Moving Legacy Device Forensics to an Online Format

Professor and Cybercrime Training Lab Director Eamon P. Doherty CCE, CPP, SSCP
School of Administrative Science, Fairleigh Dickinson University, Teaneck, New Jersey
Ester G. Doherty, M.A.S, Fairleigh Dickinson University, Teaneck, New Jersey
Elly Goei M.A.S, Fairleigh Dickinson University, Teaneck, New Jersey
Doherty@fdu.edu, FDU, H-DH2-16, 1000 River Road, Teaneck, NJ, 07666

Conference : EEE2014

Abstract - In 2013, there are still many occassions when outdated media must be examined for insurance purposes or in corporate policy investigations or criminal investigations. This paper discusses the need for teaching legacy media forensics and gives some specific examples of media that needed to be examined. The paper also proposes a model of how the subject may be taught in person as well as online. The paper shows the reader a combination of technical topics, legal topics, and educational topics.

Keywords: Legacy Device Forensics, e-Forensics, Online Learning

1 Introduction

Some people say that the pager has been replaced by the smartphone and that pagers have become extinct. However, this is not true. Glenn Bischoff, a writer for “Urgent Communications,” states that 3.5 million pagers are in use in the United States in 2012 in the public safety and health care industries [1]. Pagers often get a message almost instantaneously while text messages to cellular network customers take two to three minutes and are limited to 130 characters. A three minute delay in a message can make the difference or not in being able to save lives and property from the destructive forces of fire. Insurance investigators may sometimes ask to examine pagers to see what was known at what time and to learn when people responded. The restaurant industry also relies heavily on pagers. There is still a need for examining pagers.

An adjunct professor, who also a full time police detective, once told Dr. Dohery and a class at Fairleigh Dickinson University (FDU) that he arrested someone with a large piece of plastic containing pockets which held CDs with child pornography on them. The plastic was rolled out and hidden between a box spring and mattress. The story demonstrates the need to know how to examine a CD. If the CD is scratched and not readable, then it is important to know what tools are available to recover the text, videos, and graphics on a CD or DVD. Many people are also unaware that there is so much diversity in the formats of the CD and DVD. Here is a partial list of the formats that an examiner may encounter: “CD-i, VCD, SVCD, SACD, CD-ROM, CD-ROM XA, CD-R, CD-RW, CD-MRW, DVD-ROM, DVC, DVD-RAM, DVD-R, DVD-RW, DVD+R, DVD+RW, DVD+MRW, DVD+R Dual Layer, DVD-R Dual Layer, DVD-RW Dual Layer, DVD+VR, DVD+VRW, DVD-VR, DVD-VRW, DVD-VM, DVD-VFR, BD-ROM, BD-R, BD-R DL, BD-RE, BD-RE DL, BD-R SRM, BD-R RRM, BD-R SRM+POW, BD-R SRM-POW, BDAV, BDMV HD DVD- ROM, HD DVD-R, HD DVD-R DL, HD DVD-RW, HD DVD- RW DL, HD DVD-RAM, HD DVD-Video [9]”

There are also occasions when old computers and media are put out for garbage and then scavenged by people looking for a free system for family members and friends. There was one story of this relayed to the professor in class. The student in a continuing education class was a policeman and said that he received a report from a scavenger who picked up a system next to the garbage with child pornography on it. The system was antique and had a 5.25 inch floppy drive and a large full height hard drive. A report was made and a search warrant was obtained for the address of where the system was obtained. When the search warrant was executed, a computer seizure and examination was performed. More child pornography was uncovered on a new system and some obsolete media was also seized. It becomes obvious that there is a need to be able to examine obsolete media as well as new hard drives and media. Let’s suppose that some media was not able to be examined. Wouldn’t it be possible that a defense lawyer may try to create a doubt in a jury by stating that there may be exculpatory evidence exist in the unexamined media? If one member of the jury has a doubt, then there may not be a conviction. This scenario reinforces the case for being able to examine all the seized digital media from the crime scene.

In 2009, Dr. Doherty was approached by a leader of a credit union asking for help in imaging and accessing the data on an eight inch floppy diskette. The disk was from the 1970s and was believed to be the sole source of information about the beneficiary to an insurance policy. After a great amount of unsuccessful effort, Dr. Doherty could not obtain the
hardware and software to perform such an operation and referred the man to Kroll OnTrack Systems [2]. It became obvious that the need for such training on how to recover that data was evident. In the fall of 2013, a continuing education student had said in class that he and his son were going to specialize in investigating legacy media and devices. The man had spent all his adult life in computing and his son is a defense layer who is looking for a specialty to increase his workload. Legacy devices and media were perceived by them to be a less profitable specialty that was overlooked by the larger investigation and law firms. The father of the defense lawyer said that the classes on various legacy media topics should be taught both in person and online. He said that in person classes were good to get the hands-on practice. He also said that online classes that included short videos with supporting text would be good for his son who lives far away and often has to go to court on short notice.

In 2011 and 2012, Dr. Doherty and Elly Goei researched how to obtain data from 100 MB zip disks, 250 MB zip disks, and from jazz disks. They obtained the hardware for those disks and performed an examination of the data for a colleague. The data was then transferred to a USB flash drive and a verbal report of the contents was given. All these situations are just some of the examples of the need for teaching people about the policies, procedures, and special techniques for examining legacy devices and media.

2 Teaching Legacy Device Forensics in Person

Dr. Doherty created and taught a legacy device and legacy media class for the FDU Digital Forensics Special Interest Group which is made up of a wide range of people in the FDU community. The class was expanded from one hour to three hours and taught for FDU’s Continuing Education Department. There were many people that had an interest but could not attend because of work commitments, heavy traffic, and the cost of travel. The class included a variety of hardware that was obtained from eBay or discarded by acquaintances of Dr. Doherty. The class was divided into sections. Each section discussed a type of media or legacy device, its characteristics, its history of usage, and a methodology of how to recover the data from it. There was also a discussion of the chain of custody, The Frye Test, Voir Dire, The Fourth Amendment, Search Warrants, and some legal concepts such as “Fruit of the Poisonous Tree.”

3 Porting Specialized Classes to Mooc

An administrator at the school said that the class could easily be ported from an in person class to one that is online. The administrator said that the class would be a good candidate for being a MOOC. An online class or MOOC could follow the same format. The history of each legacy device such as the pager could be discussed, it peak years of usage, and the number of people still using such devices. Then the various models of such devices and the companies who made such devices could be discussed. There could be a couple pages discussing the file systems and URLs of places where online user manuals could be obtained. There could also be video showing the student how to use tools such as the Paraben Project-A-Phone to photograph screens. Many of the videos needed already exist on Youtube or SecurityTube so further production of video is not always necessary. The online instructor would only need to provide a link to an existing video with relevant quality content. If the tools and techniques for digital evidence seizure and examination were law enforcement sensitive, then the student would be referred to places such as Teel Technologies who teach a JTAG and chipping forensics class. JTAGs have to do with an interface within electronic devices that are used for quality assurance and testing circuits. They can also be used for probing chips and obtaining data [3].

The digital media can also be taught using the same methodology. A picture of the digital media such as the eight inch floppy drive is shown. The history of the media and its years of manufacture and peak years of usage is discussed. The formats, file systems used, and other pertinent data is discussed. Then the chain of custody and the preservation of evidence using Faraday Bags and shielding from heat and magnetic waves are discussed. Lastly tools such as DriveSpy by Digital Intelligence and other tools such as Access Data’s Forensic Toolkit are discussed. Classic subjects such as data hiding and steganography are discussed using text and video.

Lastly, the types of hardware that can be interfaced with modern computer systems are discussed. There are many vintage computer hobbyists who have recently created hardware and customized software to help people adapt mainframe eight inch drives to the computer. The Shugart Eight Inch Drive was originally made as a peripheral device for IBM Mainframe computers [4]. However, there is now a power supply board and interface kit that provides most of what someone needs to connect an eight inch drive to a personal computer www.dbit.com. There are many types of eight inch disk floppy drives available for sale on eBay. There is also a lot of documentation and boards for sale online that allow people to connect these floppy drives to modern computers. The Mitsubishi M2896 - 63 - 02M, Caldisk 142M, Shugart 801, Shugart SA850, Shugart 851, The Tandem Eight Inch Drive, The Memorex 550 Eight Inch Drive, and the DEC were just some of the eight inch floppy drives available on eBay in December 2013. All the technical manuals were available somewhere online and included detailed information on the power requirements and
interface cables too. Vintage computer clubs and hobbyists have made sources of documentation available for obscure media devices. The three authors visited the InfoAge Museum in Wall, New Jersey in 2012 and the people at the computer museum offered to help read any eight inch floppy diskette as well as help with any obsolete media needs.

When a thick eight inch by ten inch hard plastic diskette is encountered, there are other options such as using the IOMEGA Disk Cartridge System which contains a full length ISA card, cables, and eight inch Bernoulli Drive that can be connected to computers such as the HP Vectra that have room for ISA cards and contain USB ports. In figure 1 we can see a picture of obsolete media and various drives on a homemade system (HP Vectra) made from discarded computers and peripherals. The cover is off the unit so that more hardware is visible. Covers are very important to help prevent any shock hazards.

Figure 1 – Obsolete Media and Homemade Forensic PC

4 Dangers of Legacy Environments

In the 1990s, Dr. Doherty worked for Morris County ISD in Morris County, New Jersey and fixed computers, printers, and did a variety of data recovery work. There was an occasion where he was once called to fix a system that consisted of a PC connected to an IBM Quietwriter Printer. Dr. Doherty’s tie was not clipped and got caught around the roller of the printer. His face was pulled closer until it lay on the printhead of the printer. The customer perceived a possible choking hazard and pulled the plug on the printer. Another danger that was potentially lethal was from the spinning rotisseries of the decollators getting caught on a person’s tie. The decollator was used to separate three paper into three separate collated and folded identical stacks of paper. This topic was discussed by Dick Brandon in a 1973 Computer Security Handbook [5]. Some devices have high voltage inputs and need to be handled carefully. Please consider devices such as the Shugart drive include three different voltages with the highest being about two hundred and twenty volts. Many PC examiners and hobbyists are used to working with a power supply whose output is five volts. Dick Brandon also discusses accidents from high voltage [5]. Such topics are seldom if ever mentioned in computer forensics or computer security academic materials in 2013 but in our opinion should be. This should be included in a MOOC or online class.

5. The Forensic Recovery Evidence Device (FRED)

Fairleigh Dickinson University (FDU) has a FRED Forensic Recovery Evidence Device. This device is made by the corporation known as Digital Intelligence and is used by many computer forensic investigators. There are many variations of the FRED such as the FRED Sr., FREDC, and FREDDIE [6]. The FRED Sr. can be used to examine a multitude of media types. A computer forensics adjunct who is now a retired computer crimes detective once showed a FRED station in his in person class at FDU. The value of such a device is discussed in chapter 6 of “Guide to Computer Forensics and Investigations” [6]. The FRED unit is also important because it has a write blocker and can be used to examine SCSI devices. It also contains a Firewire IDE interface with a write blocker. It is important to stress that such devices can be used to collect evidence and preserve it. A short video of the capability of such a device should be included in an online class or MOOC.

6. General Legal Concepts

It is important that the students learn about concepts such as the Spoliation of Evidence, Fruit of The Poisonous Tree, The Frye Test, and the Daubert Standard. Any MOOC or online class should emphasize that evidence from an improperly conducted investigation can be suppressed if it was not protected from being tampered with or if pirated software was used to obtain the results. The Fruit of The Poisonous Tree is a legal concept in the United States that relates to evidence being suppressed if it was the result of improperly licensed or pirated software. FDU is located in the State of New Jersey and it is Dr. Doherty’s opinion that students should read a legal paper on the topic of spoliation of evidence by Lawrence Berezin ESQ. This paper called, “The History of Spoliation in the Courts of N.J.: TARTAGLIA v. UBS PAINENWEBBER INC. 961 A.2d 1167 (2008) 197 N.J. 81 [7].” The paper is an important topic and may help emphasize the need to preserve evidence, handle it properly, and make it available to the correct people in the discovery process.

The Frye Test is important because students need to make sure that they are using proper techniques accepted by academics, the legal community, and law enforcement. Students should have a test plan of how they are going to
identify, collect, preserve, analyze, and then report the findings of digital evidence. The test plan should use practices and tools accepted by the previously mentioned communities so that it can pass the Frye Test in court [8]. It would be tragic if the results of an investigation were suppressed because the tools and methodology of the investigation were considered to be pseudo science.

7. CCTV Systems (Old & New)

Dr. Doherty created some informal classes about CCTV systems for visiting Cybercrime students and members of the Digital Forensics Special Interest Group (DFSIG) which meets once a week at FDU. Students appear to be most interested in CCTV systems and Digital Video Recorders (DVR). Most are interested in connecting the DVR to their LAN and viewing the video on their smartphone while away from home. IP cameras work well with a DVR and many systems are available online for approximately one hundred dollars. Many of the IP cameras include infrared technology and allow for night viewing. Since the in person DFSIG includes people of all ages who are interested in both new and legacy systems, some adapter/conversion equipment is introduced that allows the inclusion of old and new equipment on a CCTV/DVR system.

Some students also do some work in their community and have customers who are senior citizens with legacy security systems. Some continuing education students also work in the security field and occasionally say that they need help examining the footage from a CCTV system. The amazing thing is that sometimes the footage is from a legacy system that includes one camera and a VCR that uses a VHS tape. In 2013, there were still examples of 21 inch CCTV cameras from the 1970s and VCRs being sold on eBay. Many of these systems have a long life. These 1970 analog cameras could possibly be connected to a VCR which came on the consumer market in the 1970s. In the Eastern part of the United States, VHS was a dominant format. The problem with VHS tapes is that people use them too many times and that the resolution of the archived video is poor. Many people also use the cheapest tapes possible instead of more expensive high quality VHS tapes. This also lowers the quality of the archived video. Many people with VHS security systems do not use a cleaning tape to perform regular maintenance which also degrades the quality of the saved camera footage. There were many examples of vintage CCTV systems being advertised for sale on eBay which perpetuates the use of old systems. There are many companies that will transfer the entire VHS videotapes to a digital format on a DVD for a reasonable fee. Once the film is digitized, there are a variety of tools that can be used to magnify and enhance the video.

Students have asked how long CCTV systems have been around. They want to know the history for both their own curiosity and in case they are asked about the history of CCTV during the Voir Dire process in court. CCTV systems have been used since World War Two when German Rocket scientists preferred to watch rockets launch from a safe distance [10]. The German CCTV systems were brought to America along with German Rocket scientists and the V2 rockets in a special operation known as “Operation Paperclip.” The InfoAge Museum in Wall, New Jersey has special archives and technology exhibits related to Operation Paperclip. Many of the captured scientists were given new identities and went with the CCTV and V2 rockets to the western United States where they worked on America’s ballistic missile programs. The CCTV was then used for watching the results of the atomic testing. Students who visit Las Vegas may elect to stop at the Atomic Testing Museum on Flamingo Road to see some of the exhibits which also show CCTV cameras, drill heads, and test results. Since so much of the population travels, mentioning places such as the Atomic Testing Museum, an affiliate of the Smithsonian Museum, and the InfoAge Museum in New Jersey, offer people an opportunity to combine a leisure trip with learning. It is also worth noting that the CISSP is one of the premier network security certifications that computer science students and network security practitioners wish to obtain. A section of the CISSP exam contains some questions on CCTV cameras and CCTV systems.

8. File Systems and Formats

One of the most important topics in teaching legacy device forensics is data formats and file systems. Students should be taught to identify the type of device or media they have. They should find a brand, a model number, and look for a date. Then they can do an online search and find a picture and description of an identical device. The next step is to locate an online manual and find out the technical specifications of that device. The manual often discusses any format standards for the media or device. With media such as the eight inch disk, we may learn that it uses a FAT 12 file system. From there students can learn about file allocation tables, file names, clusters, pointers, and how files are added and deleted to the disk. This can help them recover files. Teaching students to use a disk editor can also help them look for data hidden near the MBR, master boot record, and in hidden partitions. Students should be encouraged to take a class on file systems with a local computer science department for obtaining deeper knowledge. Some eight inch diskettes such as the Memorex floppy disk used hard sectors instead of soft sectors. This gives the instructor an opportunity to teach the student about concepts in file systems that are rare but may occasionally cross an examiner’s path somewhere in their career.
9. Conclusion

It appears that there is a pattern for teaching continuing education on legacy device and media forensics. There should be a section about identifying, preserving, analyzing, and reporting what was found and what it means. Identification includes finding a model number, date, data format, and instruction manual. Then one can understand what format the data is in and how it is retrieved and deleted. That can help one in selecting relevant tools for recovery and examination. The chain of custody is an important topic because the integrity of the seized media and device needs to be documented from the time it was taken until the moment it appears as evidence in court. Students should be taught about the history of the device and be prepared for the voir dire process where they are determined to be experts in court. The Frye Test and the need for using scientific methods accepted by the legal, academic, and practitioner communities needs to be stressed. The Fourth Amendment and search and seizure concepts should be stressed. Concepts such as the Fruit of the Poisonous Tree should be emphasized so that students do not use pirated software or stolen equipment to investigate legacy devices or media. Everything that can be done in person can also be done online if detailed high quality video is included along with supporting text and suggestions for further reading. Lastly, students should be encouraged to talk to experts and see legacy systems in action at places such as the InfoAge Museum.

10. References


