

Munshani v. Signal Lake Venture Fund II, et al.,  
Sup. Ct. No. 00-5529 BLS


Report of Kenneth Shear

**ELECTRONIC EVIDENCE DISCOVERY, INC.**  
**Litigation Services Memorandum**

**To: Hon. Allan van Gestel**  
**And to: Michael Walsh of Greisinger, Walsh & Maffei**  
**And to: Robert Lovett of Testa, Hurwitz & Thibault**  
**And to: Robert A. Skinner and Joan McPhee of Ropes & Gray**  
**From: Kenneth Shear, EED**  
**Re: Munshani v. Signal Lake Venture Fund II, et al.,**  
**Sup. Ct. No. 00-5529 BLS**  
**Date: September 12, 2001**

Enclosed is my report in this matter, which is being sent via FedEx to the parties and the Court. The report with exhibits totals 147 pages.

Dated September 12, 2001.

  
\_\_\_\_\_  
Kenneth Shear

**ELECTRONIC EVIDENCE DISCOVERY, INC.**  
**Litigation Services Memorandum**

**To:** Hon. Allan van Gestel  
**And to:** Michael Walsh of Greisinger, Walsh & Maffei  
**And:** Robert Lovett of Testa, Hurwitz & Thibault  
**And:** Robert A. Skinner and Joan McPhee of Ropes & Gray  
**From:** Kenneth Shear, EED  
**Re:** Munshani v. Signal Lake Venture Fund II, et al.,  
Sup. Ct. No. 00-5529 BLS  
**Date:** September 12, 2001

**Report**

**I. Question Posed:**

Whether the authenticity of an email produced by Suni Munshani in this matter, dated August 3, 2000, subject "Warrants", can be ascertained with a reasonable degree of technical certainty. If so, whether or not in my opinion the message is authentic, and the detailed grounds for that opinion.

**II. Evidence Examined:**

I, and EED technicians working under my supervision, have examined the following items:

Data Collection Date	Description of Source	Description of Process for Data Collection
3/28/2001	Munshani Thinkpad Laptop #1 Internal Hard Disk Drive	Image copy Taken by EED Technician using SafeBack Software
3/28/2001	Munshani Thinkpad Laptop #2 Internal Hard Disk Drive	Image copy Taken by EED Technician using SafeBack Software
6/7/2001	Munshani Server (Generic PC) Internal Hard Disk Drive	Image copy Taken by EED Technician using SafeBack Software
5/23/2001	Munshani External SCSI drive	Image copy Taken by EED Technician using SafeBack Software
2/24/2000	Munshani Travan Tape 1 (backup of Laptop)	Backup by Unknown Person of Munshani Laptop

2/13/2000	Munshani Travan Tape 2 (backup of Laptop)	Backup by Unknown Person of Munshani Laptop
8/27/2001	Munshani NEXT Computer Hard Drive	Image copy Taken by EED Technician using SafeBack Software
6/15/2001	Glattig Dell Precision PC 1, Internal Hard Disk Drive A	Image copy Taken by EED Technician using SafeBack Software
6/15/2001	Glattig Dell Precision PC 1, Internal Hard Disk Drive B	Image copy Taken by EED Technician using SafeBack Software
6/15/2001	Glattig Dell Precision PC 2, Internal Hard Disk Drive A	Image copy Taken by EED Technician using SafeBack Software
6/15/2001	Glattig Dell Precision PC 2, Internal Hard Disk Drive B	Image copy Taken by EED Technician using SafeBack Software
6/15/2001	Glattig Dell Precision PC 2, Internal Hard Disk Drive C	Image copy Taken by EED Technician using SafeBack Software
6/15/2001	Glattig Dell XPS Internal Hard Disk Drive A	Image copy Taken by EED Technician using SafeBack Software
6/15/2001	Glattig Dell XPS Internal Hard Disk Drive B	Image copy Taken by EED Technician using SafeBack Software
6/19/2001	Glattig Gateway PC	Image copy Taken by EED Technician using SafeBack Software
8/4/2000	Terago Server (Including mail.terago.com and webmail.terago.com email servers)	Backup by Terago Communications Inc. Information Systems using NetBackup Software
2/2/2001	Trivedi Inspiron Laptop Internal Hard Disk Drive	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
5/18/2001	Trivedi Inspiron Laptop Internal Hard Disk Drive	Image copy Taken by EED Technician using SafeBack Software
2/2/2001	Trivedi Toshiba Laptop Internal Hard Disk Drive	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
5/18/2001	Trivedi Toshiba Laptop Internal Hard Disk Drive	Image copy Taken by EED Technician using SafeBack Software
2/2/2001	Trivedi Dell Dimension Home PC, Internal Hard Disk Drive A	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
5/18/2001	Trivedi Dell Dimension Home PC, Internal Hard Disk Drive A	Image copy Taken by EED Technician using SafeBack Software
2/2/2001	Trivedi Dell Dimension Home PC, Internal Hard Disk Drive B	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
5/18/2001	Trivedi Dell Dimension Home PC, Internal Hard Disk Drive B	Image copy Taken by EED Technician using SafeBack Software
2/2/2001	Trivedi Generic Desktop Home PC, Internal Hard Disk Drive A	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
5/18/2001	Trivedi Generic Desktop Home PC, Internal Hard Disk Drive A	Image copy Taken by EED Technician using SafeBack Software

2/2/2001	Trivedi Generic Desktop Home PC, Internal Hard Disk Drive B	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
5/18/2001	Trivedi Generic Desktop Home PC, Internal Hard Disk Drive B	Image copy Taken by EED Technician using SafeBack Software
2/2/2001	Trivedi Generic Desktop Home PC, Internal Hard Disk Drive C	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
5/18/2001	Trivedi Generic Desktop Home PC, Internal Hard Disk Drive C	Image copy Taken by EED Technician using SafeBack Software
2/12/2001	Stuck Desktop Computer Internal Hard Disk Drive	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
2/10/2001	Weingarten Desktop Internal Hard Disk Drive	Image copy Taken by Deloitte & Touche Technicians using EnCase Software
2/10/2001	Weingarten Laptop Internal Hard Disk Drive	Image copy Taken by Deloitte & Touche Technicians using EnCase Software

Detailed findings with respect to these items are set forth in the Opinion and Basis for Opinion sections, below.

### III. Opinion:

The questioned message is allegedly from Hermant Trivedi to Suni Munshani, dated August 3, 2000, subject "Warrants." In my opinion, the questioned message is clearly not authentic, based upon the following:

1. Evidence that the message header was copied from a second message
2. Inconsistency between the message ID and the message time in the questioned message.
3. Inconsistency between the sent and received dates shown on the questioned message and the create and last modified dates of the message in the Outlook message file on Mr. Munshani's computer.
4. Absence of any record of transmission of the questioned message in the Terago Communications Corp. email server logs.

5. Absence of any record on Mr. Trivedi's computers and other computers provided by counsel for Mr. Trivedi that the message was sent.

#### **IV. Basis for Opinion:**

The questioned message is found on Mr. Munshani's laptop computer stored by the Microsoft Outlook 2000 email program in a "personal folders" file (also known as a ".PST" file). Microsoft Outlook is a standard email client program. Email systems typically require two kinds of programs: email clients and email servers.<sup>1</sup> The end-user of the system (i.e., the individual creating, sending, receiving and reading messages) normally uses the email client program to create, send, receive, open, store and otherwise deal with messages, attachments, and other email items. In this case, the Microsoft Outlook 2000 email program was configured to save sent and received messages on the hard drive of Mr. Munshani's laptop.

Once a message has been written and sent from an email client, it is transmitted to an email server on which the end-user has an account or mailbox. The email server (sometimes referred to as an email post office) is a program whose function is to share email messages between various users and store messages for end users with mailboxes or accounts on the server. When the message is sent over the Internet it will be transmitted from the server where the sender's account is found and received by a server

---

<sup>1</sup> What is referred to as an "email server" in the text of this report is also sometimes referred to as a mail transfer agent or MTA. There are several types of mail transfer agents, but the distinctions are not germane to this report. What is referred to as an "email client" in the context of this report may also be referred to as a mail user agent or MUA.

on which the recipient's account is found. In many instances, the message will be transmitted through intermediate servers.

We were provided with two laptop computers by counsel for Mr. Munshani in connection with this matter. One of the laptops (the working laptop) was described by his counsel as the one used by Mr. Munshani to receive the questioned message. The other laptop (the evidentiary laptop) was described by his counsel as having been used by Mr. Munshani to provide a copy of material relevant to this matter to counsel. The questioned message is found on Mr. Munshani's working laptop in a file, called "OUTLOOK.PST", a standard Microsoft Outlook personal folders file. As set forth above, I have concluded that the questioned message is clearly inauthentic. The observations on which I base my opinion are as follows:

a. The Record of Transmission of the Questioned Message over the Internet

The questioned message states that it is from Hermant Trivedi, dated August 3, 2000. Another message (hereafter referred to as the "comparator message") from Mr. Trivedi, also dated August 3, 2000, is found in Mr. Munshani's email. It is apparent that the questioned message was created in part by copying the comparator message after it was received in Mr. Munshani's account.

Messages sent over the Internet consist of a header and message body. The Internet message body contains the text of the message and the content of any attachments. The Internet message header contains information about the addressing and transmission of the message, including sender, recipient, subject line, various dates and times (including times of sending, receipt and transmission), information about the email servers through

which the message passed in moving over the Internet from sender to recipient, and several types of message ID codes.

The Internet message headers from the questioned message and comparator message are as follows:

**Questioned Message**

**Return-Path: hemant\_trivedi@terago.com**  
**Received: from mail.terago.com (mail.terago.com [208.141.104.1])**  
**by hedgefund.ushedgefund.com (8.11.0/8.11.0) with ESMTTP id**  
**e73MfZ331592**  
**for <sun@ushedgefund.com>; Thu, 3 Aug 2000 15:45:31 -0400 (EDT)**  
**Received: from webmail.terago.com (webmail.terago.com [10.0.1.8])**  
**by mail.terago.com (Switch-2.0.1/Switch-2.0.1) with ESMTTP id**  
**e73MfW903843;**  
**Thu, 3 Aug 2000 14:41:32 -0500 (CDT)**  
**Received: from terago.com (ostrich.terago.com [10.0.20.18])**  
**by webmail.terago.com (8.8.8+Sun/8.8.8) with ESMTTP id RAA01318;**  
**Thu, 3 Aug 2000 14:41:31 -0500 (CDT)**  
**Message-ID: <3989e793.87BDEEE2@terago.com>**  
**Date: Thu, 03 Aug 2000 14:43:47 -0500**  
**From: Hemant Trivedi <hemant\_trivedi@terago.com>**  
**Reply-To: hemant@terago.com**  
**Organization: Terago Communications, Inc**  
**X-Mailer: Mozilla 4.73 [en] (Windows NT 5.0; U)**  
**X-Accept-Language: en**  
**MIME-Version: 1.0**  
**To: suni@ushedgefund.com**  
**Subject: Warrants**  
**Status:**

**Comparator Message**

**Return-Path: hemant\_trivedi@terago.com**  
**Received: from mail.terago.com (mail.terago.com [208.141.104.1])**  
**by hedgefund.ushedgefund.com (8.11.0/8.11.0) with ESMTTP id**  
**e73MfZ331592**  
**for <sun@ushedgefund.com>; Thu, 3 Aug 2000 18:41:35 -0400 (EDT)**  
**Received: from webmail.terago.com (webmail.terago.com [10.0.1.8])**

by mail.terago.com (Switch-2.0.1/Switch-2.0.1) with ESMTP id  
e73MfW903843;  
Thu, 3 Aug 2000 17:41:32 -0500 (CDT)  
Received: from terago.com (ostrich.terago.com [10.0.20.18])  
by webmail.terago.com (8.8.8+Sun/8.8.8) with ESMTP id RAA01318;  
Thu, 3 Aug 2000 17:41:31 -0500 (CDT)  
Message-ID: <3989F5A3.87BDEEE2@terago.com>  
Date: Thu, 03 Aug 2000 17:43:47 -0500  
From: Hemant Trivedi <hemant\_trivedi@terago.com>  
Reply-To: hemant@terago.com  
Organization: Terago Communications, Inc  
X-Mailer: Mozilla 4.73 [en] (Windows NT 5.0; U)  
X-Accept-Language: en  
MIME-Version: 1.0  
To: suni@ushedgefund.com  
Subject: Re: Suhas Patil discussions re: terago  
References:  
<NDBBLKJGGMFAFPIFJBIOEECNCLAA.suni@ushedgefund.com>  
Content-Type: multipart/alternative;  
boundary="-----E550E9EFC1FC59FBC471DB92"  
X-UIDL: d3e748a535a94a068dd90ae50ea23aa1  
Status: U

(Copies of the full message contents for the questioned message and comparator message are attached as Exhibit A and B to this report.) Of particular significance in this case are the "ESMTP ID's" of the messages. The initials ESMTP refer to Extended Simple Mail Transport Protocol. Email servers running this protocol are normally known by the abbreviated designation, "SMTP servers." When a message is transmitted through a series of such SMTP servers, each server assigns an "ESMTP ID" to the message. The function of this ESMTP ID is to permit the message to be tracked and logged on the SMTP server, and to fulfill these functions the ESMTP ID of each message passing through the server must be unique on the server. The ESMTP ID is automatically assigned to each message by the SMTP mail program without manual intervention.

The message headers from both the questioned message and the comparator message list the same sequence of email servers through which the messages purportedly traveled from Mr. Trivedi's computer to Mr. Munshani's computer. Each message indicates that it was transmitted through an email server called "mail.terago.com", to a second email server called "webmail.terago.com" and finally to a server called "hedgefund.ushedgefund.com". If both messages were authentic, each message would have a unique ESMTP id on each server. But for the two messages above, the ESMTP ids are the same for each of the three transmitting servers:

<b>hedgefund.ushedgefund.com</b>	<b>e73MfZ331592</b>
<b>mail.terago.com</b>	<b>e73MfW903843</b>
<b>webmail.terago.com</b>	<b>RAA01318</b>

The presence of identical message identifiers for three consecutive relay servers indicates that, to a virtual certainty, one of the two messages is inauthentic.

Although the ESMTP ids are identical for the two messages, the message headers show different times for the relay of each message through each server:

<b>Server:</b>	<b>ESMTP ID</b>	<b>Transmission Time</b>	
		<b><u>Questioned Msg</u></b>	<b><u>Comparator Msg</u></b>
<b>hedgefund.ushedgefund.com</b>	<b>e73MfZ331592</b>	<b>15:45:31 (EDT)</b>	<b>18:41:35 (EDT)</b>
<b>mail.terago.com</b>	<b>e73MfW903843</b>	<b>14:41:32 (CDT)</b>	<b>17:41:32 (CDT)</b>
<b>webmail.terago.com</b>	<b>RAA01318</b>	<b>14:41:31 (CDT)</b>	<b>17:41:31 (CDT)</b>

Comparison of the transmission time of the message and the ESMTP ID on the "webmail.terago.com" server demonstrates that the questioned message is inauthentic. This can be determined because the time of the message is encoded in the ESMTP ID by

the email server program used by the webmail.terago.com server on August 3, 2000 (version 8.8.8 of the Sendmail program). The time encoded in the ESMTP ID of the messages does not agree with the transmission time of the questioned message, but does agree with the transmission time of the comparator message. Therefore, it is clearly the comparator message which is the valid one.

Sendmail version 8.8.8 assigns each message an ESMTP ID with the first character of the ID reflecting the hour during which the message was received using military time, with the hour 0 represented by the letter A, hour 1 represented by B, and so forth, through hour 23 represented by the letter X. Therefore, on the webmail.terago.com server as of August 3, 2000, a message with an ESMTP ID beginning with the letter "R" must have been received during hour 17. This is the hour of receipt of the comparator message, demonstrating that the comparator message is valid. But the questioned message shows receipt on the webmail.terago.com server during hour 14 – inconsistent with the message's ESMTP ID. This discrepancy is a clear indication that the header of the questioned message is inauthentic, because the date and time setting reflected in the ESMTP ID and the date and time stamp from the same machine must agree on a valid message.

In gathering data for this report, I spoke with Dennis Glatting, the administrator of the hedgefund.ushedgefund.com email server. Mr. Glatting recalled having had problems with the hedgefund.ushedgefund.com servers at some time in the year 2000 affecting the processing of multiple email messages during an unspecified time period. Mr. Glatting further recalled that he might have addressed these problems by making adjustments in

message headers that were stored on the hedgefund.ushedgefund.com server. Mr. Glatting stated that he had no documentation of the problem or any steps taken to correct it. In order to determine whether the subject message was affected by some systematic manipulation of message headers, I have collected the Internet header information from other messages found in Mr. Munshani's mailbox during the time period two weeks before and two weeks after August 3, 2000. Other than the comparator message and questioned message, there are no other instances where messages are found in Mr. Munshani's Outlook file with duplicate ESMTP IDs, ESMTP IDs that do not agree with the associated transmission times, or any other anomalies similar to those seen in the header of the questioned message. Therefore, in my opinion, whatever activity Mr. Glatting was describing does not account for the spurious header in the questioned message. Exhibit C to this report is a listing of messages from Mr. Munshani's PST file received during the time period July 21, 2000 through August 17, 2000, where the ESMTP ID follows the format described above in which the first letter represents the hour of sending. I have omitted subject, sender, recipient, etc., in view of the Courts' request that I preserve privacy insofar as possible.

It is significant that the ESMTP IDs of the questioned message and comparator message are the same not only for the webmail.terago.com and mail.terago.com servers, but also for the hedgefund.ushedgefund.com server as well. The duplication of the hedgefund.ushedgefund.com ESMTP ID shows that copying of the comparator message occurred after the message had been received by the hedgefund.ushedgefund.com server. Therefore, in my opinion the message was not tampered with before it was received by

the hedgefund.ushedgefund.com server, which I understand to be owned by Mr.

Munshani.

b. Date and Time of the Questioned Message and Other Messages Stored by Microsoft Outlook on Mr. Munshani's Laptop

The Microsoft Outlook 2000 program was installed on Mr. Munshani's laptop computer and used to hold messages received by Mr. Munshani. The questioned message is found in a standard Microsoft Outlook 2000 message storage file called a Personal Folders file (also known as a .PST file) on Mr. Munshani's laptop. The PST file on Mr. Munshani's working laptop contains 4468 messages stored during the time period 2/9/2000 through 2/19/2001. The Outlook date of the questioned message, particularly in context of other message dates in Mr. Munshani's PST file, provides further support for the conclusion that the questioned message is not authentic.

When messages are created, sent, received or saved using the Outlook 2000 program, the program records a variety of message properties, such as message dates, subject, sender, recipient and various other items of information about the message. When the Outlook 2000 program is installed, messages are presented in a default view that shows only a few of these message properties. In this case, the Outlook Created date of the questioned message is important in my analysis, because it is not consistent with the received date.

It should be noted that the Outlook created date is not visible when Outlook 2000 is set up using the default configuration, and there is no indication that there even is such a date available. Rather, in the default configuration, the user only sees the message

received or sent date, depending on what folder is being viewed. To view the created date, a user of Outlook must reset the configuration of the program interface, using the “field chooser” or a view menu option. When Mr. Munshani’s laptop computer was inspected by EED, the Outlook Personal Folders file containing the questioned message was configured so that the Outlook create date and time were not visible. I viewed the Outlook create date and time by resetting the configuration.

1. Outlook Created Time of the Questioned Message and Comparator Message:

When a message is saved by Microsoft Outlook into a Personal Folders File (.PST file), Outlook records the date / time of this save action, labeling it the “create date”. There are several actions that can result in the message being saved into an Outlook file, including receipt of the message, sending or saving a message, making a second copy of it or importing it from some other format into a .PST file. In this case, the questioned message carries an Outlook create date of December 19, 2000 (time, 12:58 a.m., EST). This date is inconsistent with the message having been received in Mr. Munshani’s Outlook file on August 3, 2000. By contrast, the comparator message carries a creation date of 8/3/2000 10:08 p.m. EDT, which is consistent with the other message dates shown in the message header.

2. Outlook Modified Time of the Questioned Message and Comparator Message:

Microsoft Outlook also records a “modified” date / time of a message, which is the last time the message was saved into a PST file using the Outlook program. The modified date/time changes when the content of the message or a property of the message is changed. For example, if a previously unopened message is opened, or if a message is

forwarded, this may change the last modified date, although this depends to some degree upon the specific configuration of the Outlook client. In this case, the questioned message carries an Outlook last modified date and time of December 19, 2000 (time, 12:58 a.m., EDT). This time is exactly the same, to the second, as the Outlook created date and time. (See Exhibit A, reflecting the precise Outlook created date and time of the Questioned Message.) This would not be the case for a valid Outlook message, unless the message had never been opened. By contrast, the comparator message carries a last modified date of 8/3/2000 10:18 p.m., which is consistent with the other message dates shown in the message header, and is about 10 minutes after the created date of the message, a pattern that would be expected if a message were opened shortly after it was downloaded into the Outlook account. (See Exhibit B, reflecting the precise Outlook last modified date and time of the Comparator Message.)

### 3. Message Creation Times in Mr. Munshani's Personal Folders File:

The Personal Folders file on Mr. Munshani's laptop holding the questioned message was first used on February 9, 2000. On February 9 and 11, 2000, 485 messages appear to have been imported into the file. This can be seen because, when a message is imported into Outlook from another type of message store, the created date of the message is set by Outlook to the time of the import. In Mr. Munshani's Outlook file there are a large number of messages with identical or near-identical creation times on 2/9/00 and 2/11/00, but earlier sent and received times. When a new Personal Folders file is set up and messages imported, it normally results in Outlook creation times (which reflect the date and time when the messages have been imported into the Personal Folders file) that are

subsequent to the message sent or received times (which reflect the date and time when the message was originally sent or received.) This is so in the Personal Folders file seen on Mr. Munshani's laptop.

Subsequent to the import of messages February 11, 2000, except for the questioned message, all of the other messages in the subject personal folders file from Mr. Munshani's laptop are consistent with a normal pattern of usage of Outlook, as follows:

(a) Most of the messages display a Creation Date that is the same or one day later than the Received date. (Discrepancies of one day would occur if, for example, the message were received on the server holding Mr. Munshani's account on one day and downloaded to his Outlook Personal Folders file on the next day.)

(b) If the computer were not used to send or receive email for a period of inactivity, it is expected that no messages would be created in the Personal Folders file by the Outlook 2000 client during that period, and then a backlog of messages from previous days would be created at the end of the period of inactivity. For example, if the Outlook program were not used for a week, one would expect to see a series of messages with received times during that week, but no created times during that week. Then, if the Outlook program were used again, one would expect to see the group of messages downloaded at the same or very nearly the same time. This pattern is also seen for a variety of time periods ranging from two to eight days.

(c) There is evidence of a date malfunction involving the hedgefund.ushedgefund.com email server and/or Mr. Munshani's laptop. The seven messages with an Outlook Creation Date of 6/21/2000 between 2:56 p.m. and 4:14

p.m. have a received date that is 12 days and 3 hours previous to the Creation Date. It should be noted that the Outlook Creation date is generated by the system time of Mr. Munshani's laptop computer, while the received date of a message is generated by the system time of a different computer (the email server where Mr. Munshani's email account is found). A discrepancy of this kind would be expected if the system times of the two computers were out of synchronization for a few hours.

The only message in the Personal Folders file on Mr. Munshani's laptop not fitting<sup>2</sup> the above patterns is the questioned message, which carries an Outlook Creation date that is 135 days subsequent to the sent and received dates found in the message header. No other message among the 4468 found in Mr. Munshani's Personal Folders file has a similar date discrepancy. A discrepancy of this magnitude is further indication that the message is not authentic and was created after the alleged send and received dates. A listing of the message dates for the items in Mr. Munshani's PST created after February 11, 2000, is attached as Exhibit D to this report. I have omitted subject, sender, recipient, etc., in view of the Courts' request that I preserve privacy insofar as possible.

c. Logs of Messaging Activity on the "mail.terago.com" and "webmail.terago.com"

Servers

The header of the questioned message reflects that it was transmitted by two servers owned by Terago Communications, Inc., called "mail.terago.com" and "webmail.terago.com". I obtained backups of these servers from Terago through

---

<sup>2</sup> Only seven of the messages in Mr. Munshani's main PST have this type of discrepancy between the laptop and server dates. There are no indications of a similar discrepancy for other messages in the PST.

counsel. EED technicians restored the data from the backup tapes. I inspected the tapes themselves and the listings of the restored data, and determined that the tapes were properly labeled and the contents were consistent with a backup done in the ordinary course of business on August 4, 2000. There are no date discrepancies or any other indications of any tampering whatsoever. In my opinion the tape received by EED from Terago is an authentic backup of the Terago Communications Inc. server that contains logs of its email systems.

Under my supervision, EED technicians examined the restored data from the webmail.terago.com and mail.terago.com servers. Logs for both of these servers were found. We located a system log ("syslog") dated August 3, 2000, for both of these servers. The system log records the ESMTP ID (and sometimes additional information) for messages sent and received by the server.

The system log for the webmail.terago.com email server contains the following entry:

```
Aug 3 17:41:32 webmail sendmail[1318]: RAA01318:  
from=<hemant_trivedi@terago.com>, size=4746, class=0, pri=124746, nrcpts=4,  
msgid=<3989F5A3.87BDEEE2@terago.com>, proto=ESMTP,  
relay=ostrich.terago.com [10.0.20.18]  
Aug 3 17:41:32 webmail sendmail[1320]: RAA01318:  
to=<scott_sarkinen@signallake.com>,<barts@signallake.com>,<mikew@signall  
ake.com>,<suni@ushedfund.com>, delay=00:00:01, xdelay=00:00:00,  
mailer=relay, relay=mail.terago.com. [10.0.1.6], stat=Sent (2.0.0 e73MfW903843  
Message accepted for delivery)  
Aug 3 17:42:15 webmail ipop3d[1321]: port 110 service init from 10.0.20.25  
Aug 3 17:42:15 webmail ipop3d[1321]
```

This log entry clearly reflects the transmission of the comparator message, as can be seen from the message ID (3989F5A3.87BDEEE2@terago.com) and the transmission time. The message ID, which is reflected in the header of the comparator message set

forth in part (a) above, is a code that uniquely identifies the message on the entire Internet.

Likewise, log entries are found in the mail.terago.com system logs that reflect the transmission of the comparator message on that system. The log entries are as follows:

```
error: safesasl(/opt/sendmail/smmta-8.10.0/lib/sasl/libplain.so) failed: Group
writable directory
Aug 3 17:41:32 mail sendmail[3843]: e73MfW903843:
from=<hemant_trivedi@terago.com>, size=4909, class=0, nrcpts=4,
msgid=<3989F5A3.87BDEEE2@terago.com>, proto=ESMTP, daemon=MTA,
relay=webmail.terago.com [10.0.1.8]
Aug 3 17:41:33 mail sendmail[3845]: e73MfW903843:
to=<scott_sarkinen@signallake.com>, delay=00:00:01, xdelay=00:00:01,
mailer=esmtpl, pri=214909, relay=zealous.cnchost.com. [207.155.252.26],
dsn=5.1.1, stat=User unknown
Aug 3 17:41:34 mail sendmail[3845]: e73MfW903843:
to=<mikew@signallake.com>,<barts@signallake.com>, delay=00:00:02,
xdelay=00:00:02, mailer=esmtpl, pri=214909, relay=zealous.cnchost.com.
[207.155.252.26], dsn=2.0.0, stat=Sent (SAA06694 Message accepted for delivery)
Aug 3 17:41:35 mail sendmail[3845]: e73MfW903843:
to=<suni@ushedgefund.com>, delay=00:00:03, xdelay=00:00:01, mailer=esmtpl,
pri=214909, relay=cv365314-a.norwlk1.ct.home.com. [24.228.0.171], dsn=2.0.0,
stat=Sent (e73MfZ331592 Message accepted for delivery)
Aug 3 17:41:35 mail sendmail[3845]: e73MfW90384
```

Again, these log entries clearly refer to the comparator message, as indicated by the message ID and the time of transmission.

No log entry is found in the webmail.terago.com system log that would refer to the questioned message (message ID 3989e793.87BDEEE2@terago.com). A log entry is created whenever a message is transmitted through an email server of this kind.

Therefore, the absence of log entries referring to the questioned message shows that it was not sent through the mail.terago.com or webmail.terago.com servers.

d. Lack of record of Questioned Message on Mr. Trivedi's Computers

I, and EED technicians working under my supervision, have searched the data from Mr. Trivedi's computers, including his electronic mail files, and we have not found any record of his having sent the questioned message. Details of these searches are set forth below for each computer that we examined. This is consistent with the above evidence indicating that the questioned message was not authentic.

e. Other considerations

I, and EED technicians working under my supervision, examined several other computers provided by Mr. Munshani and Dennis Glatting, who was identified to us as the network administrator for Mr. Munshani's email servers. In my conversation with Mr. Glatting, he informed me that a computer at Mr. Munshani's home served as the primary hedgefund.ushedgefund.com server, and that a computer at Mr. Glatting's home office served as a backup to receive email sent to hedgefund.ushedgefund.com if the server at Mr. Munshani's house were not functioning. Mr. Glatting further explained that the servers at Mr. Munshani's residence and Mr. Glatting's home office had been reconfigured between August 3, 2000, and the date when EED inspected the computers and that no backups existed from the August, 2000, time period. I was informed by Mr. Glatting that logs for the hedgefund.ushedgefund.com servers from the time period of the questioned message no longer were in existence. Nevertheless, certain computers used for the hedgefund.ushedgefund.com email server at various times were made available by Mr. Munshani and Mr. Glatting, and we examined the hard drives from these computers

to determine if any residual or deleted data might be present that would provide evidence of the creation or receipt of the questioned message.

We did not locate any such evidence, and in particular we did not locate any logs for the hedgefund.ushedgefund.com email server on the computers provided by Mr. Munshani or Mr. Glatting. Because these logs have not been preserved, it was not possible to confirm whether or not any record of the questioned message appeared in the hedgefund.ushedgefund.com logs or to evaluate the validity of any such records.

f. Detail of Examination by EED of Computer Systems and Media in this Matter

I, and/or EED technicians working under my supervision, examined nineteen systems (including live systems and backup tapes) in connection with this matter. For some of the systems, multiple image copies were examined. A description of the systems and the information derived from our examination follows.

*General Procedures for Copying and Examination of Computer Data:* The general procedure for this inspection was as follows: EED made image copies of the hard drives of computers made available for inspection by the parties using a computer program called SafeBack, version 2.0. This program is a standard forensic utility sold by New Technologies, Inc. The images were restored to clean hard drives and searched using EnCase, a standard forensic software sold by Guidance Software and additional searching was done using EED proprietary utilities. EED also examined image copies of hard drives of certain computers made by Deloitte and Touche technicians using EnCase. These image copies were restored and searched using EnCase and EED proprietary utilities. EnCase and EED's proprietary utilities reliably search plain text data, but not

data held in other formats, such as compressed files and certain email storage files, including personal folder files. In order to account for non-plain text formats, EED technicians examined file listings to identify data types and specially examined data in non-text files deemed likely to hold data created by the computer's user.

For each of these items I, and/or EED technicians working under my supervision, examined the item to determine the general contents and performed a search to determine whether or not the questioned message was present. Where the questioned message was located, we performed further work as described below. In searching for the questioned message, or portions thereof, we used the following search terms:

<b>Term</b>
The importance of
keeping you excited
hard to overstate
CEO and founder
personally committing
deliver these warrants
last round of funding
will be 2 years
manage this with Signal Lake
e73MfZ331592
e73MfW903843
RAA01318
3989e793.87BDEEE2

These search terms were selected to locate the questioned message or portions of the message on the various systems we searched. Search hits were reviewed when one or more of the search terms were found. The results of the examination and searches were as follows:

**1: Terago DLT Tapes:**

The questioned message purports to have come from Hermant Trivedi and to have been sent through the electronic mail server of Terago Communications, Inc., on August 3, 2000. I requested the backup for August 4, 2000, of the Terago Communications, Inc. computers used as electronic mail servers. This date was chosen as the next backup after the alleged send date of the questioned message. This backup would include any log entries reflecting sending of the questioned message. I was provided with one DLT tape by counsel for Terago. The tape contained a backup of data from several computer servers made using Veritas Software's NetBackup program. Of relevance to this inquiry, the backup contained data from two servers used by Terago for electronic mail, "mail.terago.com" and "webmail.terago.com" The content of the backup tape was restored onto an EED hard drive. I and EED technicians examined the content of the backup and determined that its contents reflect a backup of the relevant Terago servers and we saw no evidence of any tampering.

The data was from a UNIX system (Sun Solaris version 2.6), including logs from the Sendmail electronic mail server program. Typically electronic mail servers of this kind hold email logs in compressed files designated by the extension ".z". Such logs were found in the mail/var/log directory, the appropriate location for such files in a working Sendmail system. These logs are from the "mail.terago.com" system. The following log files were located:

File name	Last Modified
Sysidconfig.log.z	4/11/2000
Syslog.0.z	7/29/2000
Syslog.1.z	7/22/2000

Syslog.2.z	7/16/2000
Syslog.3.z	7/8/2000
Syslog.4.z	7/2/2000
Syslog.5.z	6/25/2000
Syslog.6.z	6/18/2000
Syslog.7.z	6/11/2000
Syslog.z	8/3/2000

The file named syslog.z contains the logs of the mail system from August 3, 2000.

We searched the content of this file for the ESMTP ID found in the questioned message and the comparator message for this server (e73MfW903843) and did locate this ID in the following entries:

**error: safesasl(/opt/sendmail/smmta-8.10.0/lib/sasl/libplain.so) failed: Group writable directory**  
**Aug 3 17:41:32 mail sendmail[3843]: e73MfW903843:**  
**from=<hemant\_trivedi@terago.com>, size=4909, class=0, nrcpts=4,**  
**msgid=<3989F5A3.87BDEEE2@terago.com>, proto=ESMTP, daemon=MTA,**  
**relay=webmail.terago.com [10.0.1.8]**  
**Aug 3 17:41:33 mail sendmail[3845]: e73MfW903843:**  
**to=<scott\_sarkinen@signallake.com>, delay=00:00:01, xdelay=00:00:01,**  
**mailer=esmtpl, pri=214909, relay=zealous.cnchost.com. [207.155.252.26], dsn=5.1.1,**  
**stat=User unknown**  
**Aug 3 17:41:34 mail sendmail[3845]: e73MfW903843:**  
**to=<mikew@signallake.com>,<barts@signallake.com>, delay=00:00:02,**  
**xdelay=00:00:02, mailer=esmtpl, pri=214909, relay=zealous.cnchost.com.**  
**[207.155.252.26], dsn=2.0.0, stat=Sent (SAA06694 Message accepted for delivery)**  
**Aug 3 17:41:35 mail sendmail[3845]: e73MfW903843:**  
**to=<suni@ushedgefund.com>, delay=00:00:03, xdelay=00:00:01, mailer=esmtpl,**  
**pri=214909, relay=cv365314-a.norwlk1.ct.home.com. [24.228.0.171], dsn=2.0.0,**  
**stat=Sent (e73MfZ331592 Message accepted for delivery)**  
**Aug 3 17:41:35 mail sendmail[3845]: e73MfW903843**

We found no other occurrences of the string e73MfW903843. These entries reference the unique message ID of the comparator message, 3989F5A3.87BDEEE2@terago.com. However, there is no reference to the unique message ID of the questioned message, 3989e793.87BDEEE2@terago.com.

We also found compressed .z files in the webmail/var/log directory. These logs are from the "webmail.terago.com" system. The following log files were located:

File name	Last Modified
Syslog.0.z	7/30/2000
Syslog.1.z	7/23/2000
Syslog.2.z	7/16/2000
Syslog.3.z	7/9/2000
Syslog.4.z	7/2/2000
Syslog.5.z	6/25/2000
Syslog.6.z	6/18/2000
Syslog.7.z	6/11/2000
Syslog.z	8/4/2000

We examined the last compressed file and found within a file named "syslog." Log entries were located containing the ESMTP ID shown on the questioned message and comparator message ("RAA01318"):

**Aug 3 17:41:32 webmail sendmail[1318]: RAA01318:  
from=<hemant\_trivedi@terago.com>, size=4746, class=0, pri=124746, nrcpts=4,  
msgid=<3989F5A3.87BDEEE2@terago.com>, proto=ESMTP,  
relay=ostrich.terago.com [10.0.20.18]**

**Aug 3 17:41:32 webmail sendmail[1320]: RAA01318:  
to=<scott\_sarkinen@signallake.com>,<barts@signallake.com>,<mikew@signallake.  
com>,<suni@ushedgefund.com>, delay=00:00:01, xdelay=00:00:00, mailer=relay,  
relay=mail.terago.com. [10.0.1.6], stat=Sent (2.0.0 e73MfW903843 Message accepted  
for delivery)**

**Aug 3 17:42:15 webmail ipop3d[1321]: port 110 service init from 10.0.20.25**

**Aug 3 17:42:15 webmail ipop3d[1321]**

No other occurrences of the ESMTP ID RAA01318 were found in the webmail.terago.com log. These entries reference the unique message ID of the comparator message, 3989F5A3.87BDEEE2@terago.com. However, there is no

reference to the unique message ID of the questioned message,  
3989e793.87BDEEE2@terago.com, in the webmail.terago.com log.

## **2: Stuck desktop computer**

This computer was imaged by Deloitte and Touche personnel on 2/12/2001 using EnCase software onto CDROM media and was restored onto a EED hard drive using the EnCase program. The computer is described as follows:

Computer Make and Model Number: Gateway GP6-400  
Serial Number: ROP0128

The hard drive found in the computer is described as follows:

Make and Model: Quantum Fireball EX 10.2 AT  
Hard Drive Serial Number: 37183447912

The restored image from the Deloitte and Touche CDs contained a single hard drive formatted as a FAT32 partition of 9.54 (9.6) gigabytes of which 6.54 gigabytes was occupied.

We generated a listing of this computer using Encase, and determined that two email programs were installed on the computer, Outlook Express and AOL mail.

We searched the drive for the search terms set forth above using EnCase. There were 287 hits. We found 90 Zip files on this drive. We did not find the message in question in any of the files compressed in the zips.

Of the search hits only one (a Microsoft Word document called "sunifabrication.doc") contained a portion of the message in question. This document contains no indication that the message was sent by Mr. Trivedi. Rather it was a document discussing the inauthenticity of the questioned message. (I have not relied

upon the content of the "sunifabrication.doc" file in connection with my opinion in this matter.) The "sunifabrication.doc" file was created substantially after the alleged date on which the message was sent.

### **3: Mr. Munshani's IBM Thinkpad #1**

We examined an IBM Thinkpad provided by counsel for Mr. Munshani. A full image copy of the hard drive from this computer was made by an EED technician using the SafeBack program, version 2.0, on 03/28/01 at 155 Federal 17<sup>th</sup> Floor in Boston Massachusetts. The date/time of the computer was within 1 minute of the time on the technician's watch.

The computer is identified as follows:

Make Model # IBM Thinkpad 600  
Serial Number: 78 – m4660 Type 2645-420 264541U78 M4660  
Color: Black

The hard drive in the computer is identified as follows:

Make/Model: IBM DARA 21200 E 182115 J  
Serial Number: Not available  
The hard drive has a capacity of 12 gigabytes.

Our search of the drive's contents disclosed only one pertinent search term hit, a file named "Return .doc" in the "My Documents" folder created on and last modified February 2, 2001. This document contained copies of the headers from three messages: (a) the questioned message, (b) the comparator message, and (c) a third message apparently from Hermant Trivedi dated August 3, 2001. The content of this file did not affect my opinion in this matter, due to the file being dated subsequent to the received

dates shown in the messages and also subsequent to the Outlook creation date of the questioned message.

We generated a listing of the contents of the drive and further examined it for email stores and file formats not amenable to a text search. The Notes mail stores were not searched because the last accessed, create, and last write dates were all in February of 2000, prior to the date of the message in question, and in my judgment not relevant to this investigation.

We examined the Microsoft Outlook personal storage files (.PST files) found on this computer and determined that there was one .PST file holding copies of the questioned message and the comparator message. This file was found on what would have been viewed as the "D" drive on this computer (i.e., on the second partition of the hard drive). The file is found in the directory "d:\toshare" and is called "outlook.pst". It has a Windows creation date of December 14, 2000. The Windows "creation" date is set when the file is first saved in its present physical location on the drive.<sup>3</sup> This file has a "last saved" or "last modified" date of February 23, 2001. The "last saved" date for an Outlook .PST file is generally the last time the file was closed, because the Outlook program changes the "last saved" date on each occasion that the file is closed.

#### **4: Mr. Munshani's IBM Thinkpad #2**

We examined a second IBM Thinkpad provided by counsel for Mr. Munshani. A full image copy of the hard drive from this computer was made by an EED technician

---

<sup>3</sup> For example, when a new file is created, its creation date and time is initially the date on which the file was first saved. If a file has been copied the creation date and time of the copy is the date and time when the copying took place. If a file is moved to a different drive, the creation date and time is reset to the time of the move.

using the SafeBack program, version 2.0, on 03/28/01 at 155 Federal 17<sup>th</sup> Floor in Boston Massachusetts. The date/time of the computer was within 4 minutes of the time on the technician's watch.

The computer is identified as follows:

Make Model: IBM Thinkpad 600  
Serial Number: 78 – A1342 Type 2645-41U 264541U78A1342  
Color: Black

The hard drive in the computer is identified as follows:

Make/Model: IBM DYKA-23240 E 182115 T 04/98  
Serial Number: 264541U78A1342.  
This hard drive has a capacity of 3.4 gigabytes.

Our search of the drives contents disclosed only one pertinent search term hit. In the drive free space (i.e., the part of the hard drive not in use by an active file) is found in a print spool file, which appears to have been created in connection with a printout of the message. (A print spool file is created when a Windows application, such as Microsoft Outlook, is used to printout files. The print process formats the data for printing and stores it temporarily in a spool file until it is processed by the printer. A print spool file is created automatically by Windows when printing occurs, and normally is automatically deleted at the conclusion of the print process by Windows.) The deleted print spool data is found in cluster 41668. (Windows hard drives are subdivided into clusters which are numbered sequentially.) This file had no effect on my findings or opinion in this matter.

A copy of an Outlook .PST file containing the questioned message and comparator message was located on the hard drive of this computer. The contents of this file are identical to the file found on Mr. Munshani's other laptop, discussed above. The .PST

file is found in the directory, "C:\WINDOWS\Profiles\suni\Local Settings\Application Data\Microsoft\Outlook\" and the file is called "outlook.pst". It has a Windows creation date of January 18, 2001 and a Windows last saved or last modified date of February 27, 2001.<sup>4</sup>

**5 and 6: Travan Backup tapes provided by Mr. Munshani**

Two Travan backup tapes were provided by counsel for Mr. Munshani on March 22, 2001. The two tapes were examined using Iomega Backup 98 version 3.2:

Tape 1 was named "Feb24-2000FullBackup-passw". Two sessions were found on this tape: "Feb24-2000FullBackup (C:)" and "Feb24-2000FullBackup Dmax32 (D:).

Tape usage statistics are as follows:

2,443,519,501 bytes used, 1,643,673,600 bytes free  
Initial Format Date 1/21/2000 11:53 A.M.  
Times formatted: 1  
Date Named: 2/24/00 10:48 AM  
Last Write: 2/24/00 10:48 AM

Tape 2 was named "Feb13-2000 00001". Two sessions were found, "Feb13-2000 (C:)" and "Feb13-2000 Dmax32 (D:)" Tape statistics are as follows:

Bytes used 2,142,608,145  
Bytes free 1648128000  
Initial Format 1/22/00 12:15 PM  
Last Format 1/22/00  
Last Write: 2/13/00 5:33 PM

Due to the fact that the backup date and the last write date of these tapes were prior to the date of the message in question, only general examination was conducted of the restored

---

<sup>4</sup> The meaning of "creation" and "last modification" dates for Outlook files is discussed above at fn. 3 and accompanying text.

data from these tapes. The tapes appear to be backups of Munshani's laptop from February, 2000.

#### **7: Mr. Munshani's External SCSI drive**

This hard drive was sent by Mr. Munshani to EED's offices in New York, and imaged on 5/23/01 by an EED technician onto 4mm tape media using SafeBack, version 2.0. This image was restored and examined at EED's offices in Seattle.

The hard drive is described as follows:

Make and Model: Seagate Model ST43400N

Serial Number: SE 852558

Description: External beige SCSI enclosure, approx 12" x 6" x 24" in dimension, with tape drives—other identifier—slight crack on front panel top/right on side.

The SafeBack program saw the drive as 2777 megabytes. The Windows98 "fdisk" program did not disclose any partitions. The Seagate documentation for this hard drive states that this hard drive has a formatted capacity of 2912404054 bytes.

A plain text search of the entire physical drive using the search terms noted earlier did not result in any search term hits. We examined the hard drive using a disk editor and only found binary data which began at logical sector 8482320 and ran till the end of the drive. The remainder of the drive was filled with hex 00's.

#### **8: Mr. Trivedi's Dell Dimension home PC**

Counsel for Mr. Trivedi made available a Dell Dimension PC on May 18, 2001, and an image copy of the hard drive was taken using SafeBack version 2.0. The date/time settings were checked and found to be 2 hours and 50 minutes earlier than a known accurate clock. The computer is identified as follows:

Make Model #: Dell Dimension XPS M2335

Serial Number: Not available  
Color: Beige/ Cream

The hard drives in the computer are identified as follows:

DRIVE A

Make/Model: Quantum Fireball ST  
Serial Number: 156719119333N  
Capacity: 6.4 gigabytes

DRIVE B

Make/Model: Maxtor 91366U4  
Serial Number: HY0PY570  
Capacity: 13 gigabytes

On March 28, 2001, Counsel for Mr. Trivedi also provided 31 CDROM disks represented to contain an image copy of the hard disk drives from this computer made by Deloitte and Touche technicians on February 2, 2001. The EnCase image does appear to be from the same computer EED examined.

Both the Deloitte and Touche images and the EED images were restored for examination purposes. For Drive A noted above both images contained one FAT32 partition of 2.0 gigabytes and an extended FAT32 partition of 10.6 gigabytes as viewed by Encase.

We searched both images in their entirety using Encase software. The EED SafeBack image contained 194 search hits. The Deloitte Touche EnCase image contained 190 search hits. None of the search hits on either image appeared in a context related to the message in question. We further found 23 zip files from the Deloitte Touche image and 28 zip files in the image made by EED. None of the files enclosed within these zip files contained the questioned message.

For Drive B noted above both images contained only one partition which was 6142Mb in size and formatted as an FAT32 file system. The Deloitte and Touche image yielded 19 search term hits while the EED SafeBack image yielded no hits.<sup>5</sup> There were 27 zip files on both the Deloitte and Touche image and the EED SafeBack image. None of the files enclosed within these zip files contained the questioned message.

#### **9: Mr. Trivedi's Generic home PC**

A generic desktop computer was made available to EED on May 18, 2001, and imaged using SafeBack version 2.0. The date/time settings were checked and found to be 57 minutes earlier than a known accurate clock. The computer is identified as follows:

Make Model #: Generic Desktop Computer  
Serial Number: Not available  
Color: Beige/ Cream

The hard drives in the computer is identified as follows:

##### DRIVE A

Make/Model: Western Digital Caviar 36400  
Serial Number: WM420 028 7905  
Capacity: 6.4 gigabytes

##### DRIVE B

Make/Model: IBM DCAA-34330  
Serial Number: Not available  
Capacity: 4.2 gigabytes

##### DRIVE C

Make/Model: Quantum Fireball ST

---

<sup>5</sup> The discrepancy in the number of hits found on the Deloitte & Touche image copy as opposed to the EED image copy is to be expected because the two image copys were taken at two different times. For several of the other searches set forth below, there were similar difference in the numbers of hits between Deloitte & Touche images and EED images. There was no indication that these differences reflect any deletion of data relevant to this case, and therefore I did not consider the differences to be significant in reaching my opinion. .

Serial Number: Not available  
Capacity: 6.4 gigabytes

On March 28, 2001, Counsel for Mr. Trivedi also provided 27 CDROM disks represented to contain an image copy of the hard disk drives from this computer, made by Deloitte and Touche technicians on February 2, 2001. The EnCase image does appear to be from the same computer EED examined. Findings are as follows:

Drive A:

Both the Encase images made by Deloitte and Touche and the SafeBack image made by EED showed that the drive contained two Windows 2000 (NTFS 5.0) partitions, one partition 6.0 gigabytes and another partition of 3.5 gigabytes. There were no files present in the second partition.

Search of the Encase image restored data resulted in 241 hits. We examined the context of each of the hits and determined that these were not from the message in question. We generated listings of the drive and examined them for file formats not accessible to plain text search

Search of the SafeBack image restored data resulted in 632 hits. We examined the contexts of the hits and determined that they were not the message in question. We generated a listing using Encase software to determine the presence of non-text searchable file formats and mail stores present on the drive.

Drive B:

Both the Encase image and the SafeBack image contained two partitions, one 1.0 gigabytes partition formatted as a FAT file system and a second 2.9 gigabytes partition formatted as an NTFS file system. Search of the restored data resulted in 75 hits using

the SafeBack image and 74 hits using the EnCase image. None of the search hits was the message in question. We did, however find the comparator message. We generated a listing of the drive contents using Encase and examined it for non text searchable file formats and email store. By examining the content listings for each partition, we identified the mail applications and the mail stores on the three partitions. We found that this computer had the following mail applications: Microsoft Outlook Express and Netscape Messenger. We examined the email from these files and determined that no instances of the questioned message were present.

Drive C:

Both the Encase and SafeBack images contained one 6.56 gigabytes Windows 2000 (NTFS 5.0) partition. We conducted a plain text search of the entire physical hard drive. The SafeBack image yielded 103 search term hits and the Encase image yielded 98 search term hits. None of the hits involved the questioned message. We generated a listing using Encase software and examined it for non text searchable file formats and mail stores. We found no email stores on this drive. Compressed files, including 148 zip files on this drive and 1 zoo file were identified. None of the files enclosed within these compressed files contained the questioned message.

#### **10: Mr. Trivedi's Toshiba Laptop**

A Toshiba Tecra laptop computer was made available to EED on May 18, 2001, and imaged using SafeBack version 2.0. The computer is identified as follows:

Make/Model: Toshiba Tecra 720 CDT  
Serial Number: 05618397-3  
Color: Medium Gray

The hard drive in the computer is identified as follows:

Make/Model: Toshiba (unknown model)  
Serial Number: Not available  
Capacity: 6.4 gigabytes

On March 28, 2001, Counsel for Mr. Trivedi also provided 10 CDROM disks represented to contain an image copy of the hard disk drives from this computer, made by Deloitte and Touche technicians on February 2, 2001. The EnCase image does appear to be from the same computer EED examined. Findings are as follows:

Both restored images were found to contain 2 NTFS partitions as viewed under Encase. One partition was 2.0 gigabytes and the other was 4.0 gigabytes. A plain text search of both restored images resulted in 92 search hits. Both search hits appear to be identical. None of the search hits contained the message in question.

We created a listing of the contents of the drive using Encase software and examined it for non- text searchable file formats. We found 120 zip files on both images of the drive and did not find the message in question in any of them. In examining both iterations of the hard drive we found that the email client in use to be Microsoft Outlook. We located one mail store, a file named Outlook.pst (208kb) found in the WINNT directory and did not find the message in question.

#### **11: Mr. Trivedi's Inspiron Laptop**

A Dell Inspiron computer was made available to EED on May 18, 2001, and imaged using SafeBack version 2.0. The date/time settings were checked and found to be 4 days and 23 hours later than a known accurate clock. The computer is identified as follows:

The computer is identified as follows:

Make Model: Dell Inspiron 5000  
Serial Number: Not available  
Color: Black

The hard drive in the computer is identified as follows:

Make/Model: IBM Travel Star Dara 218000  
Serial Number: TH-04964T-12567-058-08Y4  
Capacity: 18.14 gigabytes

On March 28, 2001, Counsel for Mr. Trivedi also provided 28 CDROM disks represented to contain an image copy of the hard disk drives from this computer, made by Deloitte and Touche technicians on February 2, 2001. The EnCase image does appear to be from the same computer EED examined. Findings are as follows:

Both the Deloitte and Touche image and the EED SafeBack image showed that the drive consisted of three partitions:

1. Fat32 2.0 gigabytes
2. Fat32 5.4 gigabytes
3. NTFS 3.6 gigabytes

We conducted a plain text search of the contents of both images of this drive. The Deloitte Touche image yielded 201 search term hits. The EED SafeBack image yielded 206 search term hits.. We examined the context of the search hits and found that none of them was the message in question. We did, however, found search hits which pertained to the message in question, including the file "sunifabrication.doc" also found on the Sturk computer, discussed in item 2 above..

We further generated listings of the contents of each drive and examined the listings for the presence of non-text searchable file formats and email stores. By examining the content listings for each partition, we identified the mail applications and the mail stores on the three partitions. We found that this computer had the following mail applications: Microsoft Outlook Express and Microsoft Outlook. We manually examined the two instances

- a. Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook\outlook.pst
- b. Documents and Settings\trivedh\Local Settings\Application Data\Microsoft\Outlook\outlook.pst

Both files were approximately 49 kilobytes in size. Upon manual examination of these two files we did not find the message in question.

We found 79 zip files on the drive and examined each of them for the message in question, which we did not find. In addition we found several other types of compressed files in formats typically used on UNIX systems (4 .z, 3 .gz and 5 .tar files). Contents of these files were examined and did not include the questioned message.

## **12: Mr. Weingarten's Desktop PC**

On March 28, 2001, counsel for Mr. Trivedi also provided 31 CDROM disks represented to contain an EnCase image copy of the hard disk drives from this computer, made by Deloitte and Touche technicians on February 10, 2001. Findings are as follows:

This computer is described in the Deloitte & Touche paperwork as follows:

Computer Make and Model: Apple Power Macintosh G3  
Computer Serial Number: ROP 0128

The hard drive in the computer is described as follows:

Hard Drive Make and Model: Maxtor 92048U8  
Hard Drive Serial Number: W805564A

The drive contains a 19.1 gigabyte partition formatted Macintosh HFS.

We found that this computer to be an Apple computer running Virtual PC version 3.0 in addition to MAC OS. We found several email programs on this computer including Netscape and AOL on the Macintosh. We conducted a plain text search of the entire physical drive which yielded 3063 search terms hits. An examination of the context of these hits disclosed to us that none of them was the message in question. We generated a listing of the contents of the drive and examined it to for non text searchable file formats and email stores which might contain the message in question. The following file types were located: 5 hqx, 41 zip 11 sit and 14 nsf files. The contents of these files were examined and found not to contain data relating to the questioned message.

### **13: Mr. Weingarten's Laptop PC**

On March 28, 2001, counsel for Mr. Trivedi also provided 7 CDROM disks represented to contain an EnCase image copy of the hard disk drives from this computer, made by Deloitte and Touche technicians on February 10, 2001. Findings are as follows:

This computer is described in the Deloitte & Touche paperwork as follows:

Computer Make/Model: Apple Powerbook G3  
Serial Number: CK834317E6D  
HDD Make Model: Apple/IBM DTCA-24090  
HDD Serial Number: KY059898.

The Deloitte and Touche EnCase image was restored onto an EED hard drive for examination purposes. We conducted a plain text search of the entire hard drive. The search resulted in 264 search term hits. We examined the context of the search term hits

and found that they did not contain the questioned message. We created a listing and examined it for non searchable file formats and mail stores. We located three zip files and 1 .sit file. The contents of these files were examined and found not to contain data relating to the questioned message.

**14: Mr. Glatting's Gateway PC**

EED imaged the computer on June 20, 2001 using SafeBack version 2.0 at the offices of EED in Seattle, Washington. Though the computer was available for imaging at the offices of Software Munitions in Redmond Washington, the hard drive was taken to the offices of EED Seattle with the consent of Mr. Glatting for technical reasons. The hard drive was returned to Mr. Glatting on June 21, 2001.

The computer is identified as follows:

Make Model #: Gateway CG-233  
Serial Number: 0007773678  
Color: Cream, small stain on top

The hard drive in the computer is identified as follows:

Make/Model: IBM-DTTA-371290  
Serial Number: SNWM0WMF  
Capacity: 12 gigabytes

We found the drive to contain the following partitions:

FreeBSD (UFS) 6.0 gigabytes  
Linux Swap 1.8 gigabytes

The plain text search of the drive yielded 16 search term hits. The contents of these files were examined and found not to contain data relating to the questioned message.

**15: Mr. Glatting's XPS PC**

EED imaged the computer using SafeBack version 2.0 on June 15, 2001 at the offices of Software Munitions in Redmond, Washington. The computer is identified as follows:

Make Model #: Dell XPS 450  
Serial Number: ROT13  
Color: n/a

The hard drives in the computer are identified as follows:

**DRIVE A**

Make/Model: ATLAS  
Serial Number: 10K9WLSWW00  
Capacity: 9 gigabytes

**DRIVE B**

Make/Model: ATLAS  
Serial Number: 10K9WLSWW01  
Capacity: 9 gigabytes

The images of the hard drives were each replicated onto another drive for examination purposes in order to maintain the evidentiary integrity of the original images. We conducted a plain text search of the drive. The search yielded 3 search term hits on the first drive and 0 search term hits on the second.. The contents of these files were examined and found not to contain data relating to the questioned message.

**16: Mr. Glatting's Dell Precision PC # 1**

EED imaged the computer using SafeBack version 2.0 on June 15, 2001 at the offices of Software Munitions in Redmond, Washington. The computer is identified as follows:

Make Model #: Dell Precision 220  
Serial Number: 870DF01  
Color: Cream color

The hard drives in the computer are identified as follows:

DRIVE A

Make/Model: ATLAS  
Serial Number: S10K2-TY0922  
Capacity: 9 gigabytes

DRIVE B

Make/Model: SEAGATE ST318451LN  
Serial Number: n/a  
Capacity: 18 gigabytes

The images of the hard drives were each replicated onto another drive for examination purposes in order to maintain the evidentiary integrity of the original images. We found the drives to contain the following partitions:

Partition 1: FreeBSD (UFS) 8.5 gigabytes

Partition 2: FreeBSD (UFS) 17.1 gigabytes

We conducted a plain text search of the drive. The search yielded 26 search term hits on the second drive, the 18 gigabytes drive and 17 search term hits on the first hard drive (9 gigabytes) term hits. The contents of these files were examined and found not to contain data relating to the questioned message.

**17: Mr. Glatting's Dell Precision PC # 2**

EED imaged the computer using SafeBack version 2.0 on June 15, 2001 at the offices of Software Munitions in Redmond, Washington. The computer is identified as follows:

Make Model #: Dell Precision 220

Serial Number: B3N6901  
Color: Beige, coffee stains setup

The hard drives in the computer are identified as follows:

DRIVE A

Make/Model: SEAGATE ST318451LN  
Serial Number: n/a  
Capacity: 18 gigabytes

DRIVE B

Make/Model: SEAGATE ST39102LC(SCSI)  
Serial Number: n/a  
Capacity: 9 gigabytes

DRIVE C

Make/Model: Maxtor 5T010H1(IDE)  
Serial Number: TR0LBKC  
Capacity: 9 gigabytes

Encase disclosed that the three drives contained the following partitions:

Drive A: FreeBSD (UFS) partition of 17.1 gigabytes

Drive B: FreeBSD (UFS) partition of 8.5 gigabytes

Drive C: FreeBSD (UFS) partition of 9.3 gigabytes

We conducted a plain text search of all three drives using Encase software. The search resulted in the following results:

Drive A: 1 hit

Drive B: 2 hits

Drive C: 0 hits

The contents of these items were examined and found not to contain data relating to the questioned message.

### **18: Munshani FreeBSD Server**

EED imaged the computer using SafeBack version 2.0 on June 7, 2001, at Mr. Munshani's residence.<sup>6</sup> The computer is identified as follows:

Make Model #: Generic Desktop  
Color/Exterior Description: Brown/cream color with plastic orange inlay on front  
Serial Number: N/A

The drive is described as follows:

Make Model : Western Digital WD200 BB-00 AUA1  
S/N: NA

Encase software disclosed that this hard drive consisted of one 18.6 Gigabyte FreeBSD partition. We conducted a plain text search of the entire drive. The search resulted in 55 search term hits. The contents of these items were examined and found not to contain data relating to the questioned message. Because we were informed that there were no pertinent mail logs on this drive we did not further examine of this drive.

### **19: NEXT SCSI hard disk drive.**

EED received the following hard drive on 8/27/01 from Mr. Munshani:

Make/Model: SEAGATE ST1480N  
Serial Number: WN228562  
Capacity: 407 megabytes

We created an image of the computer using SafeBack version 2.0 and conducted a plain text search of the entire physical drives contents. The plain text search yielded 6 hits.

The contents of these items were examined and found not to contain data relating to the

---

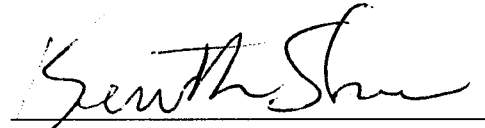
<sup>6</sup> An initial attempt to take an image copy of the hard drive from this computer was made on May 14, 2001. However, the image copy was not completed due to a power interruption that occurred during the process and due to limits on the procedures that were permitted.

questioned message. We were further informed by counsel for Mr. Munshani that the drive had not been in use for a substantial period of time prior to the questioned message.

**V. Conclusion**

Based on the above, in my opinion the questioned message is not authentic.

Submitted September 12, 2001.

  
Kenneth Shear