ASPEN PUBLISHERS

The COMPUTER & INTERNET Lawyer

Volume 24 ▲ Number 12 ▲ DECEMBER 2007

Arnold & Porter, Editor-in-Chief*

The Lamar Owens Case: How Digital Evidence Contributed to an Acquittal in an Explosive Rape Case

By Beryl A. Howell and Brian M. Heberlig

Digital evidence has held the key to putting culpable defendants behind bars. Torn from the headlines are reports of camera phones capturing real-time criminal activity,[1] Blackberries containing incriminating admissions,[2] and computers holding digital evidence crucial to identifying the perpetrator or obtaining a conviction.[3] Rarely are stories told of using the bits and bytes of virtual activity for defensive and exculpatory purposes. This is that story.

As a midshipman at the US Naval Academy, Lamar Owens had his life's dream before him to serve his country in uniform. He was already a star quarterback with a national profile, as well as the captain and Most Valuable Player of the 2005-06 Naval Academy's football team. This dream was shattered midway through his senior year when he was charged with raping a fellow midshipman in her dormitory room in Bancroft Hall at the Naval Academy. The complainant did not report the incident immediately, and when she did, with no witnesses to corroborate her allegations, the case became largely a "she said/he said," except that some of what Mr. Owens says happened occurred online.

The trial took place in a Military General Court Martial at the Washington Navy Yard in July 2006, before a panel of five Naval Academy officers. The penalty for conviction of the rape charge was up to life imprisonment. The case turned on who the jury believed: Mr. Owens or the complainant, both of whom testified at trial. Rather than rely on Mr. Owens' testimony alone, however, the defense was able to present critical digital evidence that may have made the difference and ultimately led to Mr. Owens' acquittal on the rape charge. This key evidence consisted of the results of forensic examinations of the computers

Beryl A. Howell is the executive managing director and general counsel of Stroz Friedberg, a national consulting and technical-services firm, and a Commissioner on the US Sentencing Commission. **Brian M. Heberlig** is a partner in the White Collar Criminal Defense group at Steptoe & Johnson LLP and presented the digital evidence at trial as co-counsel with Reid Weingarten defending Lamar Owens.

Wolters Kluwer
Law & Business

used by the complainant and Mr. Owens. The defense used this evidence to corroborate significant parts of Mr. Owens' testimony and undermine critical elements in the complainant's version of events.

The two sides of this story differed starkly at trial. Mr. Owens maintained that he had consensual relations with the complainant, who had invited him to her dormitory room in an AOL Instant Message (IM) sent from her computer immediately prior to their encounter. He also awsserted that he had a flirtatious relationship with the complainant and had communicated with her several times via IM in the weeks before the incident. The complainant denied that she had invited the defendant to her room. She also asserted that she was merely an acquaintance of the defendant who had rarely (if ever) communicated with him by IM. According to her testimony, Mr. Owens entered her dorm room uninvited, raped her, and left her in her bed, where she remained until her boyfriend arrived in response to her text message from her cellular telephone for help.

The complainant's boyfriend provided the authorities with a paper print-out of excerpts from an AOL IM chat session that the boyfriend and the complainant had engaged in during the time surrounding the incident. The IM communications were still open on the boyfriend's computer screen when he returned from the complainant's room after responding to her text message for help. He copied all of the IM messages with the complainant that appeared on his screen and pasted them into a Word document, which he then printed, purportedly to provide a real-time chronicle of the instant messages that they had sent to each other immediately prior to and after the alleged assault. Ironically, this paper print-out of IM messages, which were preserved by the boyfriend as potentially relevant evidence of the events that evening, turned out to substantially undermine critical aspects of the complainant's version of events.

Searching for the Digital Evidence

The Naval Criminal Investigative Service (NCIS) seized Mr. Owens' computer about one week after the incident and, more than a month later, seized the complainant's computer. Both had been heavily used during the period between the incident and the seizure. The NCIS never seized the boyfriend's computer, so the only evidence available from that computer was the paper print-out of the excerpted IM chat sessions. Despite the fact that digital forensic examinations of the two computers did not uncover a communication from the complainant inviting Mr. Owens to her room on the night of the incident, the results of the forensic examinations proved exculpatory in other significant ways.

Unlike other forms of email messaging, IM communications are normally transient and not stored in an easily retrievable form by the user, unless the default settings of the program are specifically changed to log chat sessions.[4] Such logging was not activated on either Mr. Owens' or the complainant's computer, and no IMs were archived by either party in a manner that they could be easily retrieved.

A thorough search for remnants of IM communications requires creative application of details gleaned about the persons whose IM communications are the target of the search.

It was necessary, therefore, to search unallocated, or "free," space on the computers' hard drives for any IMs that were sent or received on these computers. Unallocated areas of a hard drive hold unsaved or deleted data that has been viewed or accessed on a computer, but that data is inaccessible without the use of forensic tools. Data located in such free space is often fragmentary and may be partially or completely overwritten with other data that has been accessed during the regular use of a computer. The longer a computer is in use after an IM chat session, the greater the chance for any remnants of that chat on the computer to be overwritten, at least in part. A thorough search for remnants of IM communications, in the best of circumstances, let alone in this case, in which the computers were used continuously after the incident, requires creative application of details gleaned about the persons whose IM communications are the target of the search, as well as about the technical nature of IMs.

In this case, searches were framed not only around the screen names used by Mr. Owens and the complainant in emails and IM chat sessions but also for the words that may have been used in flirtatious communications on the night in question, acronyms, and other typical language used by the parties on social networking sites, such as MySpace or FaceBook. While typical searches consist of specific keywords, the searches for IM content in this case also included searches for customized blocks of content that the parties used for "away" messages, the HTML code producing the customized background color used to identify the parties' chat sessions, and other unique characteristics associated with their IM use.[5]

The forensic examinations of the two computers uncovered important evidence that supported Mr. Owens' defense. An important threshold issue was

whether this evidence was sufficiently scientific and reliable to be the proper subject of expert testimony at trial. While many people have a basic understanding of the properties of email messages, instant message technology is far less widespread and relatively unknown in litigation. In fact, the prosecutors objected to the expert offered by the defense and attempted to exclude her testimony. The military judge ordered defense counsel to examine the digital forensic examiner outside the presence of the jury and permitted the prosecutor to *voir dire* her on her qualifications and the reliability of forensic techniques at issue. The expert had examined hundreds of computer hard drives and was intimately familiar with the characteristics and technical properties of the IM program at issue. The judge ultimately ruled that the testimony was sufficiently reliable and helpful to be presented to the jury and held that any questions about the reliability of the forensic examination went to the weight of the evidence, not its admissibility.

Presenting the Digital Evidence

Another challenge was how to present the evidence to the jury. It would have been unwieldy and technically challenging to present the jury with the computer hard drives themselves. Moreover, pure screen shots of the fragments of information from the unallocated space of the computers were difficult to follow and consisted of jumbled bits and bytes of computer text. To synthesize this material for the jury, the defense prepared summary exhibits that contained the relevant portions of the actual screen shots combined with helpful captions explaining the information and highlights of the relevant computer texts. Although these captions and highlights were not part of the actual computer evidence, the judge deemed the summary exhibits admissible because they contained actual excerpts of screen shots from the computer. The exhibits were important to permit the jurors to visualize the technical concepts that the expert explained during her testimony.

Once the defense established the admissibility of the evidence, the results of the forensic examinations, as presented to the jury in the summary exhibits, were revealing in terms of the number and nature of the AOL instant messaging (AIM) contacts between the complainant and Mr. Owens. First, both of them had the other's screen name included in the "Buddy" list of screen names of AIM users with whom the computer user may engage in IM communications. A person's screen name may be added to a buddy list through both automatic and user-initiated mechanisms. Based upon forensic testing and examination of certain log files on the operating system, it was determined that the complainant had stored Mr. Owens' screen name in her Buddy list through a user-initiated action. In a court martial proceeding, members of the jury are permitted to ask questions, and one juror specifically asked the testifying digital forensic expert about the user-initiated action required to add a name to Buddy lists. This evidence demonstrated that the complainant had affirmatively included Mr. Owens in her list of "buddies" with whom she could chat online. Moreover, their respective IM screen names were found multiple times on the other's computer in areas of the computer hard drive indicating contact between their computers.

AIM has a setting that lists under "Recent IM Screen Names" the last 10 screen names with whom IM communications have occurred. This list did not contain either Mr. Owens' or the complainant's screen names on the other's computer. This may have been due to the length of time that passed before seizure of the computers, which were otherwise in continuous use. Searches of unallocated space on Mr. Owens' computer revealed both of their screen names in close proximity with each other and the phrase "recent IM ScreenNames." Forensic testing demonstrated that this pattern was a vestige of IM chat sessions occurring.

Second, the complainant's computer contained remnants of Mr. Owens' AIM profiles. These profiles consist of personal information that an AIM user associated with a particular screen name may wish to make available to other AIM users via a central membership directory accessible to all AIM users. Users may modify the profile information at will, and indeed, Mr. Owens' profile changed over time. The complainant's computer contained remnants of different versions of Mr. Owens' profile information indicating access to his profile on multiple and different occasions.

Third, AIM users may personalize their auto-response messages sent to other users trying to make AIM contact. These personalized auto-responses may be activated by a user who has selected the option of sending an "away" message when the user is not available to respond. Search of the complainant's computer for Mr. Owens' personalized "away" messages found multiple instances of these varied messages possibly showing contacts at different times as his "away" messages changed.

While date and time stamps could not be associated with the evidence of AIM contacts between the complainant and Mr. Owens in unallocated space or in some of the log files, tracking the changes in the "away" messages and Mr. Owens' AIM profile confirmed that the contacts had occurred over a period of time. Interestingly, rather than undermining the probative value of the digital evidence, one of the jurors asked the digital forensic expert whether the absence of date and time stamps could mean that some of the IM chats may have

occurred on the evening of the incident, to which the expert responded yes.

All of this evidence of substantial prior AIM contacts between Mr. Owens' and the complainant's computers corroborated Mr. Owens' testimony that he had communicated regularly with the complainant via IM in the weeks prior to the incident, during the period in which they were developing a flirtatious relationship. Although not conclusive because of the lack of date and time stamps on these prior chats, the evidence also left open the possibility that Mr. Owens and the complainant had engaged in an IM chat immediately prior to their encounter in which she invited Mr. Owens to her room. More importantly, the expert testimony regarding the transient nature of IM communications explained to the jury why it was not surprising, particularly given the length of time between the incident and the seizure of the computers, that the forensic examinations did not locate the actual IM in which the complainant invited Mr. Owens to her room.

Digital forensic evidence may reveal the associations, actions, and sequence of activity to enable the reconstruction of events and make the difference between guilt or innocence.

The digital forensic analysis presented at trial also focused on the activity revealed on the paper print-out from the boyfriend's computer of the IM chat session with the complainant immediately prior to and following the incident. Metadata-like information gleaned from this IM print-out flatly contradicted the complainant's testimony on a critical point. Specifically, the print-out showed continuous IM chat between the complainant and her boyfriend for about 7 minutes from 3:41 AM through 3:48 AM, at which point an IM message from the boyfriend prompted an auto response from the complainant indicating that she had set her IM program to show her as "away" from the computer.[6]

The alleged rape occurred in the next twenty minutes. At 4:11 AM, without any apparent prompt from the boyfriend's computer, an entry appears on the IM print-out showing that the complainant's screen name "returned." At 4:12 AM and 4:14 AM, the complainant sent text messages using her cell phone to her boyfriend asking him to come to her room. The IM print-out next shows an entry at 4:24 AM that the complainant's screen name "is idle," a message automatically issued by default when a chat session is open without activity for 10 minutes. No further entries appear until 5:15 AM when the entry that the screen name "is no longer idle" again appears.

Testing performed on the same version of AIM used by the complainant confirmed that the message of "returned" is automatically sent when an open IM conversation window exists and the user initiates an action on the AIM program. This user-initiated activity may include clicking "I'm back," closing the "away" window, or taking an action in an open IM window with another user, such as sending a reply or deleting or closing that session. Just moving the mouse or touching a key on the keyboard would not result in a "return" message. In short, the boyfriend's print-out contained an automatic "return" message that could have been produced only by user activity on the complainant's computer that may have occurred in a chat session that was open with another user.

This evidence undermined the complainant's testimony in critical respects. She testified that she never left her upper-bunk bed after the alleged attack and did nothing other than text her boyfriend using a cell phone that was located in a cubby next to her bed. The evidence that she "returned" at 4:11 AM to the IM session on her computer, which was located on her desk underneath her bed, contradicted her testimony that she never left her bed. Furthermore, the evidence that the "returned" message could not occur simply by hitting the mouse or keyboard refuted any suggestion that Mr. Owens might have inadvertently triggered the message while leaving her room. Finally, and perhaps most significantly, the fact that her computer did not go "idle" until 4:24 AM, 13 minutes after she "returned" to her computer, indicated that her computer was in use for approximately three minutes between 4:11 AM and 4:14 AM. The defense argued persuasively that the most plausible explanation for this evidence was that the complainant climbed down from her bunk after a consensual encounter with Mr. Owens and deleted the IM session in which she had invited Mr. Owens to her room.

The Verdict

The jury acquitted Mr. Owens of the rape charge, demonstrating how useful digital forensic evidence can be to corroborate defense testimony in a case involving electronic communications. Even when no proverbial smoking gun exists in physical space, the digital forensic evidence may reveal the associations, actions, and sequence of activity to enable the reconstruction of events and make the difference between guilt or innocence.

Notes

1. "Robbery suspect caught on camera phone in Nashville," *USA Today*, AP (Oct. 1, 2004), available at *http://www.usatoday.com/tech/news/2004-10-01-mobile-mugshot_x.htm*.
2. "Fighting Crime with Cellphones' Clues," *N.Y. Times* (May 3, 2006), available at *http://www.nytimes.com/2006/05/03/technology/techspecial3/03cops.html?ex=1186027200&en=c113a7c44b58489f&ei=5070*.
3. "Police Blotter, Weekly CNET News.com report on the intersection of technology and law," *CNET News* (October 20, 2006), available at *http://m.news.com/Police+blotter+Flap+over+nude+photos+of+Cameron+Diaz/2163-1030_3-6128130.html*.
4. Eoghan Casey, Digital Evidence and Computer Crime (2d ed. Elsevier Academic Press), 2004, at p.283.
5. For detailed description of the forensic tools and techniques used in this case, *see* Jessica Reust, "*Case Study: AOL Instant Messenger Trace Evidence*," Digital Investigation, (2006) at pp.238-243.
6. The text of the IM chat itself was also relevant because it revealed that the complainant appeared to be heavily intoxicated. This evidence, coupled with the complainant's admission that she drank approximately a dozen drinks in a two- to three-hour period, provided the basis for additional expert testimony from a forensic toxicologist. The toxicologist testified that an individual of the complainant's weight who consumed that many drinks in such a short period would be likely to suffer from intermittent, alcohol-induced blackouts in which she might appear normal and capable of giving consent to third parties but not remember such conduct.

Reprinted from *The Computer & Internet Lawyer*, December, 2007 Volume 24, Number 12, pages 1 to 4, with permission from Aspen Publishers, Inc., a Wolters Kluwer business, New York, NY, 1-800-638-8437, *www.aspenpublishers.com*.