understanding Viruses Bio-logically", Network Security, Aug., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - What does it do behind your back?", Network Security, Jul., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security

Magazine) - Why Can't We Do DNS Right?", Network Security, June, 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Eliminating IP Address Forgery - 5 Years Old and Going Strong ", Network Security, May, 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Countering DCAs", Network Security, Apr., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Collaborative Defense", Network Security, Mar., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Worker Monitoring ", Network Security, Feb., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Digital Forensics ", Network Security, Jan., 2000.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Why it was done that way", Network Security, Dec., 1999.

F. Cohen, " So Much Evidence... So Little Time", Information Security Magazine, November. 1999. Special issue with articles by "The 20 Most Influential Figures in Information Security Today."

F. Cohen, "50 Ways to Defeat Your PKI and Other Cryptosystems", The 50 Ways Series at all.net. (/journal/50/index.html)

F. Cohen, "50 Ways to Defeat Your Firewall", The 50 Ways Series at all.net. (/journal/50/index.html)

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Limits of Cryptography", Network Security, Nov., 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Security Education in the Information Age", Network Security, Oct., 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - In Your Face Information Warfare", Network Security, Sep., 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - What's Happening Out There", Network Security, Aug., 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Attack and Defense Strategies", Network Security, July, 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Limits of Awareness", Network Security, June, 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Watching the World ", Network Security, May, 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Simulating Network Security ", Network Security, Apr., 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Millisecond Fantasy", Network Security, Mar., 1999.

F. Cohen, Eli Dart "DARE: Distributed Analysis and REsponse", SANS conference, San Diego, 1999.

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Returning Fire", Network Security, Feb., 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Anatomy of a Successful Sophisticated Attack", Network Security, Jan., 1999.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Balancing Risk", Network Security, Dec., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Real Y2K Issue?", Network Security, Nov., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Time-Based Security?", Network Security, Oct., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - What Should I Report to Whom?", Network Security, Sep., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Third Anniversary Article - The Seedy Side of Security", Network Security, Aug., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - How Does a Typical IT Audit Work?", Network Security, Jul., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Technical Protection for the Joint Venture", Network Security, Jun., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Risk Staging", Network Security, May., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Unpredictability Defense", Network Security, Apr., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Red Teaming", Network Security, Mar., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Management of Fear", Network Security, Feb., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Y2K - Alternative Solutions", Network Security, Jan., 1998.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - 50 Ways to Defeat Your Intrusion Detection System", Network Security, Dec., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - To Outsource or Not to Outsource - That is the Question.", Network Security, Nov., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - The Network Security Game", Network Security, Oct., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Change Your Password - Doe See Doe", Network Security, Sep., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Penetration Testing?", Network Security, Aug., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Relativistic Risk Analysis", Network Security, Jun., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Prevent, Detect, and React", Network Security, May., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Would you like to play a game?", Network Security, Apr., 1997.

F. Cohen, "Protection Issues in ASCII Red Based on a Limited Unclassified Briefing" (C).

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Risk Management or Risk Analysis?", Network Security, Mar., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Network Security as a Control Issue?", Network Security, Feb., 1997.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Integrity First - Usually", Network Security, Jan., 1997.

F. Cohen, S. Cooper, et. al. "Intrusion Detection and Response", National InfoSec Technical Baseline, October, 1996. (Also appearing in SecureNet 97, March, 1997 and Computers and Security as cited above)

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Where Should We Concentrate Protection?", Network Security, Dec., 1996.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - How Good Do You Have to Be?", Network Security, Nov., 1996.

F. Cohen, "Managing Network Security" (series of articles in Network Security Magazine) - Why Bother?", Network Security, Oct., 1996.

F. Cohen, "Internet Holes - The SYN Flood", Network Security, Sep., 1996.

F. Cohen, "Internet Holes - Internet Incident Response", Network Security, Aug., 1996.

F. Cohen, "Internet Holes - Internet Lightning Rods", Network Security, July, 1996.

F. Cohen, "Internet Holes - UDP Viruses", Network Security, June, 1996.

F. Cohen, "Internet Holes - Eliminating IP Address Forgery", Network Security, May, 1996.

F. Cohen, "Internet Holes - Spam", Network Security, April , 1996.

F. Cohen, "Internet Holes - The Human Element", Network Security, March, 1996.

F. Cohen, "Internet Holes - Automated Attack and Defense", Network Security, February, 1996.

F. Cohen, "Internet Holes - 50 Ways to Attack Your World Wide Web Systems", Network Security, December, 1995 - January, 1996.

F. Cohen, "Internet Holes - Network News Transfer Protocol ", Network Security, November, 1995.

F. Cohen, "Internet Holes - Sendmail Attacks", Network Security, October, 1995.

F. Cohen, "Internet Holes - Packet Fragmentation Attacks", Network Security, September, 1995.

F. Cohen, "Internet Holes - Internet Control Message Protocol", Network Security, August, 1995.

F. Cohen, "Airbag Inflator Inspection System", LumenX Corporation, November, 1994.

F. Cohen, R. Knecht, C. Preston, et. al., "Planning Considerations for Defensive Information Warfare - Information Assurance", Contract DCA 100-90-C-0058 T.O. 90-SAIC-019, November, 1993.

F. Cohen, "Threats and Defenses for WCCS", US Air Force, Wing Command and Control System, August, 1993.

F. Cohen, "Information Warfare Considerations", National Academy of Sciences - National Research Council, September, 1993.

F. Cohen, "A Case for Benevolent Viruses" DPMA, IEEE, ACM Computer Virus and Security Conference, March 1992

F. Cohen, "Current Best Practice Against Computer Viruses with Examples from the DOS Operating System", DPMA, IEEE, ACM Computer Virus and Security Conference, March 1992

F. Cohen, "A Roving Emulator", Conference on Modeling and Simulation, April, 1987.

F. Cohen, "Information Protection", Curriculum Module for the graduate degree in Software Engineering, The Software Engineering Institute, June, 1986, also appearing in ACM SIGSAC in abbreviated form.

F. Cohen, "A Complexity Based Integrity Maintenance Mechanism", Conference on Information Sciences and Systems, Princeton University, March 1986.

F. Cohen, "Recent Results in Computer Viruses", Conference on Information Sciences and Systems, Johns Hopkins University, March 1985.

F. Cohen, "The HAD Cryptosystem", IACR Crypto84 rump session, Aug. 1984.

F. Cohen, "Computer Security Methods and Systems", Conference on Information Sciences and Systems, Princeton University, March 1984.

F. Cohen, "Learning Networks for Database Access", Yale Conference on Adaptive Systems Theory, New Haven, CT, June, 1983.

M.A. Breuer, F. Cohen, and A.A. Ismaeel, "Roving Emulation", Built-In Self-Test Conference, March 1983.

F. Cohen, "The Delta-Net Model of Computation", Conference on Information Sciences and Systems, Johns Hopkins University, March 1983.

F. Cohen, "The U.S.C. Roving Emulator", U.S.C. DISC Report #82-8, Dept of Electrical Engineering, University Park, LA, Ca. 90089-0781, Dec. 1982.

M.A. Breuer, F. Cohen, A.A. Ismaeel, "Roving Emulation as Applied to a

(255,223) RS-encoder System", U.S.C. DISC Report #82-6, Dec. 1982.

Software Products Developed:

F. Cohen - JDM, 2006
F. Cohen – Security Decisions, 2006
F. Cohen – Surveyor, 2006
F. Cohen - Influence, 2006
F. Cohen and Garrett Gee, 2002 - White Glove Bootable Linux CD
F. Cohen, 2002 - Responder - large-scale network deception system
F. Cohen and Garrett Gee, 2002 - White Glove developer platform
F. Cohen, Darrian Hale, et. al., 2002 - Resilience - Resilient network infrastructure
F. Cohen, Anthony Carathemus, et. al. 2001 - Secure DNS Server
F. Cohen, Anthony Carathemus, et. al. 2001 - Partition Dump
F. Cohen, Eric Thomas, and Anthony Carathemus, 2001 - Invisible Router
F. Cohen, 2000 - D-Wall - Large-scale high fidelity deception system
F. Cohen, 1999 - Network Security Simulator
F. Cohen and E. Dart, 1998 - DARE - Distributed Analysis and Defense
F. Cohen, 1998 - Deception Toolkit
F. Cohen, 1998 - The Security Maze
F. Cohen, 1997 - The Cracking Game
F. Cohen, 1997 - Automated Threat, Attack, and Defense Analysis Tool
F. Cohen, 1996 - CID Database Analysis Tool
F. Cohen, 1995 - Auditor - Internal Audit Tool
F. Cohen, 1995 - Analyzer - Network Audit Tool
F. Cohen, 1995 - Trivial HTTP Daemon - provably secure web server
F. Cohen, 1995 - Secure Gopher Server - provably secure gopher server
F. Cohen, 1993 - Calendar Supplement
F. Cohen, 1992 - PayBack Automated Bill Collection Software
F. Cohen, 1989 - Integrity ToolKit - Integrity Shell and Access Control System
F. Cohen, 1988 - Advanced Software Protection Scanner - Virus Scanner
F. Cohen, 1987 - Advanced Software Protection - Crypto-Checksum Integrity Checker
F. Cohen, 1987 - TRP - Small business office software
F. Cohen, 1986 - VCE - Viral Computing Environment
F. Cohen, 1985 - Legal Assistant - Law Office Software

Additional background

When I was young, I was interested in information technology. At an early age I built a mechanical computer. In grade school I used computers and knew other children who were interested in computers. I spent a fair amount of time with them learning about how things worked at a place called Project Solo at the

University of Pittsburgh, where I was not a member of the project, but rather a friend to many who were. I learned the language PIL (Pitt Interpretive Language) in grade school, programmed computers for my father's laboratory at the University of Pittsburgh, and as a Boy Scout, ended up joining my older brother's explorer troop at Carnegie Mellon University where I used the IBM 360 programming in Lisp and APL. In high school I programmed computers and helped others who used the PDP 8 computers that were available at that time. This ultimately included helping to teach a teacher there how to use the computer for classes.

When I went to college at Carnegie-Mellon University, I fell in love with electrical engineering and started to develop hardware and software for computers. I worked as a computer operator at Carnegie-Mellon in the early days of the ARPAnet where I worked night shifts, eventually working on research projects including the design and simulation of protocols for military packet switching networks and as a librarian for the Hearsay speech understanding project while I went to school. I graduated in 1977 with a B.S. in Electrical Engineering.

I took a job at Collins Radio installing microwave communications equipment, then joined RCA, where I designed a system to detect telecommunications equipment communicating over a wide range of frequencies. Soon thereafter, I started independent consulting. I became coordinator of computer services for Carnegie-Mellon University's Engineering School, and later for Chatham College, and in 1980 went to the University of Pittsburgh, where I got my Masters of Science in Information Science (summa cum laude) with my thesis topic on robotics. Soon after that, I went to the University of Southern California to pursue a Ph.D. in Electrical Engineering, with emphasis on Computer Engineering.

While at the University of Southern California, I earned enough to pay for my education by doing consulting for Xerox on their D-machines, and later by working for the Electrical Engineering Department operating and helping to manage and maintain their computer systems, which were connected to the other computers of the world over the ARPAnet. This includes all manner of systems administration tasks. I also got a research assistantship working on design automation systems and testing of computer hardware. As I finished my courses, I started working on a dissertation on parallel processing, which included classes in computer security and cryptography.

At that time, I came across an idea one day in class, and soon thereafter coined the term "computer virus" and wrote the first scientific peer reviewed papers on that subject ever published. I built special purpose test viruses to determine their potential for harm, and built special purpose audit and analysis mechanisms to allow me to detect the presence of these viruses on systems and do analysis to predict where and how quickly viruses would spread in such systems. This included building custom audit mechanisms to instrument computer systems,

which I did in order to make predictions using computers at other institutions. I eventually completed my Ph.D. dissertation, which was titled "Computer Viruses" and continued to do research in this and related fields thereafter.

For the next 5 years or so, this dominated much of my time and effort as I created any number of different defenses against viruses, including but not limited to most of the ones in widespread use today. This included the first virus scanner, the first integrity shell, which is the precursor of today's Trusted Computing Group's Trusted Platform Module, which is embedded in the hardware of millions of computer systems as part of their manufacturing process, operating system protection mechanisms, high surety network protection mechanisms, digital diodes, detection mechanisms, and a wide range of other related technologies.

Before graduation, I started working at Lehigh University as an instructor, which became an assistant professor position upon my graduation in 1986. Soon thereafter I moved to the University of Cincinnati as an assistant professor, and within a year after that, I became the President of "The Radon Project", a technical measurement company that operated largely by mail order doing measurements of radon gas in homes, tests of water for a wide range of contaminants, and paint for lead. This business had a large mail order and retail component and grew from 12 employees to 250 employees over the first year that I operated it. As CEO of this small to medium-sized business, I had the ultimate day-to-day decision-making authority, subject to board decisions that were quite often made in the start-up process. Because of the small size, I was also in charge of information technology and implemented most of the controls in place for quite some time. I had essentially all of the risk management responsibility and also architected the information environment, wrote much of the initial code that did calculations, and did lots of other things. For example, I helped design and build the heat pipes that kept a substantial quantity of toluene at the proper temperature to prevent its spontaneous combustion. Availability loss of this system for too long could potentially result in total business loss along with the destruction of a substantial building with people in it.

At the same time, I was doing consulting around the world in computer security, teaching short courses on computer viruses on several continents, writing articles, speaking at conferences, and doing research and development in information protection and related areas.

In the late 1980s and early 1990s I worked on a consulting basis for corporations of all sizes, and as a contractor, for elements of the US Department of Defense and other government agencies, including, without limit, the National Security Agency, the Defense Information Systems Agency, several global financial institutions, large telecommunications companies, manufacturers of different sorts, global oil and gas companies, and microelectronics manufacturers, on

various issues related to information protection. As part of my work in that time frame, I was granted a US Government Security Clearance, which I retain to this day. I also wrote and had several books published including, "Protection and Security on the Information Superhighway", "A Short Course on Computer Viruses", and "It's Alive!!!". Some of my work led directly to efforts related to the President's Commission on Critical Infrastructure Protection, and first defined the term "Information Assurance" as it continues to be used today. In 1989, I won the "Information Technology Prize" awarded by the Chartered Accountants of England and Wales for my work on the development of integrity mechanisms for computer systems.

In the middle 1990s I also started doing Internet-related investigations, including tracking down the first large-scale distributed coordinated attack over a network, working on a legal matter involving intellectual property theft, working on a matter involving an accusation of computer attack, and ultimately supporting private concerns, government agencies, and law enforcement in network-related attack cases. In that time frame I also started to do research into Internet protocol problems and how they could lead to vulnerabilities, published peer reviewed papers on the limits of digital forensics and attackers for detecting and bypassing detection of activities in computers, log analysis, and related subjects.

In the late 1990s, I joined Sandia National Laboratories, a Federally Funded Research and Development Corporation, while, under contractual agreement, I was permitted to continue to do outside consulting where no conflict of interest was present. As a consultant to and researcher for the U.S. government I was the principal investigator on seminal studies in defensive information operations, I was the principal investigator on the national information security technical baseline series of reports, which included a detailed report on the state of the art and the limitations of the art in intrusion detection and response, founded the College Cyber Defenders program that ultimately led to the formation of the CyberCorps program, and led projects ranging from 'Resilience', a network computing mechanism to allow functions to continue even when computers fails, to 'The Invisible Router', which is now used, among other things, to protect US Department of Defense networks. I also led the first substantial scientific experiments on the use of deception for information protection, and was eventually granted several patents for the methods and apparatus used in these experiments.

I also worked in critical infrastructure protection supporting the pre year-2000 studies of the vulnerabilities of critical infrastructures, advised the State Department and elements of the Department of Defense on related issues, worked on studies of weaknesses in power, water, gas, oil, financial, and other critical infrastructures and how to mitigate those weaknesses, and developed tools and techniques used to protect systems ranging from classified networks to

the Internet. During this period I also participated in various strategic exercises and studies related to information warfare, participated in other related strategic decision support groups, and was, in one instance, authorized to present the overall results of analysis of the potential effects of the Year 2000 computer system issue on US nuclear weapons to a DoD meeting related to these issues.

During my tenure at Sandia National Laboratories I also worked with law enforcement and the intelligence community to help improve their ability to deal with computer related crime and emerging threats to national security. This included testifying before congress on how to better protect critical infrastructures, and in particular, the Internet, developing law enforcement tools for digital forensic analysis, holding law enforcement training sessions to train their trainers on issues related to digital forensic and computer-related crime investigations, educational programs taught at the Federal Law Enforcement Training Center and elsewhere in digital forensics, network investigations, and related issues, becoming a member of the New York Electronic Crimes Task Force, which was run by the US Secret Service, assisting in the development of standards for electronic evidence identification, collection, preservation, and transport, testimony in federal and state criminal and civil matters, and pro bono and state-funded work for indigent defendants. In 2002, I won the "Techno-Security Industry Professional of the Year" Award for my work in digital forensics and efforts to work with law enforcement in this area. I also won a variety of awards for my work at Sandia National Laboratories.

In this same time frame I started to work as a "Practitioner in Residence" and eventually became a "Research Professor" for the University of New Haven. In this role, developed graduate curricula and taught graduate classes in the national security programs, including classes in information protection, threats, attacks, and defenses, computer-related frauds, network investigations, network forensics, computer forensics, cyber terrorism, cryptography, computer and network security, and related areas. I also worked there on Federally funded research efforts related to network intelligence and the use of computer networks by substate actors. In this same time frame, I also developed bootable CD-ROM Linux-based operating environments, including one for digital forensic examination, and which was and still is used by law enforcement, Federal agencies, and others for investigations and related purposes. These disks were also used for University classes to allow students to temporarily convert their home computers into forensics workstations for classes, and return them unaltered to their normal use the rest of the time. In this time frame I also developed other digital forensics tools, including the ForensiX software program that automated many of the previously manual operations that many investigators were using while tracking all activities and creating definitive logs of those activities for later verification.

USCF's Expert Witness Disclosure of Dr. Frederick B. Cohen

When the University of New Haven opened a campus at Sandia National Laboratories, I transitioned from Sandia to the University, and soon thereafter also started working for Burton Group, an industry research and analysis firm focused on enterprise information infrastructure. At Burton Group, I was the Principal Analyst for Security and Risk Management Strategies, and in my tenure there, I worked with large enterprise customers from all over the world, doing a wide range of consulting and using teleconference-based meetings for dealing with shorter issues. As part of this work, I authored a series of peer reviewed papers related to information protection, and ultimately, on an independent basis, wrote a series of books on the subject in my waning days there. During that period I also did research on other related subjects, continued to work on legal cases for select clients, worked for government clients on special projects through third party vendors, and continued with the University of New Haven.

After leaving the full time employ of Burton Group, where I continue to do consulting and speak at their conferences, the University of New Haven decided to refocus on liberal arts and on their central campus in Connecticut. My contract with them terminated in 2008, and while I still taught a few courses at other universities in related areas, I worked with the now retired dean who ran the programs I worked in, and the university president, who left his position in the same time frame, to form California Sciences Institute (CalSci). CalSci is a graduate non-profit educational and research institution which will soon teach graduate programs leading to M.S. degrees in National Security and Advanced Investigation and Ph.D. degrees in National Security and Digital Forensics.

In 2009, I was named the "most famous hacker" of all time by ABC news, although they associated my work with some of the more infamous computer attackers, and failed to notice the difference between my work to help secure systems and track down those who would harm others through them, and people who get arrested for computer crimes.

All told, I have authored more than 200 invited, refereed, and other peer reviewed articles, wrote a monthly column for Network Security magazine on managing network security for 6 years, and have written several widely read books on information protection.

My most recent books have focused on "Enterprise Information Protection Architecture", "Challenges to Digital Forensic Evidence", and "Digital Forensic Evidence Examination". I have also contributed chapters to books in this area, including a chapter in "Forensic Computer Crime Investigation". I participated in the creation of "Electronic Crime Scene Investigation - A Guide for First Responders, NIJ Guide" (NIJ Guide 187736), wrote a soon to be published encyclopedia article on digital forensics, and wrote and continue to write articles for peer reviewed conferences and workshops on digital forensics and related topics.