© sheelamohanachandran | dollarphotoclub.com

Handling the 21st Century Criminal Case: You Don't Know What You Don't Know

The world is comprised of massive amounts of electronic communications and personal/business computing devices that are all interconnected. It can be of no surprise that the modern criminal investigation and trial involve massive amounts of electronic data and critical testimony of computer forensics experts. To provide effective representation in a case of this nature, it is vital that the criminal defense lawyer possess sufficient expertise in the technical aspects of the case. Without this expertise, critical aspects of the defense case will likely be missed, such as missing the few pieces of discovery buried in hundreds of gigabytes of data that provide a fulcrum for the defense theory at trial, missing a suppression issue (e.g., how a particular computer or computer server was located), or missing substantive points on cross-examination of the prosecution's technical witnesses. This article provides practical advice on (1) the basics of preparing a cross-examination for a prosecution computer forensics expert; (2) how to manage and analyze large volumes of discovery; and (3) how to think about technology in the context of defense theory at trial.

Preparing a Cross-Examination of The Computer Forensics Expert

The modern juror, along with everyone else, should have some inherent skepticism towards evidence derived from computers or based on technology. Society has become accustomed to a different news article each week reporting a major security breach at a large corporation or a new security vulnerability that has subjected millions of computer users worldwide to attack. In defending a case built upon computer evidence or from any digital platform (i.e., cellphone contents, email accounts, etc.), the savvy defense lawyer must exploit that aspect to its fullest. Several factors are at play in considering the approach to take. The technical sophistication of the jury considered individually and as a whole, the defense theory at trial, the nature of the allegations, and the type of evidence involved are some of the factors to consider in contemplating how to incorporate technological elements into cross-examination and defense theory and argument.

A properly conducted cross-examination of the computer forensics expert can go a long way in creating reasonable doubt about the integrity of the government's investigation and the evidence the government derived from it. Often the testimony of a prosecution witness can be boiled down to this: "I am an accredited forensics investigator. This is the stuff I got off the defendant's computer. I did it right, so he's guilty." Yet gaps often exist in the critical details of this testimony that the well-prepared criminal defense lawyer can exploit on cross-examination.

As with preparing for any cross-examination, the lawyer should have some specific objective or point to

BY JOSHUA J. HOROWITZ

elicit from the prosecution witness. In prosecuting cybercrime cases or cases in which digital evidence or technology is a dominant aspect, the prosecution's challenge is that it must prove that the person acting behind the keyboard is the same person who is on trial for the crimes alleged. For example, in the Southern District of New York trial of Ross Ulbricht, in which he was charged with creating and operating the Silk Road website, the government on direct examination attempted to lead the jury to believe that the use of a particular PGP encryption key to sign various messages digitally must mean that the messages originated from the same person each time. To the defense lawyer with knowledge of how PGP encryption keys work, this notion is preposterous and was open to attack on many levels. The following portion of the defense cross-examination on the subject of PGP encryption keys was designed to highlight the technical and conceptual flaws in the government's assertions:[1]

Q: And a private key, which you talked about, is just a block of text like the public key that you showed, correct?

A: Correct.

Q: And when you use the term own a private key, you just mean have possession of that block of text, correct?

A: That is correct.

Q: So it could be cut and pasted and sent to someone else, correct?

A: Yes, it can.

Q: It could be shared by the person who generated the key, correct?

A: That is correct.

Q: It could be stolen —

A: Yes.

Q: Correct? It doesn't have to be the same person who uses that private key from message to message much less year to year, right?

A: It doesn't have to be, no.

Q: And it doesn't have to be the same device that uses that key from message to message, from month to month, year to year, correct?

A: That is correct.

. . .

Q: It is really the block of text. It is not whether it is a laptop or a desktop or a phone or anything like that, right? It is the block of text that counts, right?

A: It is universal, yes.

Q: So the only thing that you know when you verify is that you're communicating with someone who is using that block of text, correct?

A: That is correct.

. . .

Q: Right. Even if someone else was using the key, even if they passed on — the office manager could have made a copy of the file key, right — of the file cabinet key, right?

A: Right. There could be multiple copies of a private key that multiple people can have.

Q: And multiple people could use it at the same time?

A: They could, yes.

Q: Message to message?

A: They could.

The point that the government spent a significant amount of time trying to make on direct examination was quickly stripped of its value with a few questions designed to highlight the fallacies upon which the government's encryption-key identity theory rested.

Another area ripe for cross-examination is to attack the methodology used by the government's technical witnesses when they obtained computer forensic evidence. Like any other "science" such as fingerprinting, hair, or DNA analysis, computer forensics examinations must adhere to certain guidelines. Finding those instances in which the examiners may have deviated from those guidelines and questioning them about their actions can go a long way in creating doubt about the integrity of a computer forensics examination. Knowledge of the proper techniques and implications of improperly acquiring evidence are essential. For example, again from the Silk Road trial, asking an examiner from the FBI's Computer Analysis Response Team (CART) the right questions about causing critical data to be lost can create ammunition for closing:

Q: You didn't generate the MD5 hash value for the laptop until October 3 when you started the RAM[2] capture?

A: Correct.

Q: And the RAM capture is essentially the running memory on the laptop?

A: Yes. RAM is random access memory, that's correct.

Q: Can you just define that for the jury, please?

A: Yeah. So, random access memory is the memory in your laptop or computer that's used by not hard drive storage. It is that instantaneous memory that the basic code for the programs gets loaded into RAM and then your computer can use it in there.

Q: And that gives you a window — it gives you ability to see what processes are running on a computer, right, RAM?

A: Whether it gives you what processes are running — everything gets loaded into RAM. So all the binary codes, all the codes that the computer needs to run, is loaded into RAM. That could be the active process. That could be the operating system and so forth.

Q: So on October 3, which is two days after you received the laptop, you began to do the RAM memory capture?

A: That's correct. One of my associates and I — just to be clear.

Q: And you weren't quite sure how to do that RAM capture, correct?

A: The RAM capture was nontrivial.

Q: Right. But you weren't quite sure how to do it. You asked for assistance, in fact?

A: I did.

Q: You asked whether there was a RAM capture tool that you could use for it?

A: That's correct.

Q: And this is a relatively new field in computer forensics, RAM capture?

A: No. I wouldn't say it's a new field.

Q: Well, one of the things that is part of the RAM capture is encryption keys and passwords and other things that are stored in the memory, right?

A: That's correct.

Q: And the processes that the computer — the process of the computer programs that are running on the computer is something else that RAM can tell you, RAM memory capture would be able to resolve for you?

A: That information can be in RAM.

Q: And the active network connections at the time that the capture occurred would be something else?

A: It can be. It doesn't necessarily mean that it is.

Q: And it could also determine whether there were malware or viruses or other programs running on the system, correct?

A: It could be, yes.

Q: Now, you've used a piece of software called FMEM, F-M-E-M, to try to acquire the RAM memory?

A: That's correct.

Q: And system memory is broken down into registers called ranges. Is that right?

A: That's correct.

Q: And for FMEM you have to specifically point the program at the registers that you want the system … to capture, right?

A: That's correct. The RAM is divided into chunks, into groups, so to speak. Some are more protected.

Q: Okay. And so — and if you don't direct the capture process at the right registers of RAM they will go to something called uncachable, U-N-C-A-C-H-A-B-L-E?

A: I believe so.

Q: And you weren't sure at the time about this, is that fair to say?

A: Well, this is why I obtained the help from one of my associates.

Q: But in fact, the FMEM capture did not work entirely, correct?

A: Upon capturing what I believe was the third register or third section of the memory, FMEM crashed the computer.

Q: When it crashed the computer you were no longer able to get any of the RAM capture that you had not gotten initially, correct?

A: We were able to continue with the capture after the computer was restarted.

Q: Now, in doing your RAM capture you consulted the manuals on the computer in an attempt to find out how to proceed, right?

A: I don't recall consulting any manuals on the computer.

Q: Did you keep a running roster of commands that you issued the computer during your work?

A: Yes, we did.

Q: I am going to show you what's marked Defendant's I for identification — "K," I am sorry. Call it Defendant's K for identification. And ask you to look at page two of this document. I ask you if that refreshes your recollection that you consulted the manuals on the computer?

A: These are not the manuals for the computer. These are manuals for the applications MEMDUM and FMEM that may or may not have been on the computer.

Q: Right, but you were looking for them?

A: Yes.

Q: And did you find one for MEMDUM?

A: I don't recall whether one came up or not.

Q: Well, there's no such file for that on a Linux system, is there?

A: There could be. Depends on the Linux system. Most likely there was not, but I don't remember for certain. Chances are, since I then checked for a manual for tool FMEM, that there was no tool for MEMDUM on the system.

Q: And so you never got a full RAM memory capture, correct?

A: Can you define a full RAM memory capture, please?

Q: Well, why don't you.

A: Well, the difficulty in RAM capture is that it's live, so it's ever changing and it's ever active. When we captured what I believed was the third register or third group of memory from the RAM, the system crashed, which is not that uncommon in RAM captures. And so after we were able to restart we restarted with our own version and moved onto the next and we continued to capture the other registers that were still there.

Q: But when you had the capture open before it crashed it has all the operations going, correct?

A: Yes.

Q: And so once it crashes and then you reboot it, you've lost all of that information that's included that went live before it crashed, right?

A: You do not lose all of the information.

Q: But you lose information?

A: Do you lose information?

Q: And you don't know what information you lost?

A: You do not know.

Q: And that information is lost to us forever, essentially?

A: It is.

This portion of the defense cross-examination serves two functions. First, it highlights the fact that the FBI CART examiner crashed the target laptop, causing a loss of critical information. This can create significant room for argument

on closing depending on the nature of the defense at trial. Second, the examiner's lack of subject matter expertise is highlighted for the jury, which goes a long way in casting doubt on the credibility and integrity of their investigation.[3]

In state investigations in which there are fewer resources and less expertise than at the federal level, investigators can and do stray from forensically sound investigative work, and this may leave the state's case open to attack. For example, a failure to create a forensic image of a laptop computer alleged to contain illicit pornographic images gives the defense strong grounds for attacking the investigation on both authenticity and spoliation grounds.[4] Even at the federal level, the FBI CART members are not immune from mistake.

But where does the material for cross-examination come from? The most fruitful source of material for cross-examination of government computer experts is from their notes. If their work is done in accordance with sound forensic practice, they should have maintained documentation of each step along the way in conducting the examination. From the notes, it can be determined whether the examination was done in accordance with established forensic principles, whether any issues arose during the time their investigation was conducted, whether a complete investigation was conducted, and other issues and procedures that would be reflected in the notes of a diligent (and competent) professional. The takeaway point is that some questions always can be asked on cross-examination of the computer forensics experts that can create reasonable doubt about the integrity of their work.

Another way to obtain potentially useful cross-examination material is to use the experts' purported knowledge against them. Experts that testify on behalf of the government will likely have a long list of courses and prior experience to spout off to the jury to make themselves seem more credible. In some circumstances, this can be leveraged by the defense on cross-examination. For example, FBI CART experts who have some sort of network security training credential listed on their resumes can be asked multiple questions about Internet security and computer vulnerabilities:

Q: Now, we talked just for a second — you have training in network security, correct?

A: I do.

Q: And you were an informational technology — information technology specialist, is that one of the positions you have held?

A: Yes.

Q: So could you explain what that involves in terms of training?

A: Information technology specialist?

Q: Yes.

A: Yes. That is more on the side of maintenance and things to that nature of computer systems.

Q: Keeping networks secure?

A: Keeping networks secure.

Q: Teaching best practices to people who work on networks?

A: Just, again, managing computer systems for users and things like that.

Q: So you have to have an open port to the Internet on your computer to operate BitTorrent, correct?

A: You do. The protocol is required

that a port or a connection spot is open.

Q: The fact that he's downloading at that time, that that process is going on, means that the port was open at that time, right?

A: It was connected.

Q: And that you know from your training makes one vulnerable, correct, to have an open port like that — it makes your computer vulnerable?

A: That's how the Internet works. There are open ports on a lot of different surfaces. It is the nature of the Internet. Something has to get transferred back and forth. So, yes, a port was open on the machine to allow BitTorrent, that client, to work.

Q: But that also means that those with sophisticated computer skills could exploit an open port as well, correct?

A: Is it possible for that to happen? Yes.

Q: In fact, you could be exploited by hackers, by viruses, right? All sorts of things can get into your computer through BitTorrent? Even BitTorrent downloading, you can have viruses and malware that come with those files, right?

A: With the files you download?

Q: Yes.

A: Yes, they can contain programs that do things like that.

Q: I'm sorry. Programs?

A: There are programs that can be used maliciously, yes.

Q: Maliciously, including to operate a computer remotely, right, that kind of malware can be —

A: They make that stuff but it's again …

Q: And knowing a port is open on a computer, for someone …

A: Yes. Again, that's how the Internet works. You have these ports that are open.

In a case in which the integrity of information recovered from a computer is a critical issue, a line of questioning of this nature may, if done with the right touch, raise a few questions in the jury's mind. In practical terms, this line of questioning may get the defense team one step closer to reasonable doubt.

Discovery Management

The modern criminal case involves reams of discovery distributed on hard drives, discs, and USB thumb drives. In complex cases, it is not uncommon for the amount of data turned over in discovery to exceed several terabytes.[5] Upon receiving the discs or hard drives that contain the case's discovery, the first step is to identify what type of information is contained on the disk in a categorical sense. For example, does the disk contain forensic images of a computer system or a cellphone? The fruits of an email account search warrant?

This question can typically be answered by determining what kinds of files (or file types) are contained on the disk. For example, a search warrant return for a Gmail (Google Mail) account is typically provided to law enforcement as an .mbox file. Thus, files with the extension .mbox indicate that emails are a part of the government's investigation. These files can be accessed by freely available software such as Thunderbird. Computer forensic image files can be provided in a variety of formats, including .dd, .E01 (encase expert witness files), .img, etc. The filetype of a forensic disk image also gives some indication of how it was acquired. Depending on the circumstances, this can provide some ammunition for cross-examination down the road at trial.

After determining the makeup of the content provided in discovery, the next step is to determine the best method for analysis of the discovery. This step is critical to mounting a successful defense at trial. To avoid missing critical information buried in the discovery, an essential asset to the defense is a skilled practitioner who is capable of both manipulating the technology and building a defense at trial. For example, a production from Google in response to a search warrant may contain several .mbox files, each containing thousands of emails, with IP address login records associated with the account. If, for example, the defendant's location on a particular date and time is a critical issue in the case, these IP address records may become crucial to the defense. Most often the data is produced in a searchable format, which is necessary to sift through the mountains of information that may be produced by the government. If not, the government should be pressed to produce it in such a format.

A number of expensive e-discovery solutions are capable of indexing .mbox files. Licenses for this type of software can cost upwards of $15,000 per instance. However, this type of software does not provide the necessary answers to building a defense and still requires a skilled operator to dig out the key emails from an .mbox file.

On the other hand, free software exists that is capable of quickly creating a searchable index of multiple .mbox email files. This index allows for a large production of emails to be searched with multiple parameters. For example, a search can be constructed that will find any emails sent between 5-1-15 and 5-6-15 to a particular recipient, containing a specific keyword and containing an attachment. In conjunction with other freely available software, this setup can enable its operator to sort through piles of email to find emails that are relevant to the defense. The technology used by expensive e-discovery

providers is quite similar, while freely available software plus a skilled operator can yield the same results.

It is also advisable, if possible, to store all of the information received in discovery in one place. In a complex case involving a lengthy investigation, there may be hundreds of thousands of emails, multiple forensic images, subpoena returns from multiple companies, etc. Over time, this information may be produced by the government on multiple mediums, discs, hard drives, thumb drives, etc., which can prove difficult to keep organized. Very large external hard drives capable of storing multiple terabytes of data are now relatively inexpensive and provide good storage solutions in this situation. The key is to keep the discovery together so that valuable time is not wasted searching for the same files repeatedly. Moreover, defense counsel will be able to perform one-step, one-stop searching at trial, when time can be at a premium (such as during the examination of a witness).

However, there is no "one-size-fits-all" method to analyzing the massive quantities of discovery in the modern criminal case. The data analysis is highly specific to the defense theories to be advanced at trial and the nature of the charges in the case.

Thinking Technologically In the Context of Defense Theory at Trial

In the modern government case that is built using technology, a viable defense theory at trial must address the technical components of the government's proof. For example, if a portion of the government's case is built on identifying a defendant based on certain Internet activity (e.g., logins to a website from a certain IP address), the defense theory must incorporate an explanation for this activity.

Technology is fickle and gives defense lawyers a broad range of tools with which they can be creative. It can be thought of like Newton's Third Law, which states that for every action, there is an equal and opposite reaction. Applied to a defense theory in technical terms, for every "technically sound" piece of evidence there is *always* some alternate explanation. Every IP address can be masked, spoofed, concealed, or hidden; every Internet account can be hacked or compromised; every computer is full of security flaws and highly vulnerable; every timestamp can be manipulated; every file can be changed; and the list goes on. How to incorporate these explanations into the defense theory is highly specific to each case, depending on the nature of the government's proof, the charges, the composition of the jury, and other idiosyncratic factors.

For example, a general computer forensics expert may not be particularly helpful to the defense case. But rather, an expert who can testify about specific security vulnerabilities in the exact version of the operating system that was running on the defendant's computer at the time it was seized by law enforcement will give the jury much more to latch onto in creating reasonable doubt.

The lawyer's task in preparing an expert of this nature requires an in-depth understanding of the underlying technology. To be most effective, the lawyer's direct examination must bridge the gap by having the expert distill and explain technologically complex concepts to jury members in byte-sized pieces they will be able to digest. This requires direct questions to be formulated in a way that will create the greatest evidentiary value from the expert's testimony.

Conclusion

The technical components to modern criminal investigations and prosecutions are not going away any time soon; indeed, cases, and defending these prosecutions, will likely become more dependent on technology over time. To defend the modern criminal case, a defense lawyer must be prepared to defend against the technical components of the government's proof. An in-depth understanding of the technology is critical to mounting a successful defense at trial. Forceful cross-examination of the government's technical witnesses, effective discovery management and analysis, and cogent use of defense technical witnesses at trial are key in defending the modern criminal prosecution.

Notes

1. Transcript excerpts are from *United States v. Ulbricht,* 14 Cr. 068 (SDNY). This particular portion is from the defense cross-examination of Special Agent Der-Yeghiayan on day three of trial.

2. RAM stands for Random Access Memory. A relatively new field in computer forensics involves acquiring and dissecting the RAM from a live machine. This process potentially allows examiners to obtain encryption keys and a host of other information about the system. The process of acquisition and analysis can be complex and requires a highly skilled specialist. For more information about memory forensics and the software that can be used to dissect memory, *see* http://www.volatilityfoundation.org/.

3. Five technical witnesses testified for the government during the course of trial. Cross-examination topics included bitcoin forensics, Linux/Unix system security, network security, remote server administration (SSH Keys), and proper computer forensic techniques. For complete transcripts of the cross-examination of each of the government's technical witnesses, visit http://www.techlawny.com/#!documents/ck1e and download the PDF titled *SR Technical Crosses*.

4. A perfect example of this is a recent case from Orange County, N.Y., *People v. Naran,* Index No. 7379/11. In *Naran,* local state law enforcement officers investigating a child pornography case failed to create a proper forensic image of the suspect's laptop and the laptop stopped functioning while it was in the possession of law enforcement. The defense raised a spoliation issue and the laptop was subsequently suppressed and thus could not be introduced at trial. The case was dismissed. *See* The Times Herald Record, June 10, 2015, *Man Dismissed of Child Pornography Charges, available at* http://bit.ly/1GhRcdJ.

5. For example, in the recent *Silk Road* trial in the Southern District of New York (SDNY), discovery included over six terabytes of data. In *United States v. Budovsky,* another SDNY prosecution, news reports stated that discovery included over 52 terabytes of data. *See* Bloomberg News, Oct. 14, 2014, *Liberty Reserve Founder Denies Running Black Market Bank, available at* http://www.bloomberg.com/news/articles/2014-10-14/liberty-reserve-founder-denies-running-black-market-bank. ■

About the Author

Joshua J. Horowitz's national practice is concentrated on criminal defense matters requiring expertise in technology and computer software. He has served as the technology lawyer on the defense team in multiple federal cybercrime prosecutions, including the *Silk Road* case *(United States v. Ulbricht,* SDNY).

Joshua J. Horowitz
50 Broadway, 27th Floor
New York, NY 10004
212-203-9011
Fax 716-535-1686
E-mail joshua.horowitz@techlawny.com