Teaching Cell Phone Forensics and E-Learning

Eamon P. Doherty Ph.D. Associate Prof.
School of Administrative Science, Fairleigh Dickinson University, Teaneck, N.J., USA

Abstract - *Estimates are that six out of ten people on the planet own a cell phone. Many of these cell phones hold data relevant to a crime. Many law enforcement and private security personnel have a need to learn cell phone forensics so that they may gather information related to their investigations. However; many of these investigators do not have cell phone forensic training where they live and funds may not permit distant travel to a class. E-learning appears to be an excellent solution to deliver cell phone forensics multimedia instruction to people worldwide. Investigators can also get the practical training they need by using their own cell phone and cable along with downloadable trial versions of digital forensic software. E-learning platforms such as Blackboard also allow an environment for testing and the distribution of a cell phone forensics credentials.*

Keywords: cell phone forensics, e-learning

1 Introduction

As the Director of the Cybercrime Training Lab at Fairleigh Dickinson University, I often get emails requesting both in person and online classes for the subject of cell phone forensics. Many of the requests are from law enforcement officers, private security personnel, and private investigators from around the world need that need to learn to examine cell phones and create reports on the evidence that they find for use in courts or for corporate policy investigations. Occasional requests also arrive from online students in a master's degree program who are also active U.S. military deployed to Iraq and Afghanistan and can only attend online.

Approximately six out of ten people on the planet own a cell phone [1]. Many people who commit a crime throughout the world carry a cell phone and that phone may carry some digital evidence that pertains to the crime in question. We can now see the urgency and scope of the need for online cell phone forensics classes.

2 cell phone forensics taught in person

I presently teach cell phone forensics in person in the Cybercrime Training Lab in Fairleigh Dickinson University in New Jersey [2]. The first half of the class is hardware driven and gives the student a sense of history concerning the cell phone. The material starts with the history of the cell phone and various historical examples are viewed in person.

Then we discuss the various communication protocols such as CDMA and GSM as well as the differences between various cell phone models used around the world. The materials progress to include the various cell phone frequencies used in dual band, tri-band, and quad band phones. The material then progresses to include some of the unique types of phones such as those with two or three SIM cards that allow people to have two or three separate phone numbers and identities.

The second half of the class covers a wide range of important topics such as: the legal issues in cell phone forensics, the examination machine, and then seizing the data and creating the report. Some of the legal issues include: communication data warrants, the chain of custody, fruit of the poisonous tree, and the Fourth Amendment Exception. Communication Data Warrants (CDW) are additional warrants that are needed to read unopened email on a phone or listen to new voicemail messages that were not previously listened to. The chain of custody is an important document that shows the trail of evidence of the a digital storage device, or any other piece of evidence, from the time it was seized until the time it was presented in court [3]. The Fruit of the Poisonous Tree means that seized data from improperly licensed tools will be dismissed for use in courts. [4] The Fourth Amendment Exception allows American Customs and Border Patrol Agents to examine cell phones at ports of entry without a search warrant.

The practical part of the class is when we use Paraben's Device Seizure and Susteen Secure View as the digital forensic software tools to capture and organize the data from the cell phone. The professor connects the cable to the phone, runs the forensic tool from a standard laptop, and then creates a report with the seized data using a wizard to fill in some data about the examiner and the case.

The cell phones are kept in a Faraday Bag to inhibit connectivity and tampering. All methods of connectivity on the laptop are disabled so that outside tampering is not possible. Students are encouraged to disable the Wifi, Infrared, Bluetooth, and wired connections to the laptops. Students are also encouraged to run the latest copies of antispyware and antivirus software on the laptops in order to enhance the credibility of the examination by showing that malware did not spoil the evidence or taint the investigation process.

3 Crimes committed with cell phones

It is also important to educate the students to some of the new crimes that are evolving such as virtual kidnapping [5]. Virtual kidnapping is when someone uses a person's cell phone and says he is holding the victim for ransom. The virtual kidnapper usually mines some data from the phone such as wife, children's names, and various friends. He or she will create a plausible story with the data and demand a small quick payment. The best thing to do in this case is to play along with the drama and contact the FBI immediately. The virtual kidnapper usually only has the phone and possibly a wallet, not the victim. If the FBI is contacted early, an arrest can often be made.

Other widespread new crimes such as Cyberbullying are then discussed [6]. A person may be the victim of having his or her picture taken without consent in a tanning salon, public shower, or changing room where there was an expectation of privacy. The picture may be uploaded to a website for others to view. There may be also accompanying remarks about the victim's weight and private parts on the website. Then others may belittle the victim causing problems from lost self esteem to suicide.

4 Putting the class online – e-learning

The in person class could easily be adapted for an online environment and in my opinion, would work very well online for an e-Learning environment. Students could register for the class through continuing education and then sign in a virtual campus. This class could be easily taught as a webinar too. The students could also download a series of course materials and ask the professor questions. Students could also use their own phones and data cables for the investigation. The company called Paraben has a trial version of Device Seizure and can be used with the student phone if that model is supported. Susteen also has a trial version of their forensic software and students could use their phone with the software provided that the phone is supported.

Tests could be given online and graded using an automated tool or by the professor. A certificate could also be placed online and if the score was above a certain threshold, it would be released for the person to print. There could also be suggested further readings and videos to watch.

4.1 Minor interaction online could inhibit information sharing

In one of my in person cell phone forensic classes, I took a picture from my own cell phone that included my wife in front of a large satellite dish at Camp Evans, in Wall, New Jersey. I uploaded it to www.gpsvisualizer.com and selected an option for google maps. Then it showed a red star on a map of New Jersey. I zoomed down and the label Marconi Road was visible on the map. I zoomed down further on the map and the same satellite on my picture could be seen on the map. However; I remember where I took the picture and it was not exactly where the map showed. Even the view of the satellite in my picture would be different from where it was marked on the map. I guessed there might have been as much as twenty feet inaccuracy.

I had a good rapport with the in person class and then one of my students said something that he may not have said online where there was no trust built. He then told me that if I was in a cloudy city with high buildings, that the GPS metadata in my picture might be inaccurate to as much as one thousand feet because only two of the seven GPS satellites might be obtainable for GPS coordinates.

Another student who was a law enforcement detective then seemed confident to share a personal story too. He told me that he solved a murder investigation because the cell phone camera held the picture of a murder victim and another showed a makeshift grave with the victim in it. The picture contained metadata with the GPS coordinates of the makeshift grave. A forensic team was dispatched to the site and exhumed the corpse before much decay set in. I doubt the student would allow such details to be archived in writing if we used online learning.

4.2 E-learning is outstanding for specialized learning

Perhaps the previous discussion would not have happened in an online environment where sensitive things could be attributed to a person. However; e-learning makes it possible for large amounts of people anywhere in the world to receive a specialized class such as cell phone forensics. They can even post questions, get a credential, and learn how to further their knowledge. This in my opinion makes
e-Learning invaluable.

4.3 Sending the cell phone with data and a cable

The other option for the course is to send the person a cell phone and cable with preloaded emails, phone books, text messages, and call logs in it. Then the person can use the tools, find the data, and write a report of what is seized from the cell phone. The person could be graded on how well they get the scenario. It might be very interesting for the student too, perhaps like reading a spy novel. The only downside is that the cell phone might take as long as a week to reach some parts of the world and the person that needs a quick credential may not have it in time. From my experience, some countries such as Taiwan might also try to collect duty from the student because it might be considered a foreign purchase.

The person who gets the phone would naturally have to pay a deposit before they get the phone and cable. After the course is done and the report is graded, the person would return the phone and cable. Upon receipt of the phone, the deposit would be returned. This deposit would guarantee that either the phone be returned for other students, or that a suitable replacement could be purchased by the school.

4.4 Two options for this type of e-learning

A person who is going to be investigating phones and quickly going to court may need to use their own phone and cable and do the immediate course. The person that wants the more difficult option of finding data and creating a report would use the second option with the understanding that the course will take longer to complete.

5 Examining phones from the Far East

I sometimes have groups of students fly in from the Far East to take classes on cell phone forensics, electronic eavesdropping device detection, digital camera forensics, and take field trips for two or three week stints. The cell phones from the Far East are approximately one year ahead of the American cell phone market and often have features such as increased storage capacity, increased megapixel resolution, and other features not available on cell phones in North America. I have been told by private security contractors that Mobil Edit is the only cell phone forensic tool available to American Law Enforcement and private security contractors that can be used for these new Far Eastern phones.

5.1 Google Translate for foreign language document

Sometimes documents or text messages on a cell phone are in another language. The examiner can use Google Translate for a rough translation of one language into another. I have used Google Translate to change Chinese documents into English. This is very good for cell phone examiners who do not speak the language that is used on the phones they are examining. Google Translate is good because you can also translate from one non English language to another such as Korean to Chinese.

Sometimes documents or text messages on a cell phone are in another language. The examiner can use Google Translate for a rough translation of one language into another. I have used Google Translate to change Chinese documents into English. This is very good for cell phone examiners who do not speak the language that is used on the phones they are examining. Google Translate is good because you can also translate from one non English language to another such as Korean to Chinese.

6 Expanding the education

It is also possible to use Google Translate to translate your scripted data for the phones to thirty or more languages. Perhaps the educational materials could be roughly translated with Google Translate and then proofread and corrected by native speakers. The cell phone forensics class could then be offered in nearly every country on earth thus perhaps standardizing the education for a technical investigative skill.

6.1 Laws and content for e-learning

The content for the phones could not be used in every country. Pictures of people in bathing suits or anything that could be construed as pornography for example most likely cannot be used in conservative countries such as Saudi Arabia. There needs to be a vetting process for the materials with the general counsel at the university and perhaps someone from the embassy of the country or countries you wish to offer classes in.

6.2 From e-learning to networking with professionals

Many students who are private security contractors, private investigators, or law enforcement personnel may want to meet other cell phone forensic examiners or digital evidence investigators when they are done with the course. There are groups such as ASIS International where they could network with others in all areas of digital forensics and investigation [7]. This would help them broaden their horizons and think about expanding into other mobile device forensic examination such as PDAs and digital cameras too.

Becoming a Certified Computer Examiner (CCE) is also a good idea for both instructors and students of cell phone forensics. The CCE gives digital evidence examiners both the practical and theoretical experience examining different types of digital media and is in itself a respected credential [8, p. 448 – 449]. The CCE group is also very active with emails and one can quickly ask questions about smart phones, thumb drives, or any type of digital media needing examination and then receive a timely response.

6.3 Good definitions of technical terms are important

Many of the people who will take the class online will investigate phones and most likely go to court. They may have to give testimony and be asked technical questions. It is very important that students be given a glossary of definitions for technical terms in cell phone forensics that are accepted by their peers and the legal community.

Since the United States vs. Frye in 1923, the methodology of forensics used in the United Courts must meet the scrutiny of the court [9]. The methodology, science, tools, and vocabulary of forensics must be accepted by one's peers and be considered good science for any findings to be used in court.

There are many places to obtain definitions of terms related to cell phones, telecommunication systems, and networks. Some academics have told me that they do not like references with URLs because those links may not be active in the future and then it may not be possible to verify certain facts. When I was completing my doctorate at the University of Sunderland, I was told to only use reference books, journals, textbooks, or any other reliable published paper source.

I once taught a course on cell phone forensics for a county prosecutor's office who was just setting up a cell phone forensics lab. I gave them an extra copy of Newton's Telecom Dictionary to get them started with telecommunication definitions. They could purchase a newer reference later.

7 Pre-assessment and post-assessment e-learning

Today more than ever it is important to assess what was learned in the class and map how those skills help the cell phone examiner do his or her job. I suggest having the person take some kind of pre-assessment to see what he or she knows. Then take the course and perhaps take the same assessment to assess what was learned. In the beginning of the course there could also be a page of learning objectives.

Different countries and states may have different expectations for their cell phone examiners so perhaps some study might be done to assess what skills and learning objectives are needed for various countries in the Middle East, Europe, Far East, various American States, and Canada. Perhaps the university may wish to approach a bar association or legal community for each country and state where the education may be offered to learn what expectations of knowledge they have for cell phone investigators. Daniel Minoli, an author of a distance learning textbook says that, "The quality of the distance learning programs is a function of the selected type of solution and the particular needs of the distance learners." By following Daniel Minoli's advice and having an assessment to see if the students' needs are met, would also be a valid qualitative measurement of the program.

8 Special needs training (blind people)

The cell phone forensics class in my opinion could be modified for the blind examiner who is an online student. I have met one CCE who was blind and she has used screen readers to speak all of the text captured on a digital device such as a cell phone or laptop. I also believe that cell phone investigative kits such as Susteen Secure view have a limited number of cables and if the case was organized properly, a blind person could easily find the cable they need for an investigation. The cable would only need to go from the USB port to the phone. This could be done with feeling for the locations of the connectors and receptacles.

9 Top secret training methods

If there was some type of specialized cell phone forensics training that included questions and answers from a location such as the Green Zone in Iraq, then specialized videoconferencing protocols discussed in Richard Schaphorst's classic book, Videoconferencing and Videotelephony, Technology and Standards could be used for a preliminary discussion of standards [11]. Perhaps something newer such as the United States military's SIPRNet could also be used.

10 Conclusion

Cell phone forensics is an important discipline that needs to be taught to a variety of investigators worldwide. The majority of the planet owns a cellphone. The phones are also often present at crime scenes. These phones may hold some digital evidence to prove a person innocent or guilty of a crime or policy infractions. E-Learning is an excellent platform to provide training for cell phone forensic investigators as well as assess what was learned. The many tools available to the E-Learning community also allow the content to be effectively translated to other languages and be made accessible to special needs populations.

11 References

[1]. The Associated Press (March 2, 2009). 6 in 10 People worldwide have cell phone. Retrieved from : TBO.com, April 22, 2011, http://www2.tbo.com/content/2009/mar/02/6-10-people-worldwide-have-cell-phone/news-money911/.

[2]. Doherty, E.P., & Liebesfeld, J. (2007). E-forensics and investigations for everyone. *Preface to cell phone chapter, p. 15*. Bloomington, IN : Authorhouse. ISBN 978-1-4343-1614-1.

[3]. Vacca, J.R. (2005). Computer Forensics, Computer Crime Scene Investigation. *Evidence collection and data seizure, p. 228-229*. Boston, MA : Charles River Media. ISBN-13: 978-1-58450-389-7

[4]. Shinder, D. L. (2002). Scene of the cybercrime, Computer forensics handbook. *Collecting and preserving digital evidence, p. 551*. Rockland, MA : Syngress Publishing, Inc. ISBN 1-931836-65-5.

[5]. Harwood, M. (2011). The Real Price of Virtual Kidnappings. *Security Management, March 2011 edition, p. 46*. Alexandria, VA : ASIS International.

[6]. Vacca,J.R., & Rudolph, K. (2011),. System Forensics, investigation, and response. Sudbury, MA : Jones & Bartlett Learning. *Searching memory in real time with live system forensics, p. 248*. ISBN 978-0-7637-9134-6.

[7]. ASIS International (2011). About ASIS. Retrieved from : http://www.asisonline.org/about/history/index.xml

[8]. Whitman, M. (2009). Principles of Information Technology. Boston, MA : Thompson Education. ISBN 978-1-4239-0177-8

[9]. Vacca,J.R., & Rudolph, K. (2011). System Forensics, investigation, and response. Sudbury, MA : Jones & Bartlett Learning. *Controlling a forensic investigation, p. 125*. ISBN 978-0-7637-9134-6

[10]. Minoli, D.(1996). Distance Learning Technology and Applications. Norwood, MA: Artech House. *Introduction to the distance learning environment, p. 12*. ISBN 0-89006-739-2

[11]. Schaphorst, R. (1996). Videoconferencing and videotelephony, technology and standards. Norwood, MA: Artech House. *Video teleconferencing benefits and system design, p. 12*. ISBN 0-89005-844-5