Extending the Multidisciplinary Learning Experience in Digital Forensics Using Mock Trials

Gary C. Kessler[1], Robert Simpson[2], James Fry[3]

[1]Computer & Digital Forensics Program
Champlain College Center for Digital Investigation
Burlington, Vermont, USA
gary.kessler@champlain.edu

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia, AUS

[2]Criminal Justice Program
Champlain College
Burlington, Vermont, USA
simpson@champlain.edu

[3]Paralegal Studies Program
Champlain College
Burlington, Vermont, USA
fry@champlain.edu

Abstract

Computer forensics is a multidisciplinary, hands-on field of study and nothing reinforces this more for the student than opportunities to practice the skills while working with counterparts in other fields. This is particularly important in the area of reporting results; if written report and oral testimony are poor, even the best examination can be compromised and the results called into question.

In 2007, the Computer & Digital Forensics (C&DF), Criminal Justice (CJ), and Paralegal programs started to employ a mock trial to bring students from these three different disciplines together for a public, community event. The scenarios are pre-planned by faculty advisers. The actual incident starts with a crime scene, staged by volunteers from the college's performing arts students. CJ students secure and process the crime scene, interview witnesses, and gather evidence. Digital devices are recovered and are forensically processed by the C&DF students, resulting in a report of the analysis for the criminal investigators. All

reports are forwarded to Paralegal students who work with local attorneys who act in the role of the prosecution and defence teams. On the day of the trial, a retired criminal court judge presides over the proceedings, complete with a jury selected from volunteers from the college community. For many students, this is the first trial scenario they have seen outside of television, and the attorneys and judge ensure realism.

The biggest learning experience for the students is to realize how complex the actual process is. In particular, testifying, professionally conveying the proper message, and dealing with a possibly hostile cross-examination are surprisingly difficult. Students also learn that the evidence does not always speak for itself to gain convictions.

1.0 Introduction

Champlain College started an undergraduate degree program in Computer & Digital Forensics (C&DF) in 2003. Recognizing that digital forensics is a multidisciplinary field of study, the curriculum provides students with a good grounding in computer technology, networking, and criminal justice in addition to fundamental computer forensics and digital investigation courses [1]. Digital forensics education requires a high degree of hands-on, interactive activities, which are enhanced by courses where C&DF students take courses with peers in other disciplines, such as Criminal Justice (CJ) and information technology programs.

It is common in the public sector for the criminal investigator to identify potentially relevant digital devices and turn those exhibits over to the computer forensics team, so that the investigator's next contact with the digital part of the case is when they receive the report. For that reason, reporting is often the most visible step outside of the computer forensics lab, and poor reporting or testimony can compromise even the best digital forensics examination.

To address the need for C&DF and CJ students to work together on processing a crime scene involving digital evidence, and to experience the big picture of a case from crime to verdict (à la an episode of *Law & Order*), Champlain College has started to employ a mock trial event that involves C&DF, CJ, and Paralegal students and faculty, as well as practicing attorneys and a retired judge. For many students, this is the first trial scenario they have seen outside of television, and the attorneys and judge ensure realism.

This paper will describe our experiences with the mock trial and the lessons learned. Section 2 will describe the process of designing the case scenario, preparing the evidence, and planning the trial. Section 3 will describe the computer forensics aspects of the process. Section 4 will review our experiences and lessons learned, with future plans and changes to the C&DF curriculum as a result of the mock trials covered in Section 5. Section 6 will provide some final conclusions.

2.0 Organizing the Mock Trial

As with any major project, the mock trial requires a lot of people and planning. Our goal was that only a few people would know the complete scenario and they, of course, could not be participants. All other players -- from the witnesses and investigators to the attorneys and judge -- would only have the information provided as it would have been in a "real" case. This section provides some details about the planning process itself, defining the various players, and setting the schedule.

2.1 The Case Scenario

One of the most important aspects of the trial, of course, hinges upon the case itself and here is where a great deal of thought needs to be spent; all other aspects of the case will follow from the crime scene that is devised.

In 2007, we contrived a murder case. The scenario was two young men in a dorm lounge argued over some drugs, resulting in one of them shooting and killing the other (Figure 1). Upstairs, another couple was asleep; awakened by the noise of the argument, they heard the shot and saw the suspect depart.

Figure 1: The crime scene

In 2008, the scenario was based on a real case that had occurred in the area some years ago. Here, a man travelled to Burlington to meet with a drug dealer; the two argued, and the man severely beat the drug dealer. In this case, the victim's girlfriend and roommate were witnesses, although the girlfriend refused to testify.

During the planning, we actually treated both scenarios as if they had been made up. The CJ faculty assisted in determining what physical evidence should be found and collected at the scene and, as is usual at any crime scene, some of the materials had evidentiary value and some did not. The goal was that the investigators would collect whatever they thought was necessary to collect, obtain proper authorization

from the Court to examine the seized materials, and then ascertain the evidentiary value of the exhibits upon receiving reports back from the "crime lab."

The faculty prepared information for the lab reports. As an example, in one scenario, the crime lab reported that an empty wine bottle found near the victim had a clear handprint of the victim upside down near the bottle's neck; the investigators needed to determine if this was an indication that the victim had held the bottle upside-down and used it to attack the suspect. Digital evidence was similarly prepared to fit the case; call histories and Short Message Service (SMS) messages were used to indicate a pattern of behaviour between the suspect and victim, but it was left to the investigator to put the pattern of information together.

2.2 Roles and Players

To ensure that the mock trial would be a true learning experience, third and fourth year C&DF, CJ, and Paralegal students performed the active roles of crime scene investigation, digital forensics examination, and legal assistants, respectively. To ensure realism in the courtroom, practicing or retired judge and attorneys played those roles. Additional realism was added by use of a jury selected from the college community (including faculty, staff, and students).

The mock trial organizers worked with the college's Performing Arts program to find actors willing to participate in the event. The only two players who receive any sort of briefing about what is to take place are the victim and suspect. When the scenario is started, they play their roles and any other players become true witnesses. No attempts were made to perfectly stage the incident, however. For example, during one of the scenarios, the victim was wearing a USB thumb drive on a lanyard around his neck; after shooting the victim, the suspect inexplicably took the thumb drive. This made the investigation much more interesting and even the suspect told us later that he took the thumb drive on a whim. In addition, during one of the scenarios, a college staff member just happened to be in a place to observe the "suspect" discard a weapon, thereby becoming an actual witness after the fact; he subsequently testified at the mock trial.

Two students were recruited from each of the C&DF, CJ, and Paralegal programs, each in their third or fourth year of study. The CJ majors, both of whom had already taken courses in crime scene investigation and investigative interviewing, were assigned the roles of detective. Their job was to process the crime scene, interview witnesses (Figure 2), arrest a suspect, seize any exhibits that were thought to be relevant to the case, and prepare any necessary affidavits, subpoenas, and search warrants. They also needed to prepare investigative notes for both the prosecution and defence, and be prepared to testify at trial.

The C&DF majors, both of whom had taken Computer Forensics I and II as well as several CJ course, were assigned the task of performing the forensic examination and analysis of the digital devices seized from the scene, which included two mobile phones and a USB thumb drive (details about the digital evidence can be found below). They worked with the criminal investigators to ensure that the court

orders for the digital devices were valid and also prepared reports of their examination.

Figure 2: CJ-student "criminal investigators" interviewing witness

The Paralegal majors worked with the attorneys that formed the defence and prosecution teams. The attorneys were actual practicing lawyers from the area who agreed to participate in the trial. Because of the nature of the event, not every aspect of a criminal trial was followed; in particular, the *voir dire* process of jury selection was skipped. The paralegal students, then, assembled the information necessary for trial and helped the attorneys prepare the cases for the defence and prosecution (Figure 3).

Figure 3: From left: the defendant, defence attorney, and prosecution team (with paralegal student); members of jury are seen in the background

2.3 Schedule

Planning the trial requires some long-term preparation and planning although it is not months of constant work. In our two experiments, we started by selecting the date for the trial and then scheduling all tasks backward from that date. Our class schedule is from early September to late April, with roughly a month off from mid-December to mid-January. A comfortable schedule and task list might look like:

- Assemble faculty advisers for initial planning meeting (1 October)
- Finalize crime scene scenario, identify players (21 October)
- Start to recruit students for crime scene actors, CJ investigators, C&DF examiners, and Paralegal legal assistants (1 November)
- Start to recruit attorneys and judge for mock trial (15 November)
- Stage the crime scene and initiate criminal investigation (21 January)
- Receive digital devices for examination (25 January)
- Advertise for jurors from the college (or greater) community (1 February)
- Digital forensics report provided to investigators (7 February)
- Complete investigative reports and provide for defence and prosecution team (15 February)
- Jury selection (21 February)
- Mock trial (15 March)

The end result is a mock trial event that is planned for roughly two hours, including testimony, jury deliberation, and verdict. Any pre-trial motions are discussed between counsel and the trial judge, and settled before the trial date; the motions are summarized at the beginning of the trial but not handled in real-time.

3.0 The Digital Forensics Component of the Mock Trial

Although not a major part of the trial itself, the examination of the digital evidence plays an important role in entire mock trial process and is, naturally, an important activity for the C&DF students. The digital evidence comprised three items, namely, two mobile phones and a USB thumb drive. This section will describe some of the digital forensics aspects of the mock trial process.

3.1 Search Warrants

The Fourth Amendment to the U.S. Constitution guides the rules for how the state can search and seize evidence (state constitutions may further limit the procedures for local law enforcement). Although all of the digital devices could be seized at the crime scene, a search warrant was requested in order to actually examine the devices. There are a number of exceptions to the search warrant requirement, such as exigent circumstances, plain view, or consent. Absent those factors, police will obtain a warrant.

The role of the student examiners was to assist the student investigators in obtaining a valid warrant. In this case, it meant to ensure that the devices were properly identified and that the language properly described the scope of the examination; i.e., obtaining permission to view all available information on the

devices, including call history, contact list, SMS messages, data files, images, videos, and audio files.

The examiners also needed to ensure compliance with the warrant prior to performing the actual exam. In this case, the examiners needed to be sure that they were performing the exam within the time limits specified by the court, that the proper devices were being examined, and that the scope of the exam complied with the warrant. These points are particularly important in Vermont since this state has no "good faith" exception to errors in a search; e.g., if the police seize an LG phone and improperly identify it as an Ericsson phone, the court could invalidate a subsequent search.

3.2 Examination of the Mobile Phones

The mock trial evidence included one mobile phone seized from the suspect and one found on or by the victim. Data on the phones were used to demonstrate that the victim and suspect:

- Knew each other, as evidenced by entries in the contact list, call history, and SMS messages
- Knew people in common, as shown by entries in the contact list
- Communicated with each other soon before the crime occurred, as evidenced by the call history and SMS messages

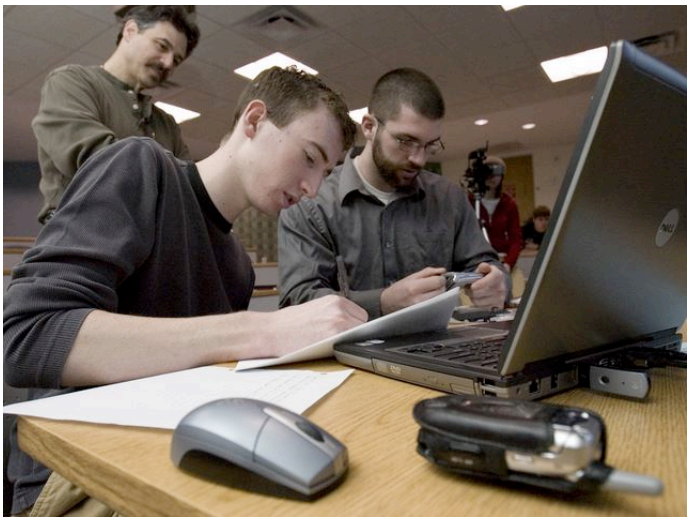

Figure 4: C&DF students examining a mobile phone (author Kessler in the background)

The two C&DF student examiners were responsible for examining the phones seized from the suspect and victim, although the examination process was open for observation to any interested C&DF students. The actual exam was supervised by

an experienced mobile phone examiner (Figure 4), and the students followed the same process and procedures, and used the same hardware and software, as is used by local law enforcement.

Although two mobile phones were seized during the investigation, a thorough exam was performed on only one of them, an LG VX 6300; this phone uses code-division multiple access (CDMA) technology and was examined using BitPim and MOBILedit! Forensics software. Only a single phone was examined because the phones did not contain real evidence; instead, we wanted the students to actually perform a mobile phone exam so that they could write an accurate report describing what they did and so that they could testify, if necessary, about how they examined the phones.

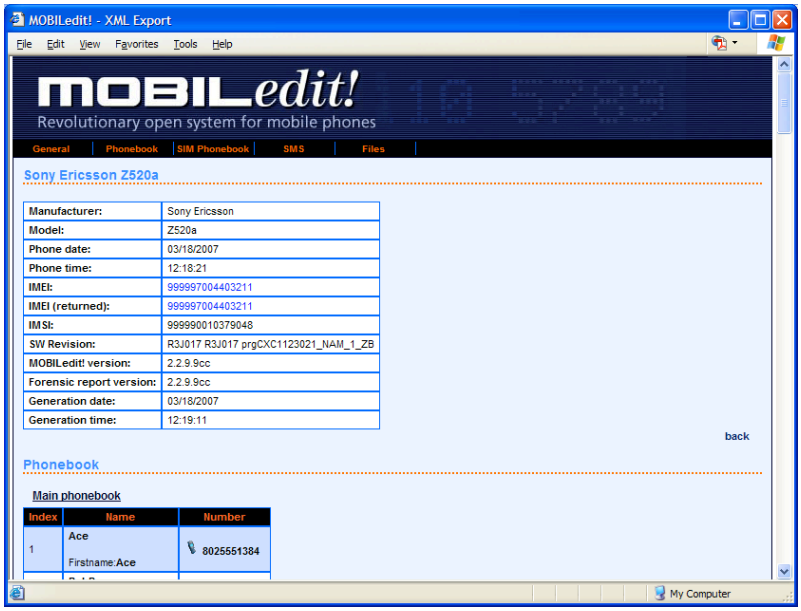

Figure 5: Mobile phone forensics report

In fact, the cell phone evidence was created by C&DF faculty to match the crime scene. As part of the storyboard for the crime, a timeline of calls and SMS message exchange was created. Since MOBILedit! creates Extensible Markup Language (XML) reports, the XML files were edited to insert appropriate evidentiary information into the report (Figure 5). This was one area where the true examination did not yield "true" results. Student examiners wrote a report on the process that they used to examine the mobile phones and also provided the reports with the manufactured evidence.[1]

[1] See http://digitalforensics.champlain.edu/dfa/archives/MockTrial2007/Suspects_Cell_Phone_2007.zip and http://digitalforensics.champlain.edu/dfa/archives/MockTrial2007/Victims_Cell_Phone_2007.zip for sample phone reports.

3.3 Examination of the USB Thumb Drive

The final piece of digital evidence was a USB thumb drive that ostensibly belonged to the victim. The thumb drive was contrived to have evidence that, in fact, highly suggested ownership by the victim although not always found *on* the victim's person -- during the first mock trial, the suspect inexplicably took the thumb drive from the body of the victim and it was found by the investigators upon his arrest.

Creating the thumb drive evidence was straightforward. In this case, three files were created: an e-mail from the victim's mother wishing him a happy birthday at some date in the recent past, a cover letter from the victim to a potential employer, and a spreadsheet containing dates, locations, names, amounts of money, and other information suggestive of drug dealing. In preparation for the mock trial, the thumb drive was completely wiped, the three files written to the drive, and the e-mail and cover letter deleted (not wiped) from the drive.

The student examiners, in compliance with a valid search warrant, imaged the thumb drive using AccessData's Forensic Toolkit (FTK) Imager[2] and performed an exam using FTK software. Students then prepared a report detailing the device examined, the imaging process, results of the examination, and an analysis of the findings.

3.4 Impact of Digital Evidence on the Trial

The student computer forensics examiners did not testify in court and, in fact, the digital evidence was barely referenced during the court proceedings; as is so often the case, the prosecution introduced the digital evidence and the defence stipulated that it was accurate. Indeed, the defence claim in both mock trials was that the defendant was innocent of the charges and the digital evidence that was planted was purposefully vague enough so as not to be the "smoking gun."

The student examiners were disappointed in not being able to testify but they learned a valuable lesson -- while computers are increasingly the instrument, record keeper, and/or target of criminal activity, digital evidence is not always what leads to a conviction. Indeed, there are many high-profile cases where the digital evidence is key to providing direction for a criminal investigation even though it is not, in and of itself, damning beyond a reasonable doubt. A case in point well known to our students was the sexual assault and murder in October 2006 of Michelle Gardner-Quinn, a University of Vermont student. Gardner-Quinn just happened to use the cell phone of a man named Brian Rooney, whom she met in downtown Burlington on the morning when she disappeared. That single call was the only information that led police to interview Rooney, who later became a suspect and was eventually convicted of the crimes in May 2008 [2]. The cell phone information led police to Rooney but was not the reason that he was convicted.

---

[2] See http://digitalforensics.champlain.edu/dfa/archives/MockTrial2007/USB_Thumb_Drive.E01 for a sample thumb drive image.

4.0 Experiences and Lessons Learned

Although we have only executed this event twice, many object lessons have already emerged for student participants and the organizers.

4.1 Lessons for the Students

For most students, the mock trial is the nearest thing that they have seen to a courtroom. The room is setup like a court, and the lawyers and judge ensure realism. Perhaps the best learning experience for all of the attendees is hearing the judge's instructions to the jury prior to their deliberations (Figure 6).

Figure 6: Vermont Superior Court Judge (ret.) Edward Cashman

Another important lesson for the students was to see first-hand the complexity of the actual investigative and trial processes. In particular, students learned how hard it is to testify in open court, professionally convey the proper message, describe technical details to a non-technical jury, and deal with a possibly hostile cross-examination.

Students also learned about the importance of thorough exams and that evidence does not always speak for itself to gain convictions. In the 2007 murder mock trial, detectives quickly focused their investigation on the suspect, a young man who

was a suspect only because of eyewitness identification. The detectives swabbed the suspect for gun shot residue (GSR), which was positive, which fit their theory that he was the shooter. Unfortunately, they did not swab the eyewitnesses for GSR, allowing the defence to raise the theory that one of them, in fact, shot the victim; when the suspect came by for a pre-arranged meeting with the victim, he found the victim dead, panicked, and ran away with the gun. Indeed, even though the suspect really was the shooter, he was found not guilty.

Similarly, in the 2008 assault, eyewitness testimony was key because there was scant physical evidence; the prosecution contended that the suspect beat the victim with a tire iron and the defence maintained that the suspect was not even in Vermont at the time of the assault. The witnesses either gave inconclusive testimony or themselves lacked veracity so that reasonable doubt caused the jury to, again, the suspect not guilty -- even though he actually did commit the crime. The lesson here was that eye witnesses are often poor recorders of events and do not always make good witnesses; physical evidence is much less emotional and less able to be confused on a witness stand.

4.2 Lessons for the Organizers

After two mock trials, the organizers are still learning how to put this event together. First, because this project involves people from so many departments, and comprises students, faculty, staff, and volunteers, the trial needs to be treated like a major project, meaning an organizing team, a project manager, and a task list. The trial is fun and educational, but putting it together is serious business and requires some central management to coordinate events and to ensure that the evidence is in synch with the crime scene.

Second, we would like to make this more of a college community event. One obvious way to do this is via the college newspaper, where we can have a reporter write an article about the crime, the subsequent arrest, and the upcoming trial. It also provides a way to obtain a jury pool and, ultimately, report on the outcome of the trial. We would also like to use this as a way to open the event to the general public.

To accomplish these best practices, the organizing team needs to be supplemented by student volunteers who can see the project through for the academic year. That is the approach that we will try in the upcoming year.

Another plan for next year is to document the event and the planning. It is our hope that we can hire a videographer and create a video storyboard so that the process can be shared on a wider basis.

4.3 Application of Law

The scenarios that have been designed for the Champlain College mock trial exercises are venue-neutral and are crimes that could occur anywhere. In that respect, the exercise is transportable and this concept of a mock crime, investigation, and trial could be modified for any jurisdiction in any country. Since

the trial itself is not scripted, the outcome is in no way pre-determined and, therefore, can comply with any local or national law.

Our crime scenarios, for example, were planned so that local (i.e., state) criminal statutes would apply. A few changes to the scenario (e.g., possession of child pornography or large quantity of drugs) could have made this a federal crime. A few more tweaks could make the scenario and digital evidence methodologies apply to any other level of crime in any other country. Educators would, obviously, need to apply appropriate investigative techniques, digital investigative tools, legal requirements, courtroom procedures, etc., but the physical and digital evidence from the crime scene could remain basically the same for planning purposes.

5.0 Future Plans and Impact on C&DF Program

The two mock trial experiences have proven to be such valuable experiences for the students that we are committed to continuing this as an annual event. The events have also made us recognize one significant deficiency in our program content.

Champlain College's C&DF program focuses on the digital forensics process rather than specific tools, with particular attention paid to written and oral communication, such as preparation of affidavits for search warrants and examination report writing. What we discovered in the process of the mock trials is that students are not specifically prepared to handle court depositions and testimony. Furthermore, no more than one C&DF student would be providing testimony in the mock trial and, by necessity, such testimony would be brief. To address this concern, the C&DF faculty have already put into place a new senior-level (fourth year) course that covers courtroom testimony, an essential skill for both the private and public sector analyst. We think that this makes a good capstone course, joining an internship experience and senior project in the last year of the program.

The mock trial organizers also recognize that digital evidence may not be given its due in the cases that have been studied. Digital evidence has, in fact, been crucial in securing conviction in several high profile cases in Vermont over the past two or three years, including aggravated assault, robbery, kidnapping, and homicide. Given our experience in the preliminaries and project logistics, we intend to give digital evidence more of a key role at the next mock trial. C&DF students will learn what it means to be qualified as an expert as well as what it means to be cross-examined about their expertise. The primary focus of their testimony, both on direct and cross-examination, will be on the reliability of the evidence that they have recovered.

While jurisdictions may differ on how to qualify an expert -- even in the U.S., state and federal courts may qualify experts using different guidelines -- courts throughout the world (including courts in the countries that do not have jury trials) are always concerned about the reliability of the evidence that they are asked to

consider. C&DF students will be required to undertake the study, planning, and thought required to answer the basic question: "How can we be confident that this evidence *is* what you say it is and *says* what you say it does?"

6.0 Acknowledgements

Several faculty members played a key role in helping organize this as an annual event. Particular thanks are given to Robert Edwards, former CJ program director; Joanne Farrell, Theatre Arts director; and Steve Loughlin, Crime Scene Investigation instructor. Thanks are also given to Vermont Superior Court Judge (ret.) Edward Cashman and attorneys Lauri Fisher, Susan Hardin, and Ted Kenney.

This work was partially supported by Grant No. 2006-DD-BX-0282 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view in this document are those of the authors and do not represent the official position of the U.S. Department of Justice.

References

1 Kessler, GC & Schirling, ME (2006). The design of an undergraduate degree program in computer & digital forensics, *J. of Digital Forensics, Security, and Law*. 1(3), 37-50. www.garykessler.net/library/C&DF_curriculum.pdf (visited July 2008)

2 Wikipedia (2008). Murder of Michelle Gardner-Quinn, en.wikipedia.org/wiki/Murder_of_Michelle_Gardner-Quinn (visited July 2008)

Kessler, G.C., Simpson, R., & Fry, J. (2008, September). Extending the Multidisciplinary Learning Experience in Digital Forensics Using Mock Trials. In D. Edgar-Nevill (Ed.), *Proceedings of CFET 2008: 1st International Conference on Cybercrime Forensics Education & Training*. Canterbury, UK: Canterbury Christ Church University.