Title: Hands-on testing of students’ Forensics competency in CSC310 using a case study of Chinese House Churches

Author: G. Jan Wilms

Objectives:
- Unlike most certification exams, where students show their knowledge by answering multiple-choice exams, we have developed a hands-on test where students demonstrate true competency with the forensic tools.
- Integration of faith and learning, notoriously hard to do in an objective discipline like computer science.

Background:
Computer Forensics is the investigation of a computer system believed to be involved in cybercrime. The goal is to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. Professionals with forensics skills are in great demand with the increasing frequency of computer hacking incidents and concern over cyber terrorism. There are special investigative tools like Encase, which are very powerful but require a deep understanding of storage devices, operating systems, and networking.

Because there is a shortage of professionals in this field, the CS department introduced CSC310 a few years back, which covers forensics, ethical hacking, and information assurance. In order for our graduates to be competitive, we prepare them to take an (optional) industry certification exam like CHFI or EnCe. However, like so many certification exams, the questions are Multiple-Choice based, which means that a good test taker who has never had any hands-on experience with the technology can still get a passing score by cramming exam-specific self-study guides.
Innovation:
This time we wanted students to experience a more authentic hands-on experience, similar to what a professional would experience in a real case. Students received a virtual hard drive where they had to locate and document evidentiary materials of intentionally hidden “criminal” activities. Using child pornography as a test-bed, while certainly real-world and apropos, would be too controversial and a liability. Because of Union’s distinct Christian mission, we decided a fitting case study and an integration of faith and learning would be hidden biblical references. This is not so far-fetched, as in some countries like China only state sponsored religion is allowed, and independent house churches are illegal and actively persecuted. Hence practitioners intentionally use fuzzy terms like “daddy” to refer to God the Father. A forensic examination thus is not just a simple search for obvious phrases like Christ, Bible, Thou, etc.

Part of the innovation was also the use of virtual machines, rather than real computers (similar to a Mac running Windows programs). This allowed the instructor to delete files and remove partitions, preserve browser caches and RAM images, which would be permanently lost if over-written on a real machine. Because the virtual machine is just a large file, it was easy to give all students their own copy, which they could investigate on their own computers. Moreover, it has a roll-back feature, so students could always restart from scratch if they messed up. I have not come across any other courses elsewhere that have employed virtual machines for such purpose.

Students were tasked to find 10 evidentiary materials, each hidden using different mechanisms. These ranged from the obvious (hidden attribute, deleted but not yet overwritten, recycle bin), to thwarting mechanisms to prevent string searches (renamed extension, zip files, Unicode), to more hardcore obfuscation (ADStream, slack space, removed partition, printer spool file). We even used steganography (text messages hidden within a picture).
Outcome:
While most students did well on the theory test, some struggled with this new hands-on exam. However, since it was a take-home exam, most were eventually successful because there wasn't any time-pressure. Another factor that helped them was that it wasn't an open-ended search – they knew exactly how many evidence items had been hidden, and their Biblical literacy helped them focus their search and recognize the “evidence”. Frustration followed by a sense of accomplishment is often a necessary path to deep understanding. An unintended benefit was that students learned first-hand that merely inspecting a machine subtly changes some of the data (but the roll-back feature of the virtual machine gave them a second chance).

A planned improvement for next time is to let a group of students hide the evidence for other groups to find. In the world of computer security, this is called white-hat hacking, i.e. learning the tools and tricks used by the criminals, in order to better defend against such incursions.