Teaching Digital Camera Forensics in a Virtual Reality Classroom

Associate Professor Eamon P. Doherty Ph.D
[1]School of Administrative Science, Fairleigh Dickinson University, Teaneck, New Jersey, USA

Abstract - *A 2009 study shows that 77% of American households have a digital camera. Some of these digital cameras may be used by criminals at crime scenes to document their deeds for their own purposes or for proof of deed to collect a fee from others. Law enforcement or private security personnel may need training in how to collect existing or deleted pictures from a digital camera without compromising the data. Traditional classroom instruction demonstrating and explaining such techniques has worked well for students to the present time. However; there is a growing need for this type of training for students who are military personnel deployed overseas, foreign law enforcement personnel, and geographically diverse students with limited funds for travel. Virtual classroom instruction appears to be a cost effective solution to teach digital camera forensics to students around the globe who cannot get this training conveniently where they live or work.*

Keywords: VR classroom, digital camera forensics

1 Introduction

I am the Director of a Cybercrime Training Lab at Fairleigh Dickinson University. I often receive emails inquiring about in person and online classes with regard to the subject known as digital camera forensics. Some of the requests are from: divorce lawyers, law enforcement officers, private investigators, and people who have gone on vacation and lost all their digital pictures on their camera due to operator mishandling or hardware failure. Many of the law enforcement officers work rotating shifts and can only attend online due to the unpredictability of their work schedule.

On January 28, 2009 Kyle Schurman said "According to a recent study from the Consumer Electronics Association (CEA), 77% of American households now own at least one digital camera" [1]. People who take digital pictures often push the wrong buttons and delete pictures that are important to them. This segment of the public would like to be able to recover sentimental photos from a cruise or a relative's wedding. This process is merely data recovery.

Then there is the law enforcement investigation where digital camera evidence must be gathered without altering the evidence. Such a case may involve a murder or rape. A rapist may use a digital camera to take a picture of the victim. A United Kingdom newspaper called the Daily Telegraph reports, "Lord Judge said "a pernicious new habit has developed" and photos were often taken either to show off, add further humiliation or to blackmail [2]. Law enforcement officers who arrest these rapists need to learn how to preserve and recover this evidence from a digital camera so that they may proceed to successfully prosecute the aggressor and get justice for the victim. For small town law enforcement officers who are far away from Regional Computer Forensics Labs (RCFL), we can now see the urgency for on demand digital camera forensics classes.

Divorce lawyers often receive camera cell phones or digital cameras with pictures of the unfaithful partner's paramount. The cell cameras phones may also hold hostile text messages between husband and wife which are sometimes called "nastygrams." The lawyer needs to be able to obtain this digital evidence, process it, and prepare it for a report to use for court or arbitration.

2 Moving an in person class to a virtual classroom

In my opinion, the digital forensics class that I teach in person would work well if moved online to a virtual environment such as Second Life. Some of my students are comfortable with virtual reality (VR) and have used VR environments or have seen family members use such VR gaming environments as "Everquest" and "America's Army." America's Army is used by many young people as a recreational multiplayer online game that requires groups of people to work on a task as a team [3,4]. Many young veterans who are returning to school used an advanced version of America's Army to train and in my opinion could effectively use avatars and a virtual environment to train about digital forensics.

Let us now consider the implementation of my digital camera forensics class to a VR classroom. Students could first register online at the University continuing education website. Then they would be instructed to create an avatar in Second Life and download Second Life on their laptop. My class could meet in a Second Life private island classroom for digital camera forensics. A variety of digital cameras could be shown to the students. I could then connect a cable from the laptop to a USB write blocker. Then I could connect a cable from the USB write blocker and to the digital camera and demonstrate how no temporary files or evidence would be changed on the digital camera. This concept of using a write blocker to prevent changing the data on an attached device is difficult to do if one only reads about it or sees a picture. In the virtual classroom, I would also prepare my examination machine by running antispyware, antivirus software, and disabling all connectivity to the computer so no evidence tampering occurred.

Then my virtual teacher avatar would demonstrate how to fill out a chain of custody form that takes the evidence from the time of digital camera seizure until the time it appears in court. If the camera had Wi-Fi or Bluetooth, I would keep it in a Faraday Bag to demonstrate that I was blocking all forms of potential connectivity to other networks or devices.

Then my virtual classroom teacher avatar would use Susteen Secure View or Paraben's Device Seizure to seize and organize all the data from the digital camera cell phone. A report would be generated with all the pictures having MD5 digital signatures. The virtual teacher would burn copies of the reports on CDs for both the prosecution and defense.

The virtual classroom teacher could then demonstrate how deleted data from a standard digital camera (not a cell phone camera), can be undeleted as long as it was not written over with new pictures. This type of camera often uses a FAT file system just like the ones found in Microsoft Windows or DOS. Perhaps some basic operating systems concepts could be displayed on a virtual blackboard. The avatar of the teacher could demonstrate that when a file is deleted, the first letter of the filename in the file allocation table is replaced with a sigma. If the file is restored, the sigma is often replaced to an underscore and the operating system will recognize the location of the file and display the picture.

The virtual teacher could then give a presentation how to recover the pictures by using a tool such as RecoverMyFiles, AccessData's Forensic ToolKit (FTK), or Guidance Software's Encase. The pictures would most likely be recovered if they were not overwritten. Sometimes the thumbnails can be recovered even if the full high resolution picture is deleted and overwritten.

The students could then be given a digital camera phone and digital camera in the virtual classroom and then asked to extract the data and create a report. Then they could take a test. If the reports from the devices and the results of the written tests are satisfactory, a credential could be given. This credential could then be downloaded and printed in the student's office in the real world.

2.1 Successes with virtual classrooms in Second Life

Some schools have a mix of part time and full time graduate students. Some are first responders while others are not and aspire for a career in emergency management. Dr. Bob Berry at the University of North Carolina has had success using a virtual classroom in Second Life to teach emergency management, conduct exercises, and then investigate what mistakes were made [5]. The virtual classroom takes time to set up but students like being able to talk to one another and interact with equipment and people in this novel environment. This appears to be a good learning modality for visual learners.

I had sat in Dr. Berry's presentation about using Second Life as a learning platform to teach emergency management and conduct exercises at the 13th annual Emergency Management Higher Education Conference in Emmetsburg, Maryland. In my opinion, Dr. Bob Berry had success because he was prepared with materials to help students create characters in Second Life and encouraged them to be persistent and learn to use the avatars the characters in the virtual environment. Whether one has distance learning students using Second Life or one has a group of students using Second Life in a computer lab, it is my opinion that it is necessary to have some type of tech support to help the people get started and then have a skilled and patient teacher to conduct the class.

2.2 Moving the class to a traditional online learning environment

We said earlier that some of my students are comfortable with virtual reality and have seen family members use such gaming environments as "Everquest" and "America's Army." However; many students I teach privately said that do not know what virtual reality is and would not select a class that used it. Most of those students said that they preferred an in person class but some said that online learning a text based virtual campus such as Blackboard was acceptable.

It is my opinion that the digital camera forensics class could be a success in Blackboard if students downloaded PowerPoint slides and took online tests. They could also have a link to a manufacturer's website for downloading a trial version of digital forensic software that they could use to examine their digital camera or digital camera cell phone. After successful completion of a task and test, they could obtain and print a certificate with their name on it. A very similar type of online learning and credentialing is done by FEMA [6].

3 Teaching digital camera forensics in person

I have taught digital camera forensics in person in the Cybercrime Training Lab at Fairleigh Dickinson University in New Jersey for approximately three years. In class, we first start with a display of some of the types of digital cameras available on the market. Then students are exposed to some of the digital cameras that are commonly embedded in devices such as binoculars and telescopes. Next we proceed to digital cameras found in cell phones.

In a digital camera forensics class, we then discuss the metadata that is in the digital picture. In Windows 7, one can right click on a picture and choose the properties tab. Then one can find information on the camera type and model. If the pictures are on a read only CD where they will not be altered, a non forensic tool such as Google's Picasa 2 or Picasa 3 can be used to show us the details about the lens and focal point of the camera.

One of the techniques that has been successful in getting the students enagaged in the conversation of digital camera forensics is when I show a 1945 digital picture of F. Castro and a former student's father at Okinawa (see figure 1.). I aquire the picture from my digital camera and ask the students if this picture was from the camera. The students will say that there were no digital cameras in 1945. Then I ask how it got on my computer. A younger student will often tell me that the digital camera is similar to a mass storage device connected to a digital / optical lense and that many files other than pictures may be stored there.

Then we will examine the metadata of the picture and notice that the resolution of the picture is not supported by digital camera. Someone else with my camera specifications may say that the picture format, GIF is not supported by my camera. We may examine the metadata further and learn that there is no camera make and model but actually a scanner model. A student will ask if I have such a scanner and I will tell them that I scanned a photograph and transferred it from my desktop to my digital camera.

After the technical conversation, we often go to the non techical discussion about the picture. I ask if F. Castro is Fidel Castro or could it be Frank Castro or Francis Castro. The students then talk about how they would investigate if the picture might be of President Fidel Castro of Cuba. I ask how old is President Castro now and how old was he in 1945. Then I ask them how old does the man in the picture appear to be.

Then students ask what President Fidel Castro might have been doing in 1945. We look online at some biographies and learn that he was in law school. Then we discuss how difficult law school is and that one cannot take much time from it and it most likely is not him. Students will also note that the biographies never say he visited Japan as a young man.

Then another student may notice a wedding ring in the picture and ask if there was a Mrs. Fidel Castro. Most students never heard of one and the online biographies do not mention an early marriage. The analysis of the picture gives students an understanding that there are many things to consider about a picture and that research plays a part in an investigation.

Another student may notice that the man in the picture has a beard but that it is shaped differently than other pictures of Fidel Castro. Another student might ask Fidel might want to visit Japan.

Some students might notice that the dog tag of the man in the picture looks different than the American ones and the mystery deepens again. They wil flip back to the technical discussion again and suggest running a facial biometrics program on the picture of F. Castro against a known picture of Fidel Castro at age 19. Other students who are investigators have suggested to write to the Cuban Embassy and ask.

I feel the same picture and discussion would work well in a virtual classroom and help students discuss technical and non technical considerations.

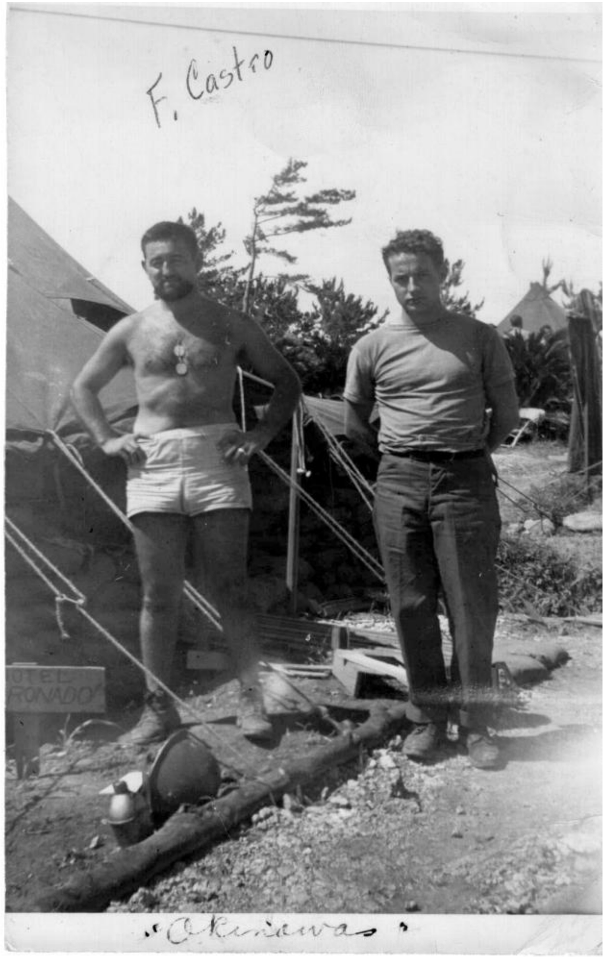

Figure 1 – F. Castro at Okinawa in 1945.

4 Credentials for the digital camera forensics teacher or practitioner

If someone is going to teach computer forensics, I would like to see a doctorate in computer science with some forensic certificates too. In my opinion, this type of teacher could go into the technical aspects of file recovery and discuss where files are stored and where parts of files may be found in the Microsoft Windows Swap File. However; a lawyer with some computer science and computer forensic training could also be a good professor because he or she could emphasize the legal aspects of examining a camera, especially if it was taken by an angry spouse without consent of the owner.

A computer crime detective with a forensic psychology doctor's degree could also be good because that person could also discuss the motivations of those who misuse digital cameras. The psychological aspect is important because it is important to know the patterns of a criminal and the mindset so that the investigator may understand the intent. Intent is an important component of crime.

I often tell people to become a Certified Computer Examiner (CCE) because it is a recognized credential in digital forensics [7]. The Microsoft operating systems that one learns about for the CCE examination uses the FAT 32 file system often found in digital cameras. This means that the file recovery techniques used for that credential can be used for the digital cameras. One should also try to find classes in digital camera forensics. One can also get Guidance Software's Encase certification which many people value for a wide area of digital forensics.

5 Suggested further education for digital camera forensic specialists

I would also suggest that people take any online or in person classes in Operating Systems and File Systems. These classes are found in most computer science departments. Brian Carrier has a very detailed book on file system forensic analysis which helps one understand how the operating system handles files that are being allocated to space or deleted [8].

The person who is the student needs to have a resume with his her education and work experience ready to discuss with the teacher. That resume should include formal university training, continuing education, and seminars. Then the student should also write briefly about his or her work experience including any investigations that he or she took part in.

The teacher can then see where the student needs more knowledge and then suggest further reading, webinars, or other methods of education to build that area of knowledge up. The teacher should be looking for report writing skills since the presentation of evidence for court or corporate officers is so important to an investigation. The teacher should also look for technical skills such as a knowledge of file systems, operating systems, and basic networking. The technical skills should also include the use of free Linux based tools that help the investigator acquire an image or complete copy of all the storage media located in the camera. Lastly, the teacher should evaluate the student's knowledge of legal principles that are relevant to the geographic area where the student may participate in investigations.

In my experience, many law enforcement students are often strong in report writing, investigating skills, and legal principles. However; they often need more technical knowledge such as operating systems and the advanced use of digital forensic tools.

In my experience, computer scientist students have excellent technical skills but need to learn more skills in conducting an investigation, interviewing people, and in legal principles. These students often need to be reminded that not following legal protocols, not having a proper chain of custody form, or not having properly licensed digital investigative tools can compromise an investigation.

The online teacher could conduct this type of conversation in a private chatroom, by telephone, or in a special section of a private island in a place such as Second Life. In certain circumstances, it might be best to conduct the discussion by email so that the student has a written statement of strengths and weaknesses and then can document ways to address those concerns. The point is that there are so many telecommunication modes that can work in tandem with the online virtual classroom to assist the student.

6 Conclusion

It is my opinion that students could be taught digital camera forensics by in person classes, by asynchronous online methods such as Blackboard, or by synchronous methods such as the virtual classroom in Second Life. In person classes work best for traditional learners who live near the university but this method only serves a small minority of people who need to study digital camera forensics. The asynchronous online Blackboard version of the class in my opinion serves the most people because it allows any size group of people anywhere and anytime to quickly take the class. They can also practice with their own digital camera or camera cell phone, and then print a credential after successfully completing the class. Lastly the synchronous version of the class in Second Life allows small groups of people anywhere to get personalized instruction but the drawback is that they have to wait until a scheduled class runs. If the class runs during business hours in the United States, it is nine hours later to a deployed soldier in Iraq. The time may not be convenient for the both the student and teacher. The main point is that online learning in any form allows students to obtain quality education that would normally not have been possible before the popularity of the Internet.

7. References

[1] URL Accessed March 5,2011 http://cameras.about.com/b/2009/01/28/stats-show-popularity-of-digital-cameras.htm

[2] Whitehead, T., (2011), U.K. Daily Telegraph, URL accessed March 5,2011 http://www.telegraph.co.uk/news/uknews/law-and-order/8360156/Rapists-who-attack-in-home-face-longer-in-jail.html

[3] URL Accessed March 5,2011 http://events.americasarmy.com/

[4] URL Accessed March 5,2011 Morris, C., (2002) "CNN Money, Your Tax Dollars at Play" http://money.cnn.com/2002/05/31/commentary/game_over/column_gaming/

[5] Berry, B., (2010)," Pedagogy, Student Preparation and Technology Issues in a Simulated Environment Professor Carlie Merritt and Professor Robert Berry", Conference Proceedings of the 13th Annual Emergency Management Higher Education Conference, June 7-10,2010 at FEMA, Emmetsburg, Maryland

[6] Pine, J.,(2007),"Technology in Emergency Management", Wiley Publishing, Danvers, MA, p244, ISBN 978-0-471-78973-4

[7] Vacca,J.,(2011),"System Forensics, Investigation, and Response", Jones & Bartlett Learning, Sudbury, MA, p248, ISBN 978-0-7637-9134-6

[8] Carrier, B.,(2005),"File System, Forensic Analysis", Published By Addison Wesley, Upper Saddle River, New Jersey, ISBN 0-321-26817-2