TEACHING DIGITAL FORENSICS AND CYBER INVESTIGATIONS ONLINE : OUR EXPERIENCES

Elizabeth K. Hawthorne, PhD
Rose K. Shumba, PhD
University of Maryland University College

Abstract

This paper describes our experiences of teaching cyber investigations and digital forensics online. Additionally, it discusses open source toolkits and remote virtual labs appropriate for teaching cyber investigations and digital forensics effectively in a distance education environment. Both faculty and student experiences as well as lessons learnt from teaching these courses online at the University of Maryland University College (UMUC) are covered.

Keywords: Digital forensics, cyber investigations, online education

Introduction

According to the 44th President of the United Stated, “America's economic prosperity in the 21st century will depend on cybersecurity” (Obama, 2009). “While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts… to implement the CNCI (Comprehensive National Cybersecurity Initiative)… we must develop a technologically-skilled and cyber-savvy workforce...” (CNCI Initiative 8, 2008). Consequently, new in the international Association for Computing Machinery/Institute of Electrical and Electronics Engineers Computer Science Curricular Guidelines is the Information Assurance and Security knowledge area (ACM & IEEE, 2013). Because of its increasing importance, digital forensics is included in this new security knowledge area.

Digital forensics is an emerging area within the broader domain of computer/cyber security whose main focus is the discovery and preservation of digital evidence for proof of corporate or criminal wrongdoing and ultimate prosecution of illegal activity (Jarrett, 2010)

Evidence gathered from computing devices is becoming a routine part of criminal cases with nearly 85% of the current caseloads involving digital evidence (Davis, Cowen, & Philipp, 2005). The prediction is that the field cannot meet the demand for digital forensics professionals in the near future. Consequently, many colleges and universities are adding forensics courses and degree programs to their curriculum in order to satisfy the need for forensics specialists. Given the vital need for digital forensic professionals [4] and the steady rise in the number of colleges/universities offering online courses [5], this paper describes an online Digital Forensics (DF) program at UMUC, the resources identified as useful in teaching the DF courses, as well as lessons learned from both student and faculty experiences.

The UMUC Digital Forensics Program

The University of Maryland University College (UMUC) headquartered in Adelphi, MD is a leader in online education teaching students across the globe. The UMUC offers an online undergraduate course CCJS 321 entitled *Digital Forensics in the Criminal Justice*

System(UMUC undergraduate, 2014), an online Digital Forensics and Cyber Investigation Graduate Masters and Graduate certificate program (UMUC graduate, 2014).

A baccalaureate degree from UMUC with a major in cybersecurity requires the successful completion of 120 credits of coursework, including 33 credits for the major; 41 credits in general education requirements; and 46 credits in the minor, electives, and other degree requirements. At least 17 credits in the major must be earned in upper-level courses (numbered 300 or above). Coursework focuses on network security, digital forensics and ethics in information technology. Specific course requirements for the cybersecurity major include the following:

- Required foundation courses (9 credits): CSIA 301, CMIT 265, and IFSM 304
- Required core courses (15 credits): CSIA 303, 412, and 413; CMIT 320; and CCJS 321
- Supplemental major courses (6 credits): Chosen from CCJS 390 and 421; CMIT 321, 340, 424, 425, 440, and 460; and any CSIA
- Required capstone course (3 credits): CSIA 485

The *Digital Forensics in the Criminal Justice System* course is “An overview of the criminal justice system and the application of digital forensic evidence in criminal justice cases. The objective is to apply Constitutional and case law to the search and seizure of digital evidence, determine the most effective and appropriate forensic response strategies to digital evidence, and provide effective courtroom testimony in a case involving digital evidence” (UMUC undergraduate, 2014). Course titles and descriptions for the remaining undergraduate courses in the cybersecurity bachelor’s degree program are available from www.umuc.edu/academic-programs/bachelors-degrees/cybersecurity-major.cfm. An articulation agreement between UMUC's Undergraduate School and Graduate School allows eligible students who complete their undergraduate degree at UMUC with a major in cybersecurity to reduce their total coursework for the MS in cybersecurity or cybersecurity policy by 18 credits (UMUC, 2014)

The Masters of Digital Forensics and Cyber Investigations requires that students complete 36 credits including the following courses:

- CSEC 610: Cyberspace and Cybersecurity,
- CSEC 620: Human Aspects in Cybersecurity: Ethics, Legal Issues and Psychology,
- CSEC 650: Cyber Crime Investigations and Digital Forensics,
- CSEC 661: Digital Forensics Investigation, and
- CSEC 662: Cyber Incident Analysis and Response

The CSEC 650 course covers the theory and practice of digital forensics. Topics include computer forensics, network forensics, cell phone forensics, and other types of digital forensics. Discussion also covers identification, collection, acquisition, authentication, preservation, examination, analysis, and presentation of evidence for prosecution purposes.

The CSEC 661 covers the processes and technologies used in the collection, preservation, and analysis of digital evidence in local, networked, and cloud environments. An examination of policies and procedures related to security incidents, exposures, and risks and technologies used to respond to such threats.

All the students in the program are required to take a Cybersecurity Capstone course, CSEC 670. The CSEC 670 course is a study of and an exercise in developing, leading, and implementing effective enterprise- and national-level cybersecurity programs. Focus is on establishing programs that combine technological, policy, training, auditing, personnel, and physical elements. Challenges within specific industries (such as health, banking, finance, and manufacturing) are explored (UMUC graduate, 2014).

Resources for Online Teaching

UMUC's Virtual Classroom

UMUC uses both open source tools and commercial tools and remote virtual labs for teaching online DF courses. UMUC has its own virtual lab that has been used to teach the Cybersecurity courses. Hands-on learning is an integral part of UMUC's online classroom. UMUC uses two labs to teach Cybersecurity/Information Assurance courses, 1) the Virtual Lab and 2) the Virtual Desktop and Applications Environment.

UMUC Virtual Lab: The architecture of the UMUC Virtual lab is such that it has VMware Vcloud Director Server software, and VSphere hypervisor servers. The hardware consists of seven high end Dell PowerEdge R710 servers, Dell gigabit switches, and a Dell Storage Area Network (SAN).The lab allows at the moment a maximum of 265 VM connections concurrently. The Virtual lab isolated and is accessed through a VPN. Students are provided with two sets of instructions; one to access the VPN and the other for accessing the Virtual Lab. The virtual lab has open source tools installed.

The UMUC Virtual Desktop and Applications Environment: UMUC also has a Virtual Desktop and Applications (VDA) environment provided by a cloud service provider Aeronomy. Two courses in our Digital Forensics program and the undergraduate students use the Virtual Desktop Infrastructure part of the environment. The Virtual Desktop Infrastructure access instructions are provided by UMUC IT Services. The VDA has Guidance Software EnCase, Access Data Ultimate Toolkit and Mobile Plus installed. CSEC 661 and CSEC 662 are using the VDA lab.

Open Source Toolkits

One of the challenges facing students enrolled in online courses is having access to expensive, commercial forensic tools, such as Guidance Software EnCase, Access Data Ultimate Toolkit, and ProDiscover Forensics. Nevertheless, online students need the opportunity to gain hands-on experience with digital investigation technologies, and freely accessible open source forensics toolkits and remote virtual laboratories are viable options for distance education instructors who may not have the budget to purchase commercial forensic tools.This paper describes five open source digital forensics toolkits: (1) Sleuth Kit with Autopsy, (2) Sans SIFT Workstation, (3) DFF, (4) DEFT with DART, and (5) Helix. Open source toolkits run on a variety of operating system platforms, such as Windows, Linux, UNIX and Mac OS. Table 1 delineates these five different open source toolkits by supported operating systems, while Table 2 lists these same toolkits by supported image formats.

Table 1: Open source toolkits by supported operating systems

Open Source Toolkit	**Supported Operating Systems**			
	Windows (DOS, FAT, NTFS)	Linux (EXT)	Unix (UFS)	Mac OS (HFS)
Sleuth Kit with Autopsy	X	X	X	X
Sans SIFT	X	X		
DFF	X	X		
DEFT with DART		X		
Helix	X	X	X	

Table 2: Open source toolkits by supported image formats

Open Source Toolkit	**Supported File Formats**		
	Raw Format (DD)	Advanced Forensics Format (AFF)	Expert Witness Format (E01, EWF)
Sleuth Kit with Autopsy	X		
Sans SIFT	X	X	X
DFF	X	X	X
DEFT with DART	X	X	X
Helix	X		

The Sleuth Kit™ is a collection of command line tools for investigating disk images. These low-level tools are used to recover electronic evidence; its core functionality is the in-depth analysis of volume and file system data (Sleuth Kit, 2014). Autopsy™ is a digital forensics platform and graphical interface for Sleuth Kit (Autopsy, 2014). The Sleuth Kit™ and Autopsy™ run on Windows, Linux, OS X, and other Unix platforms.

The SANS Investigative Forensic Toolkit (SIFT) Workstation is a VMware appliance, pre-configured with the necessary tools to perform detailed digital investigations. An international team of forensics experts created the SIFT Workstation and made it available to the whole community. SIFT version 3.0 matches modern forensic tool suites demonstrating that advanced investigations can be accomplished using freely available and frequently updated open source tools (SANS Institute, 2014). The SIFT Workstation runs on both Windows and Linux platforms.

The Digital Forensics Framework (DFF) was updated in February 2013 and is open source digital investigation software built on top of a cross-platform Application Programming Interface (API). DFF is appropriate for both novice and professional examiners. Separate user and developer guides are available online supported by a rich community via blog, wiki, forum and an IRC chat channel (Digital Forensics Framework, 2014). DFF runs on both the Windows and Linux platforms.

The Digital Evidence & Forensic Toolkit (DEFT) is made up of a live GNU/Linux distribution and includes the Digital Advanced Response Toolkit (DART). In addition to a long list of open source Linux applications and scripts provided in DEFT, the DART suite contains another impressive list of open source Windows applications. DEFT and DART are used to support the digital forensics course currently offered at the University of Bologna and many other Italian universities (Fratepietro, Rossetti, & Dal Checco, 2012).

Helix was designed to be forensically sound and very careful not to touch the host computer in any way. As a live Linux distribution, Helix focuses on incident response. Student examiners must have a sound understanding of incident response and forensic technique for proper use of Helix. For example, this tool can be used to scan for graphic evidence, such as JPEG and GIF images on a live Windows system. Helix executes on the Windows, Linux and UNIX platforms (SecTools, 2014)].

Remote Virtual Labs

The three remote virtual labs - CSSIA, RAVE, and VITAL - suitable for teaching digital forensics and cyber investigations at a distance are discussed. CSSIA, the Center for Systems Security and Information Assurance at Moraine Valley Community College in Illinois is a National Science Foundation Advanced Technological Education (ATE) National Resource Center. One of its incredible resources is the development and maintenance of national infrastructure models for learning based on scalable and affordable remote virtual lab environments. The standardized virtual data center provides the means for cybersecurity educators to develop multiple curriculums that can easily be deployed and shared by institutions interested in teaching all types of cybersecurity programs. The CSSIA virtual environment currently supports five complete courses and plans to develop additional courses in digital forensics as well as Microsoft and Linux OS platforms (Center for Systems Security and Information Assurance, 2013).

With initially funding from the National Science Foundation of the United States, the Remote Access Virtualized Environment (RAVE) was created to help meet the national need for experienced cybersecurity workforce by providing access to valuable hands-on laboratory opportunities for students around the nation. RAVE is a remotely accessible state-of-the-art virtual lab environment, allowing thousands of students from a wide range of institutions to enrich their educational experience. This system was developed and tested at the University of Alaska Fairbanks and is replicated at the United States Military Academy at West Point.

RAVE provides access to cybersecurity lab facilities and materials to a wide range of intuitions, and, consequently, provides more students with empirical learning opportunities in this critically important field. Qualitative and quantitative metrics inform the development of new lab-based learning activities (Nance, 2010).

The Virtual Information Technology and Assurance Lab (VITAL) at New York University Polytechnic (NYU-Poly) was created in response to the critical need for a simple virtualization environment designed for teaching cybersecurity courses. Utilizing the open source XEN virtualization environment, VITAL was specifically customized to be easy to use for both students and professors. VITAL makes use of Virtual Machines (VMs) within a closed networking environment, providing hands-on access to a diverse blend of operating systems (e.g., Linux and Microsoft) and digital forensics tools. All access to VITAL is done via a web browser. VITAL is designed to work with a wide range of browsers (Firefox 3+, IE8, Safari 4) under a variety of OS (BSD, Linux, Windows, Macintosh). VITAL was initially funding by a NSF capacity building grant with continued support from NYU-Poly Department of Computer Science and Engineering and the NYU-ePoly Online Learning Program. Lab and lesson materials are available for download along with the installation materials and documentation (NYU-Poly, 2014).

Lessons Learnt from Our Experiences

Feedback from students indicates that lab exercises appear to be a very effective method for teaching digital forensics. Students would like more labs to be added to the classes. As most of the courses are being migrated to the Virtual Desktop and Applications (VDA) environment, the resources will be more elastic and more hands-on exercises will be available. The majority of the students commented that the commercial digital forensic toolkit *Encase* from Guidance Software is a very powerful with too many features, making it less user friendly. Another student team exclaims “It is NOT always possible to recover everything and it is NOT always possible to figure out 100% of the crime given the evidence that is recovered. The larger the volume of files to be analyzed, the more complex and time consuming the investigation becomes.”

UMUC faculty and students use several Internet-based resources that are very useful to supplement the chosen textbooks for the online digital forensic courses. These include:

- *Best Practices In Digital Evidence Collections*(SANS, 2009). This discusses evolving evidence handling procedures.
- *Best Practices for Computer Forensics* (Scientific Working Group on Digital Evidence, 2013). This covers all the best practices from seizing evidence, equipment preparation, forensics imaging, forensic analysis and examination and documentation and reporting.
- *Best Practices for Seizing Electronic Evidence, A Pocket Guide for First Responders* by the U.S. Department of Homeland Security (United States Secret Service, 2014). This is a document developed by a working team of various law enforcement agencies who convened to identify common issues encountered in today’s electronic crime scenes.
- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* by the U.S. Department of Justice (Jarrett, 2010). This document explains the constitutional limits of warrantless searches and seizures in cases involving computers, with the Fourth Amendment limiting the ability of government agents to search for and seize evidence without a warrant.
- *FBI Law Enforcement Bulletin*(The FBI, 2001). This is a good document that reviews some of the tools and methods an investigator can use to conduct investigative analysis and identify suspicious financial transactions.

- *Good Practice Guide for Computer-Based Electronic Evidence*(Association of Chief Police Officers, 2014).
- *Best Practices for Computer Forensics*(SWGDE, 2006) and *A Simplified Guide To Digital Evidence* (National Institute of Justice, 2008)are also very useful for teaching digital forensics online.

Conclusion

This paper describes UMUC's virtual lab for teaching digital forensics and cyber investigation online as well as feedback from distance education students enrolled in the master's degree program. Additionally, it investigates five open source toolkits and three remote virtual labs, which were initially funded by the National Science Foundation of the United States in response to the urgent need to have well-educated cybersecurity practitioners. Open source toolkits and remote virtual labs are becoming a viable option for effectively teaching digital forensics and cyber investigations online. They provide the previously missing opportunity for the growing number of online students to gain the same hands-on experiential education as delivered in a face-to-face classroom setting.

References:

ACM, & IEEE. (2013, December). *Computer Science Curricular Guidelines 2013.* New York: Association for Computing Machinery. doi:10.1145/2534860

Allen, I. E., & Seaman, J. (2007). *Online Nation: Five Years of Growth in Online Learning.* The Sloan Consortium. Retrieved from http://sloanconsortium.org/publications/survey/online_nation

Association of Chief Police Officers. (2014, February). *Good Practice Guide for Computer-Based Electronic Evidence* . Retrieved from ACPO: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Autopsy. (2014). Retrieved from www.sleuthkit.org/autopsy/

Center for Systems Security and Information Assurance. (2013). *NSF ATE National Resource Center*. Retrieved from CSSIA: www.cssia.org

CNCI Initiative 8. (2008, January). *National Security Council.* Retrieved from The Whitehouse: www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Davis, C., Cowen, D., & Philipp, A. (2005). *Hacking Exposed Computer Forensics.* New York: McGraw-Hill/Osborne.

Digital Forensics Framework. (2014, May). *DFF*. Retrieved from www.digital-forensic.org

Evans, K., & Reeder, F. (2010, November). *Human Capital Crisis in Cybersecurity: Technical Proficiency Matters.* CSIS Commission on Cybersecurity for the 44th Presidency. Retrieved from http://dspace.cigilibrary.org/jspui/bitstream/123456789/30098/1/A%20Human%20Capital%20Crisis%20in%20Cybersecurity.pdf?1

Fratepietro, S., Rossetti, A., & Dal Checco, P. (2012). *DEFT and DART*. Retrieved from www.deftlinux.net/doc/EN-deft7.pdf

Jarrett, H. M. (2010). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation.* Washington D.C.: U.S. Department of Justice. Retrieved from http://publicintelligence.net/u-s-doj-searching-and-seizing-computers-and-obtaining-electronic-evidence-in-criminal-investigations/

Nance, K. (2010, September 15). *Collaborative Research: Remote Access Virtualized Environments (RAVE): Piloting a National Infrastructure for Cybersecurity Education*. Retrieved from NCET:

http://center.ncet2.org/index.php?option=com_patents&controller=awards&tmpl=component&view=awards&layout=award&frame=awards&user=46028&id=1121_nsf

National Institute of Justice. (2008, April). *A Simplified Guide to Digital Evidence*. Retrieved from http://www.crime-scene-investigator.net/SimplifiedGuideDigitalEvidence.pdf

NYU-Poly. (2014). *About VLab*. Retrieved from CyFor at NYU-Poly: http://cyfor.isis.poly.edu/13-about_vlab.html

Obama, B. (2009, May 29). *Remarks by the President on securing our nation's cyber infrastructue.* Retrieved from The White House: www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

SANS. (2009, September). *Best Practices in Digital Evidence Collections*. Retrieved from SANS Digital Forensics and Incident Response Blog: http://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection

SANS Institute. (2014). *SIFT Workstation*. Retrieved from http://computer-forensics.sans.org/community/downloads

Scientific Working Group on Digital Evidence. (2013, September). *SWGDE Best Practices for Computer Forensics v. 3.0*. Retrieved from https://www.swgde.org/documents/Current%20Documents/2013-09-14%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-0

SecTools. (2014). *Helix*. Retrieved from Top 125 Network Security Tools: http://sectools.org/tag/forensics/

Sleuth Kit. (2014). Retrieved from http://www.sleuthkit.org/sleuthkit/

SWGDE. (2006, July). *Best Practices for Computer Forensics*. Retrieved from Scientific Working Group on Digital Evidence: http://www.oas.org/juridico/spanish/cyb_best_pract.pdf

The FBI. (2001). *FBI Law Enforcement Bulletin*. Retrieved from http://leb.fbi.gov/

U.S. Department of Homeland Security. (2007). *Best Practices For Seizing Electronic Evidence v.3: A Pocket Guide for First Responders.* United States Secret Service. Retrieved from http://www.forwardedge2.com/pdf/bestPractices.pdf

UMUC. (2014). *Articulation Agreements between The Graduate School and Undergraduate School*. Retrieved from www.umuc.edu/academic-programs/upload/articulation-agreements.pdf

UMUC graduate. (2014). *Master of science in digital forensics and cyber investigation*. Retrieved from UMUC: http://www.umuc.edu/academic-programs/masters-degrees/digital-forensics-and-cyber-investigations.cfm

UMUC undergraduate. (2014). *Bachelor's degree requirements for the cybersecurity major*. Retrieved from UMUC: www.umuc.edu/academic-programs/bachelors-degrees/cybersecurity-major.cfm

United States Secret Service. (2014). *Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders*. Retrieved from http://www.forwardedge2.com/pdf/bestpractices.pdf