Why having the Technical and Legal knowledge is important in the Computer Forensics Field

Matthew Ferry

DeVry University

**Abstract:**

This paper provides a brief look into three issues within the Computer Forensics Industry: maintaining the chain of custody, maintaining data integrity, and other common problems. Each issue will also try to explain why it is important for someone in the Computer Forensics field to have both technical and legal knowledge.

Why having the Technical and Legal knowledge is important in the Computer Forensics Field

An employee for a local company goes out for lunch one day. When he returns, he notices extremely long and somewhat panic-stricken faces. After a brief inquiry as to what has happened he is informed that the company had just been notified that their network system had been hacked, and that the investigation was already under way to determine exactly how, and why this happened, as well as who was responsible and what information was compromised or stolen. A computer forensics team shows up and begins to collect evidence. A short while later, the management staff addresses the employees that need to know and informs them that the computer forensics team knows exactly what they are doing and will catch the people responsible. Many months pass, a suspect is found, arrested and prosecuted. However, during the course of the trial it is revealed that evidence was not collected or analyzed properly by the computer forensics team making that evidence inadmissible, and without more, untainted evidence, the suspect walks free with a sly grin on his face.

The above is just a hypothetical case, but how often does this type of scenario play out in the computer forensics world due to a lack of technical and legal knowledge? The fact that the possibility for this to happen exists is one of the main reasons why having both the technical knowledge and the legal knowledge is extremely important. Without that knowledge the collection and examination process of evidence could be hampered, or even destroyed. Unfortunately, trying to define the required technical and legal knowledge is extremely complicated, because in the field of computer forensics they are extremely intertwined. Considering this, perhaps the best way to define this is not by trying to define technical and legal knowledge individually, but by defining how technical and legal knowledge affect computer forensics in the aspects of maintaining the chain of custody, ensuring the integrity of data, and preventing other common mistakes.

According to an article on the American Bar Association website Law Practice Today entitled “The Dangers of Do-It-Yourself Computer Forensics,” the number one danger to Computer Forensics is that of a “weak or non-existent chain of custody” (Shirk, 2007). Many people may see this as a lack of legal knowledge because the chain of custody is almost solely dealt with within our legal system, and they would not be wrong. However, failure to maintain the chain of custody can not only result in evidence being inadmissible, but once the chain of custody has been violated it taints any other form of examination that may have been performed on that evidence  and could potentially cause the credibility of the examiners to be questioned as well. In an article on informit.com Scott Lalibert and Ajay Gupta provide an excellent example of the seriousness, and type of detailed efforts that are required for evidence collection and maintaining the chain of custody from their book “DEFEND I.T.: Security By Example.” In their example, they explain that when they seized a computer system or device that a chain of custody form had to be filled out and signed by all involved parties. Once secured, the seized computers were not just protected by a locked door but also by a surveillance system that was turned on whenever there were less than three people in the room (Lalibert, 2004). This type of attention to detail  demonstrates that protecting the chain of custody is not just about the legal knowledge to know that maintaining the chain of custody is important, but also the technical knowledge to know what other technology may be needed in order to ensure that there are no chain of custody gaps that can be questioned. This is important because insufficient chain of custody logs create time periods where the evidence is unaccounted for, which creates an issue for the courts. If there are flaws found in the chain of custody, then the courts cannot be sure that the integrity of the evidence has been maintained.

Aside from maintaining the chain of custody, the one question that must be answered with an undeniable affirmative in order for any digital evidence to be useful is “Is the data that is being presented as evidence the same data that was found on the seized device?” This means that analyzing the data must be done in a very methodical manner, because without a methodology and proper procedures, something could potentially be changed or damaged. This is a very good reason why “Spoliation and Tampering” is the second issue listed on “The Dangers of Do-It-Yourself Computer Forensics” (Shirk, 2007). Most people that consider themselves “tech or computer” savvy do not usually consider that every moment that a computer or device that has a computer chip is being used that data on that device is constantly being changed. Instead they think of digital data that changes as something that happens when they add, delete, or modify a file; but, so long as they don’t make any changes to the information that is contained within that file that no changes have been made. This is simply not the case, merely opening a file to see what the file contains changes information on the computer about that file (such as the last modified date or last accessed date) (Shirk, 2007). This information, as extremely insignificant as it may seem, becomes very critical during a computer forensics investigation. The significance of this is that if a file was last opened or modified after the evidence had already been seized, and presented as original evidence, then it could be argued that that data was planted or altered and that we have no way of truly knowing what information was on the evidence at the time of being seized. Thus, it is a matter of legal knowledge to know that if data integrity is compromised it is not just a matter of “a minor mistake was made,” but also a matter of “this case could have just been lost.” This is also a matter of technical knowledge because the examiner needs to know how to safely access and document the data and its integrity so that when that integrity comes under question that the answer can be given that the data “is the same data that was seized.” However, even knowing this, it does not prevent other mistakes from being made that can be just as detrimental to a computer forensics case.

No one likes to think about mistakes being made, especially when it comes to mistakes that could affect the outcome of a court case, however this does not change that fact that we are human and mistakes will happen. Thus, the best way to prevent them is to understand how they happen. The issue of mistakes being made, is also the third and fourth reasons on “The Dangers of Do-It-Yourself Computer Forensics” as careless mistakes made by lawyers, and overlooked data(Shirk, 2007). This also corresponds with another article that was written by Setec Investigations for the webpage Forensic Focus, when they list their issue number one as that of “ignoring electronic information or attempting discovery of it in a disorganized manner”(Investigations, n.d.).

Both of these articles indicate that in order for electronic data to be discovered and used properly that the discovery process must be done in a methodical and thorough manner. If the discovery of evidence is not done in a methodical and thorough manner every time, then eventually, something will be missed. Taking a closer look at the careless mistakes from lawyers, by those that fall into this issue, it is seen that it is really an issue of not understanding that important data can be overlooked either intentionally or unintentionally. It is not just a matter of the client not forwarding information because they do not want to incriminate themselves (Shirk, 2007). It is also a matter of information that does not get discovered because someone considered it “not relevant” that potentially did not have the technical or legal knowledge required to make that determination.

This type of mistake shows a lack of technical knowledge because it potentially limits the sources that a lawyer has available to them. Even in the extremely rare case that a client forwards the lawyer everything that the lawyer asks for, by not using a professional examiner the lawyer essentially restricts the information that is made available for the case to only the information that he requested, or from sources that had been thought to check. This also shows a lack of legal knowledge, because it shows a lack of focus on the importance of digital evidence, and making sure that everything that could potentially be evidence within the bounds of the case is analyzed and considered. This means that that lawyer has potentially left the case open to be blind-sided by information that should have been known.

Of course, this issue does not just exist because lawyers make mistakes, but it also exists because examiners can make mistakes by limiting the scope of a warrant, or in the process of executing a warrant, not recognizing digital media devices properly. This could be anything from not collecting external hard drives, to missing CDs or USB thumb drives (Shirk, 2007). USB thumb drives can be particularly tricky, because they come in so many unusual styles. The social media page of pinterest has an “Unusual USB Flash Drive” page, that has images of USB drives as common as a tiny soccer ball, to incredibly unusual such as a strawberry (Pinterest.com, n.d). And while CD’s and DVD’s are fairly common these days, because of that commonality it is possible to hide or store these in locations that would not considered to be common, such as inside a book, or even inside a movie DVD case possibly under legitimate DVD’s. Knowing that these devices exist, and that it is extremely easy for these items to be hidden almost in plain sight, it becomes equally important for computer forensic examiners to be on the lookout for anything that could potentially be a USB drive, or location that could store a CD or DVD without damaging the disk. That innocuous looking miniature guitar, or CD spindle or case may actually contain digital media that stores data vital to the case that is being investigated. While this is only one example of an area where key data could be missed, and it may seem simple to check for digital media in these types of locations, when data is missed in this manner, it shows a lack of technical knowledge, and reflects a lack of focus on the importance of potential evidence, and making sure that everything that could be evidence within the bounds of the warrant is considered as potential evidence and appropriately seized and therefore available for analysis. It also demonstrates a lack of legal knowledge for almost the very same reason, with one important difference. Not only was the evidence missed, but it may also present the opportunity for that evidence to be destroyed that would not have existed otherwise, and could actually result in fines or other penalties for not preserving data (Investigations, n.d.).

While there are other issues not presented here that could affect the outcome of a computer forensics investigation, these issues are some of the most important. The last thing that an investigator should want to hear is that a case that they have worked on, or are working on has been severely set back, or even worse, dismissed, due to mistakes made during the investigation process. These three issues of maintaining the chain of custody, ensuring that data used for evidence has not been spoiled or tampered with, and preventing other common mistakes such as missing digital evidence, all show why it is important for a computer forensics investigator to have both the technical and legal knowledge. Without one or the other, it becomes exponentially more probable that something will be missed, or a mistake will occur that will detrimentally affect the outcome of the case that they are working on.

**References**

Investigations, S. (n.d.). *Learning from Other's Mistakes: Issues Arising from Electronic Discovery*. Retrieved April 05, 2013, from Forensic Focus: http://www.forensicfocus.com/electronic-discovery-mistakes

Lalibert, S. &. (2004, October 01). *The Role of Computer Forensics in Stopping Executive Fraud*. Retrieved April 03, 2013, from informIT: http://www.informit.com/articles/article.aspx?p=336258&seqNum=3

Pinterest.com. (n.d). *Unusual USB Flash Drives*. Retrieved April 05, 2013, from Pinterest.com: http://pinterest.com/jademcdade/unusual-usb-flash-drives/

Shirk, E. (2007, November). *The Dangers of Do-It-Yourself Computer Forensics*. Retrieved April 04, 2013, from Law Practice Today: http://apps.americanbar.org/lpm/lpt/articles/tch11071.shtml