CASE BRIEFING

Suni Munshani vs. Signal Lake Venture Fund II, LP, et al.
Massachusetts Superior Court, Civil Action No. 00-5529 BLS

Involved Parties

Suni Munshani was the plaintiff in the Suni Munshani vs. Signal Lake Venture Fund II, LP, et al. case. His history involved "chairman of the board for a New York-based bandwidth management company," graduation from the "prestigious India Institute of Technology," a fifteen year history of investing in corporate startups, and board membership to several other technology-related companies (Miller 2).

Hermant Trivedi was the purported sender of the alleged e-mail to the plaintiff. He was the Chief Executive Officer of Terago Communications, Inc. and as such was the defendant in this case.

Kenneth Shear of Electronic Evidence Discovery, Inc. was the lead forensic analyst that prepared the fact-finding 147 page report that outlined his company's thorough inspection of both the plaintiff and defendant's seized equipment, mail exchange server logs, drive backups, etc.

Dennis Glatting was the network administrator that oversaw the plaintiff's e-mail servers. He served as a witness that provided information concerning the workings of several servers positioned not only in the plaintiff's home, but at other places of business.

Honorable Allan van Gestel was the Justice of the Suffolk County Court system that oversaw and ruled accordingly on the proceedings of this case.

Case Background

In the Suni Munshani v. Signal Lake venture Fund II, LP, et al., Suffolk County Court case, Mr. Munshani sued the venture-capital based company for $25 million because the CEO, Hermant Trivedi, had allegedly promised him warrants with which to purchase stocks at very favorable pricing. Simultaneously, he filed suit in federal court against Terago Communications Inc., "an Andover-based semiconductor manufacturer and one of Signal Lake's portfolio companies" (Miller 2). According to Mr. Munshani, the unfulfilled offer in question was presented to him on August 3, 2000, via e-mail, because he had helped Terago Communications Inc. raise venture capital with which to invest in new corporate startups. Mr. Munshani, in an attempt to bolster the argument in his favor, produced that e-mail that had allegedly been sent from the CEO to him. In that e-mail, the wording and promises were inline with Mr. Munshani's sworn statement and allegedly the e-mail began as follows (Miller 3):

Suni,

> The importance of keeping you excited about Teago is hard to overstate. As CEO and founder I am personally committing to deliver these warrants to you at the last round of funding. The period we discussed will be two years. Please let me manage this with Signal Lake.
>
> Regards, Hemant

Mr. Trivedi was dumbfounded and maintained that he had never written or made any such promises to Mr. Munshani (written, oral, or otherwise). Even after an internal investigation where the defendant's company hired their own forensic investigators to duplicate and run scans on corporate systems and mail servers, no such records were produced that validated that an e-mail had been sent to Mr. Munshani with any such promises (Weigarten 2). While this was going on, the defense for Mr. Trivedi filed affidavits on February 16, 2001 stating that the alleged e-mail had been forged and was not legitimate. Mr. Munshani's counsel filed their own affidavit to the contrary on February 19, 2001 swearing that it had not been forged. With both parties at a standoff, the honorable Suffolk County judge, Allan van Gestel, summoned the services of an independent computer forensic analyst on March 9, 2001 that was not associated with either party and therefore had no bias to the case. His Seattle-based company's forensic services were enlisted in order to determine which party was telling the truth. He was given the following charge by the court (Suni 3):

> "The expert shall provide this Court and the parties with a written report setting forth his opinion as to whether the authenticity of the August 3 e-mail can be ascertained with a reasonable degree of technical certainty, and, if so, the expert shall state his opinion on such authenticity and the detailed grounds for that opinion."

Forensic Analysis

On early 2001, the court-appointed computer forensics expert, Kenneth R. Shear of Electronic Evidence Discovery, Inc., began a seven-month process duplicating, analyzing, and extracting digitally stored data. He then scrutinized and evaluated the uncovered evidence and compiled a 147-page report that presented evidence refuting the authenticity of the e-mail in question. This final report's findings were submitted to the court in full on September 12, 2001.

In total, Mr. Shear and forensic investigators working under his supervision, examined 33 data storage devices over a 7-month period. The inspected devices ranged from laptop and personal computer hard drives to tape disk and SCSI drive backups. It was Mr. Shear's final opinion, as outlined on page 3 of his report, that the message in question was "clearly not authentic," but more so than just his opinion, he provided 5 specific points that substantiated his opinion (Shear 5). They are summarized as follows:

1. The investigation had uncovered evidence that was consistent with the copying and pasting of e-mail header data from another e-mail that had been sent at an earlier time, but with completely different textual content.

2. The investigation had unveiled an inconsistency with the e-mail's message ID and the alleged time stamp that the e-mail reflected.

3. The investigation had unveiled inconsistencies with the received, sent, create, and last modified dates embedded within the e-mail message as saved on the plaintiff's personal computer.

4. The investigation failed to unveil any record of the alleged e-mail as ever having passed through the corporate e-mail servers of Terago Communications, Inc. as should have been the case providing the defendant had indeed sent the e-mail as implied and sworn to be the Plaintiff.

5. The investigation failed to unveil any record of the e-mail as being created, manipulated, sent, or even ever existing on the computer systems used by the defendant.

As far as the actual basis and presentation of specific evidence in support of Mr. Shear's opinions, that was the subject of the rest of the prepared report. The "Basis for Opinion" section of the paper went step-by-step explaining what methods the forensic investigators took, what they were looking for, and what they uncovered. They included very specific details and even when they used computer terminology as it pertained to their findings, they included explanations so that the members of the court (i.e., possibly non-technical laymen) would be able to comprehend and understand Mr. Shear's findings.

On page 6 of the final report, Mr. Shear explained how the Microsoft Outlook 2000 product on Mr. Munshani's laptop works and how it was configured. The points of interest were how e-mails were being downloaded from the e-mail server and how they were being sent, received, opened, and stored. The investigation revealed a rather normal setup: that e-mail messages were being downloaded from an e-mail server and stored to the laptop's internal hard drive in a Personal Folder file format as maintained by the mail client in use (i.e., Microsoft Outlook 2000 in this case). What the forensic analysis was able to reveal was that the e-mail in question was actually a copy of another e-mail received the same day from Mr. Trivedi (referred to as the "comparator message" throughout Mr. Shear's report and from this point forward in this case brief). The comparator message was the original e-mail and from it, it appeared that Mr. Munshani had first duplicated the legitimate comparator e-mail and then proceeded to change the body of the e-mail and certain data in the e-mail's header. As a side note, and as explained thoroughly in Mr. Shear's report, an e-mail header or e-mail message header, consists of detailed information about the mail servers that it traversed after leaving the sender's computer until it arrived in the receiver's computer. Message header data

contains information such as identification (ID) tagging for use by the mail servers, transmission and addressing data, times and dates pertaining to sending and receiving, the subject line, target party data (i.e., the e-mail addresses used in TO, CC, and BCC fields) and sender party data (i.e., the from e-mail addresses). End users do not normally need to see an e-mail's header data because the mail client software that they are using interprets and displays only the pertinent data automatically (such as who an e-mail is from, who it was too, the subject line, and the body of the e-mail). Mr. Munshani was savvy enough to understand that this header data needed to reflect the other content that he was changing, but lacked a comprehensive understanding of what exactly should have been changed.

What gave away his duplication process was the discovery of an ESMTP ID number that was the same in both the comparator e-mail and the alleged e-mail that Mr. Munshani's entire case was based on. This was an issue because ESMTP ID's are unique to the server so that they can be tracked. Unique to the extent that no two e-mails passing through the same e-mail server are going to have the same ID. An ESMTP ID is simply a unique number assigned by an SMTP server (Simple Mail Transport Protocol is the protocol used to transfer e-mail over the internet and between servers). It becomes an ESMTP ID (Extended SMTP) when an e-mail has to traverse more than one mail server to reach its target. This is common for e-mail that is sent between different networks (i.e., between users that do not have e-mail addresses on the same mail server). In both the comparator e-mail and the alleged e-mail, all three ESMTP IDs were identical. This provided, with virtual certainty, that one of the two e-mails was not legitimate.

Further analysis revealed that the ESMTP ID as created by the mail software on one of the three mail servers actually used an hourly time stamp method for the first character of the ESMTP ID. When converted from a letter to a number, it revealed which hour of the day the ESMTP ID was generated. When Mr. Shear's team converted the ESMTP ID into a time stamp, it matched the time stamp of the comparator e-mail's traversal of the mail servers per not only the mail server logs, but also the time and dating of the e-mail itself. What differed completely was the actual time stamping of the alleged e-mail. Not only was it not possible for the exact same ID's to exist, but the fact that the IDs reflected an time stamp further invalidated the alleged e-mail because the times in the header data differed from what they should have been.

Order of the Court

After the report of the forensic investigator was accepted and remained un-refuted by either side for 21 days, Mr. Munshani was found to have greatly abused the trust of the court as well as the whole of the judicial process. The honorable Suffolk County judge Allan van Gestel not only fully dismissed Mr. Munshani's case, but he also ordered the plaintiff to pay all of Signal Lake's legal fees resulting from his perpetration of fraud.

Lessons Learned

In my opinion, the forensics' report is full of important techniques along with detailed data recovery methodologies, but even more importantly than those are the lessons that apply to individuals who are only neophytes when it comes to computers and their intricacies. In my opinion, the following are general lessons learned from this case and as such are applicable to non-forensic analysts:

1. E-mails are very important. When anyone sends an e-mail or receives an e-mail they've received a piece of an evidentiary chain. The e-mail doesn't necessarily get deleted when a user deletes it from their computer for several reasons. For one, it may exist on another mail server while in transition or while waiting to be downloaded by the receiver. At the very least, evidence that the e-mail passed through one or more mail servers is maintained in server logs. Second, the e-mail may exist on the receiver's computer and third, it may exist in a backup anywhere along the line between the original sender and the e-mail's final destination. One should never assume that they have the only copy of an e-mail.

2. Creating an archive of e-mails is important. If one is diplomatic in their e-mails and doesn't have anything pejorative to conceal, then by deleting messages, one potentially places themselves in the position of appearing as if they were attempting to hide possible evidence. A lack of documentation, especially if another party has copies of e-mails, can actually hurt oneself when embroiled in a heated court case. On the flipside, if the other side has attempted to hide or delete possible evidence, then by maintaining a copy of e-mails, you'll have the advantage.

3. In the corporate environment, maintaining one's own e-mail servers is vital. The importance of such an act is fundamental in providing detailed mail logs as well as understanding what the mail logs record. When a corporation employs its own knowledgeable IT staff to oversee its own internal mail servers, the IT administration will know how best to make backups of the logs in order to maintain not only an evidentiary chain, but also the format of the logs and what is contained within them. This saves time and money in the event that the logs need to be inspected. Also, third party mail servers usually will not maintain lengthy backups as they have no need to. Important evidence may be deleted in a third-party mail server environment whereas, internal mail server administration would be more apt to maintain lengthy archives of mail records (including offsite archives).

4. Digital E-mail Identification is a very important consideration when sending and receiving sensitive corporate-related information. Digital IDs work by tagging an e-mail with a specific marker. If the structure or the body of the e-mail changes after it has been sent, the marker will fail a validation check. This would prove that an e-mail had been tampered with

and at the very least will demonstrate that it is not in the same format as when it had left the sender's mail client.

Works Cited

Armstrong, Illena. Now in Session: The Judiciary and the Digital World. August 2002. <http://www.westcoast.com/asiapacific/articles/2002_08/feature/2_feature.html>.

Miller, Jeff. VC's breach-of-partnership lawsuit derailed by finding of bogus e-mail. 11 November 2001. Mass High Tech. 15 March 2007. <http://www.signallake.com /litigation/MassHighTechNewsBreachOfPartnership.pdf>.

Shear, Kenneth. Report of Kenneth Shear. 12 September 2001. <http://www.signallake.com/litigation/shear_report_munshani.pdf>.

Suni Munshani v. Signal Lake Venture Fund II, LP, et al. 1-7. No. 00-5529. Suffolk County Superior Court. 9 October 2001. <http://www.signallake.com/ litigation/ma_order_munhshani.pdf>.

Weigarten, Michael and Adam Weingarten. Email Tampering - This Time, The Good Guys Won. January 2002. Business Communications Review. <http://www.signallake.com/litigation/emailtampering.pdf>.