New Challenges in Teaching e-Forensics Online

Professor Eamon P. Doherty, CCE, CPP, SSCP
School of Administrative Science, Fairleigh Dickinson University, Teaneck, USA

Abstract - This paper discusses how the topic of forensic imaging has changed because of the introduction of a new technology known as the solid state drive (SSD). The differences between the SSD and the magnetic disk hard drive are also discussed. This paper highlights the importance of online education for teaching e-forensics, how it is delivered, and why it is important for educating certain populations who cannot get to a traditional classroom. Lastly, this paper also discusses the need for a conference among many stakeholders to create a publically known standard, perhaps an ISO standard, for the SSD and why it would help for court cases involving the imaging and investigation of SSDs.

Keywords: Computer Forensics, Cyber Forensics, Computer Security

1 Introduction

Teaching computer forensics online is very important since many policeman and National Guardsmen often have unpredictable work schedules and cannot attend in person classes [1]. Online learning is also the only option for those students who want to study a very specialized topic such as e-forensics when they are deployed with the military and cannot travel freely. Creating a forensic image or a clone of a hard drive is considered by some authorities to be the most important task in computer forensics. The forensic image is a byte for byte copy of a suspect's hard drive. It includes both the used and unused space. A backup is only a subset of a forensic image because a backup only includes the files with data and not the unallocated space or “empty space” where remnants of evidence can be. Forensic examiners need to look at both allocated and unallocated space for exculpatory evidence to find someone innocent, not just guilty. If an examiner only has a backup, a defense attorney might create some doubt that some exculpatory evidence, finding his or her client innocent, resides in unallocated space. This is one concept that is important for new students of e-forensics to learn. There should also be an identical SHA-1 or MD5 hash of the forensic image and the suspect’s hard drive or storage device which verifies that the image is a perfect clone of the suspect’s drive. All experiments to produce evidence on the cloned image drive should also work on the suspect’s drive. It should become obvious how important the forensic image has become in digital forensics. It is also common knowledge among people that hold a CCE (Certified Computer Examination) that some digital forensic examiners can have a career working for private investigators and lawyers while only specializing in the forensic imaging of hard drives. Therefore the forensic imaging of hard drives is a subject of great importance to anyone who teaches e-forensics. Two popular digital forensic tools that can be used to create a forensic image of a disk and provide a hash function for verification purposes are SMART from ASR Data Acquisition & Analysis and Winhex from X-Ways Software Technology AG [2].

This paper will discuss how one university has used online learning to teach the forensic imaging of hard drives in its computer forensics classes. In the last two decades the hard drives that have been encountered have been those with magnetic platters and read write heads. The methodology of forensically imaging these types of drives has been well established and has been accepted in many court cases. When an investigative technique and set of tools have been accepted by the legal community, the academic community, and practitioners, it is said to have passed the Frye Test.

The challenge to the established methodology of the forensically imaging of hard drives is the introduction of a new technology known as the solid state drive (SSD). These hard drives may have over twenty computer chips on their circuit board instead of platters with read write heads. Many of these drives also have proprietary algorithms and technology so that it is not possible to know where the data lies on the drive. The drive size or storage capacity is not constant and dynamically changes as blocks are labeled bad and no longer used by the operating system. There is also a garbage collection program that runs when the solid state drive is powered. This means that part of the drive may be deleting evidence while the computer forensic technician is simultaneously collecting evidence on another part of the hard drive. The challenge is further complicated by the various manufacturers of solid state drives who each have their own methods of storing and deleting data on the solid state drive. This means that computer forensic educators need to invite computer forensic practitioners, SSD manufacturers, and attorneys to create a national or international conference to discuss the framework of how to forensically image the solid state drive and have the image be accepted for use in a court case. If a set of tools and methodologies for imaging a solid state drive could be developed and accepted by the academic, legal, and practitioner communities, this would be a big breakthrough for computer forensics. It would also mean that computer forensic examiners would have a set of tools and
methodologies to pass the Frye Test. “Citing Frye v. United States, 54 App. D.C. 46, 47, 293, F. 1013, 1014, (1923), the court stated that expert opinion based on scientific technique is inadmissible unless the technique is generally accepted as reliable in the relevant scientific community [3].” Having a set of standards for SSD technology would also mean that educators would be able to develop a new online lesson and allow students to learn how to image the solid state drive and get a MD5 hash that is the same for the suspect’s drive and the newly created image for use in a computer forensic examination. This standard would have a high probability of passing the Frye Test and be useful to students who are eForensics practitioners.

2 Teaching Forensic Imaging Online

Fairleigh Dickinson University (FDU) has two classes that discuss the process of forensic imaging. One class is called MADS 6697 Current Issues in Cyber Forensics. The other class is called MADS 6637 Computer Seizure and Examination. Both classes are often taught in a traditional classroom, but are also taught online. Many students will self-identify themselves as policemen that live in rural areas and cannot easily attend the main campus. Some of these policemen and policewomen work the night shift or rotating shift thus making the online learning environment the only feasible solution to advance their education. Other students will self-identify themselves as national guardsman that were deployed in a place such as the green zone in Iraq or abroad. It becomes obvious that online learning is a feasible option for those in a war zone where commuting safely to a classroom is not possible. Some students in these classes often self-identify themselves as unemployed and seeking a career change. Online learning can be a good option for those who cannot afford the high price of gasoline for commuting to school faraway and for those who cannot take public transportation from their home to the university.

The students start by registering for their class, paying the tuition, and then getting their books. They are next given a username and password for a class such as computer seizure and examination. The class is conducted in FDU Webcampus and uses the online educational program known as Blackboard. Each week consists of activities such as textbook readings, reading course documents, and participating in a discussion board where students interact among themselves as well as with the professor. There are also course links where students can access video or Microsoft PowerPoint slides on topics such as forensic imaging. There are many YouTube videos on the subject of forensic imaging of hard drives. These films are produced by academics, practitioners, students, and commercial product vendors. These films show a variety of tools and techniques to forensically image a hard drive and verify the results. It is important to first verify which people, tools, and techniques are credible before presenting them to the students. The student will begin his or her knowledge of the hard drive by reading about the hardware such as the read-write heads and the platters that are used in the traditional magnetic platter hard drives. Chapter fourteen of the sixth edition of Operating System Concepts by Siberschatz, Galvin, and Gagne are a good source for teaching students the subject of mass storage structure and I/O scheduling [4]. The student then reads about the operating system and such concepts as the file directory, the file allocation table (FAT), clusters, and chaining. There is a body of literature that is well established about how magnetic platter hard drives store, retrieve, and delete information. The course documents for the class contain text, pictures, and links to vetted online videos. The education of how the hard drive works and how it can be forensically imaged applies to new hard drives as well as classic hard drives such as the Seagate Technology Model ST-412 with a capacity of ten megabytes. Figure 1 shows a full height ST412 hard drive on the right. It was partitioned into two logical drives of E and F. It is much bigger than a more modern common hard drive such as the Western Digital hard drive with an eighty gigabyte capacity which is also pictured in figure 1. It is important to teach students that evidence can appear in logical drives or in a hidden partition between the two drives.

The next step is to teach the students how to create a forensic image of a magnetic platter hard drive. The simplest method is to start with a piece of hardware to wipe a hard drive and then duplicate the hard drive of a simulated suspect’s hard drive to the wiped hard drive. Some hard drive duplicating equipment has an option for wiping a hard drive. This means that each byte of a hard drive is written with a pattern of zeroes so that there is no doubt about malware or evidence from another case being on a hard drive that will later contain the forensic image of the suspect’s hard drive. The Logicube Solitaire Hard Drive Cloning Device Duplicator is one of many viable options for people with or without a technical background. This device simplifies the forensic copy/imaging process. The suspect’s hard drive is connected to the outside of the Logic Cube device and the wiped drive is connected inside the device [5]. Some menu buttons on the Logic Cube are selected and the
process of forensic imaging begins until completion. A printer may be connected and a report about the MD5 hash can be printed.

Figure 2- The Logic Cube Equipment

Another method of teaching students to create a forensic image of a suspect’s hard drive involves changing the bootup order of the devices in the bios. The bios settings can be changed so that the system first checks the CD drive, floppy diskette drive, or a flash drive for an operating system or bootable program. Then a CD with a program such as Helix 2 can be booted up so that a forensic imaging program is run. This will prevent the operating system on the subject’s hard drive from booting up and changing access times and file dates thus potentially compromising the evidence and having it suppressed as possible evidence in court. Once a program such as Helix 2 or Access Data’s FTK Imager is run, then the forensic image of the hard drive can be made through a USB storage device that is connected to the suspect’s USB port. This technique is taught online by the use of text, PowerPoint slides, and a video. Once the forensic image of the simulated suspect’s hard drive is created, the MD5 hash of the suspect’s magnetic platter hard drive can be compared to the forensic image thus insuring a perfect match for examination purposes.

3 Issues Concerning a SSD

Scott Moulton, a computer forensic practitioner and speaker, says that the solid state drive (SSD) device is becoming more popular because it runs quietly and extends the time that one can run the laptop with only the battery as a power source [6]. He also says the device is popular because it weighs less and produces less heat than a conventional magnetic platter hard drive. It appears from the speech that there are not identical standards among all the various SSD makers and it may limit the forensic examiner’s ability to get to all parts of the drive to access potential evidence. Scott also said that there are times when the SSD is powered on and quietly running, the garbage collection is moving data, and also zeroing out unallocated space [6]. He also discusses occasions on small consumer grade memory sticks when the device marks cells as bad and the storage capacity is not as large as it was [6]. Bell and Boddington, two writers for the Journal of Digital Forensics, Security, and Law, say, “Put simply: the SSD technology which is replacing magnetic hard drives is neither simple, well understood, nor homogenous; rather it is complex, poorly documented, and highly heterogenous. [7]” Bell and Boddington then further state, ”Worst of all, it is active – that is to say, the SSD may act under its own initiative, and may undertake quite remarkable (and highly evidence-destructive) actions even in the absence of write commands from a computer, potentially regardless of efforts by police and forensic analysts to prevent invalidation of evidence [7].” From our previous discussions of forensics, it appears that this set of changes leaves a possibility that a defense lawyer might suggest that there is no guarantee that the tampering of evidence did not occur.” It then becomes evident that manufactures should develop a set of standards about how data is stored, deleted, and repositioned on a SSD drive. The manufactures of SSDs may need to be approached by various governments and representatives of various legal systems to consider the redesign of these drives in the interests of the safety of the world community. Some attempts to add security features to technology to stop counterfeiting of US currency for example have been adopted whole heartedly by the printer industry. The color laser printer industry has added a technology that allows the serial number of the printer to be embedded in the paper. This feature when combined with a special purple light, allows the United States Secret Service the ability to know what printer a counterfeit United States currency note was printed on. However; other previous attempts by the United States government to change technology manufacturing for purposes for national security have not always been successful. The inclusion of a clipper chip in technology is one example of a good security precaution that failed miserably. In 1994, the New York Times reported this about the clipper chip, “The Administration's goal was to make it easier for law enforcement officials to conduct legal wiretaps on new generations of devices that send information over the telephone system, including wireless phones, computers and facsimile machines [8].”

4. Teach Best Practices of SSD Imaging

There is a possibility that the computer forensics community and legal community may have passed a golden age of forensics where it is consistently possible to get an exact forensic image of a solid state drive with MD5 verifiable results. If the manufactures do not disclose how their FTL Flash Translation Layer maps blocks of data from an abstract data structure to real SSD locations on the SSD, and how to cease the garbage collecting of data when performing a forensic image of a SSD, then a “best practices for SSD imaging” may be the best option that the e-forensics
profession may obtain. A similar issue has arisen with some mobile devices that also compact space, reduce fragmentation, and do garbage collection. A best practices for SSD e-forensics may be to have a guideline for tampering such that if the possibility of tampering is suggested, the data in question may have to be verified by both parties in litigation.

Bell and Boddington wrote about a series of controlled experiments that measured the amount of data loss with SSDs [9]. The experiment that showed the least spoilage of data occurred when the machine was immediately shut down after a destructive process and a Tableau write blocker was installed on the hard drive while it was turned off. The solid state drive was then turned on with the write blocker in place. A forensic investigation showed less than a one percent loss of data. Perhaps the installing of a write blocker on a dead system might be a consideration for a best practice.

5 Soliciting a Solution from the eForensics Student

The e-learner is very often an adult learner with many years of practical experience in law enforcement, the military or private security. He or she may only be in class to provide an audit trail for the knowledge that he or she gained informally in the work world. It would behoove the professor to use webex or another group conferencing technology to solicit a solution to obtaining a consistent verifiable forensic image of the SSD. Skype also has a group feature that allows multi-party VSee is a videoconference program that has had some success in Louisiana and could be considered for a small conference on the subject. It is possible that group discussions over time with various students could lead to a solution.

6 Encouraging the Use of Free or Low-Cost Tools

The e-learner may not always be able to afford many of the pricey eforensics tools that corporate investigators and law enforcement personnel may use. Rather than widen the digital divide, one should always provide an option for e-learners to use tools that can be downloaded and used for free such as Access Data’s FTK Imager and some of the early versions of e-forensics’s Helix as shown in figure 3. Students can get practical experience and learn valuable new concepts by downloading free or low cost tools to practice the forensic imaging of hard drives, SD cards, and SSD drives. The practice may also enhance their confidence in using these tools and help convince a future employer of their abilities while discussing them in a job interview.

Some students have reported that they like using eFense’s Helix because it comes on an ISO image that can be downloaded and put on a CD. If the bootup order in the BIOS starts with a CD, then the student can bootup without changing the hard drive and then use the ‘Live Acquisition’ tool to create a forensic image of the hard drive. The source is chosen. The destination drive such as a USB SSD drive can be selected after it is plugged in. Then a student can also name the image file and use a common file extension such as dd. The icon of a camera on the left side of figure three is an easy way for students to get information about the system’s hardware and obtain any IP address if it is connected to a network. There is also documentation. Students who are comfortable with a tool can also seek newer versions of software that cost money when they have employment.

7 Conclusion

Magnetic hard disks are well understood and the forensic imaging and examination of these drives has become an established science that is accepted in court cases. The introduction of a new technology known as the solid state drive (SSD) has produced some concerns among digital forensic investigators, students, professors, attorneys, and the legal communities. These sets of heterogeneous devices behave in an unpredictable manner and have some aspects of their operations cloaked in a shroud of secrecy. This makes it difficult to consistently forensically image a solid state drive and get a MD5 hash that matches for both the suspect’s drive and the imaged drive. Therefore it may be necessary to get the manufacturers, academics, practitioners, and the legal community together to create a series of best practices or modify the design of the device so that it may be forensically imagined with consistent results and examined easily for use in a digital forensics examination.
8 References


