STEALing Lab Support for Digital Forensics Education

Timothy M. Vidas
Naval Postgraduate School
tvidas@nps.edu

David A. Branch
University of Nebraska at Omaha
dbranch@mail.unomaha.edu

Alex Nicoll
BAE Systems Inc.
alex.nicoll@baesystems.com

Abstract

Digital Forensics is still an emerging field of study where the best methods for gaining subject matter expertise are still unclear. This paper presents a worked example of pairing traditional learning methods with a highly adaptive laboratory environment in a university setting.

The example environment and pedagogy presented here represent a unique collaborative relationship between academia, industry and government parties. Several learning styles have been employed at the university level to provide opportunities for conventional students to excel, meanwhile training and topical exploration opportunities exist for regional industry and government parties.

1. Introduction

The University of Nebraska at Omaha (UNO) is a National Security Agency Center of Excellence (NSA CoE), which among other things allows National Science Foundation (NSF) Cybercorp Scholars to participate in the academic program and requires a community service element of the university. Community Service can be quantified in many ways; one way UNO services the surrounding community is by extending Digital Forensic Education through the Nebraska University Consortium on Information Assurance (NUCIA). NUCIA offers Forensic education in five core ways: traditional academic undergraduate coursework, custom bootcamp style coursework, partnered bootcamp style courses, requested subject based tutorials and through training sessions at conferences and workshops.

The emerging field of Digital Forensics has distinct perspectives. Even the "cyber" names and inconsistency in course titles demonstrate the infancy of the field. The diagram shown in Figure 1 details three distinct viewpoints (Law Enforcement, Military, Industry) [1] on what is slowing becoming known canonically as "Digital Forensics." NUCIA attempts to be active in all three viewpoints both by participation in related groups and by cultivating graduates that can quickly and efficiently integrate into those areas.

Many of the strategies presented here may be expanded from Digital Forensics to generally apply to information assurance education.

2. Core Digital Forensic Educational Endeavors

This section details the five core undertakings that NUCIA maintains in the Digital Forensics field.

2.1. Traditional academic undergraduate coursework

The University of Nebraska at Omaha is on a 15-week semester schedule, largely on site. In order to keep its courses fresh and relevant, and its instructors at the top of their field, NUCIA brings together a blend of academics and practitioners on a topical basis. This topical pairing allows students to experience real-world examples through lab activity and narrative learning that may not otherwise be available.

The luxury of having a rather large lab environment as well as leveraging unprecedented industry partnerships places NUCIA in a unique position to foster the blending of hands-on experience with traditional lecture based learning. Laboratory resources include large quantities of traditional digital forensics equipment, such as hardware write-blockers and hard disks, for students to use during hands-on laboratory exercises. Partnership agreements have allowed NUCIA to use the top software in the field, such as EnCase Enterprise and the Forensics ToolKit (FTK), on every machine in the laboratory environment. This gives students a concrete way to not only learn the tools, but compare them to each other and to other alternatives, such as Sleuthkit and Autopsy.

This work was funded in part by AFOSR Grant Award # FA9550-04-1-0232

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, United States Navy, Department of Defense, or the U.S. Government.

1530-1605/08 $25.00 © 2008 IEEE

The lab environment is flexible enough to provide class wide as well as smaller group or individual activities. Students not only utilize the lab environment to complete assignments or self-paced labs, but also to perform related activities on a personal exploration basis. Some students who are involved in professional forensics activities actually “bring their work to school,” which is encouraged. Under the right circumstances this can provide real-world case studies and discussion points for class activity.

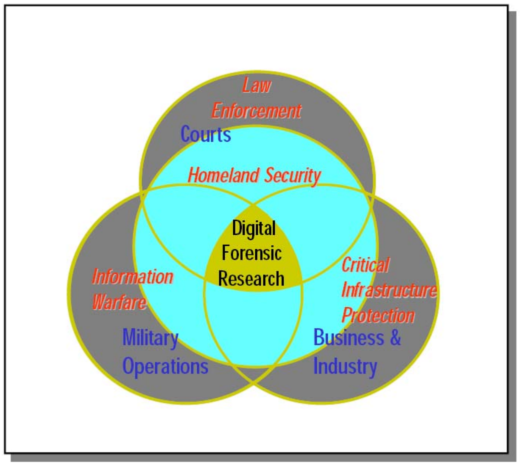

Figure 1: Nucleus of Digital Forensic Research

Students are encouraged to participate in Capture the Flag (CTF) exercises. Participation is on a voluntary basis and the participation (or lack of) is not reflected in the curriculum at all, yet students still actively choose to give up personal time in order to participate. “Live Fire” CTF exercises may be the sole way for participants to safely learn unique under pressure skills[2]. Current instances of CTF exercises blend problem-based and collaborative learning styles with that added aspect of immediacy. The unique lab structure allows for physically separated teams (e.g. “red” and “blue”) to partake in an “internal” CTF that is hosted on a lab isolated network, and also allows for certain sanitized machines to be used for “external” academic CTF activities such as UCSB iCTF[3] and U-Dresmod’s CIPHER[4].

Several learning methods are currently being investigated not only in Digital Forensic education, but in the education field as a whole. Web-based instruction is of particular interest[5,6]. One method that seems to have particular success with digital forensic students in our environment, is the use of puzzles. Puzzles are available in two forms to digital forensic students. General “puzzle boxes” are available to all Information Assurance students. These are faculty configured computers that are always available on the lab network, but typically no physical access is granted to the students. A solution to such a puzzle may entail finding a mis-configuration such as an anonymous ftp server that allows uploading or over-writing to a web server directory. The second type of puzzle is distributed only to the forensic students. These puzzles are comprised of facets of digital forensics that may not be covered in class due to time constraints, or may be offered only through special advanced topics courses. The puzzles are pre-packaged sets of evidence, and the related computing environment that allow students to explore topics of interest, such as peculiar EXIF data in JPG files. The forensic puzzles are progressive: only one is available at any time. Once the current puzzle has been solved, another potentially more difficult puzzle is immediately available. Depending on participation levels, the number of puzzles exhausted in one semester varies. Students solving a puzzle must provide a written solution. Students solving a forensic puzzle must also be ready to verbally discuss the puzzle at the beginning of the next class period.

Though a few Forensic puzzles may have a small extra-credit value associated with them, the incentives for students to solve puzzles are largely reward based. Candy, lunch, minimal hardware (leftover thumbdrives, books, iPods, etc) and above all the prestige of solving the puzzle drive student participation.

2.2. Custom Bootcamp Style Coursework

Partnerships and contracted work with companies like Lockheed Martin have resulting in some very interesting projects such as the Rapid Response Cyber Forensics (RRCF) program. RRCF is a custom designed training program that provides an array of participants with basic forensic training. Participants are carefully chosen by Lockheed Martin and then screened with a pre-quiz from the course instructor in order to maximize the potential for successful completion of the weeklong course. In addition to the hand selected industry participants, some interested university students and faculty may be permitted to sit in on a course, and in some cases students are employed to refine or create material for inclusion in the program.

2.3. Partnered Bootcamp Style Coursework

NUCIA and the Peter Kiewit Institute (PKI) have forged unique relationships with leading vendors to ensure the highest quality of education to their student body. The partnerships with Guidance Software and AccessData are of particular importance to digital forensics education, and help in two distinct ways: providing the use of software for academic purposes, and providing a vector for tool training in the area. Not only are several copies of the proprietary software available for use in the lab, but both vendors have either trained resident faculty to be course instructors or lend their own instructors to facilitate in-house, certified training for some of their products. This local training is substantially cheaper to many law enforcement and industry members due to the reduced travel costs when compared to another coastal training facility, and empty course seats can be occupied by a limited number of university students or faculty at no cost.

2.4. Requested Subject Based Tutorials

NUCIA hosts and participates in numerous activities with the local Cyber Crime Task Force (CCTF), Nebraska Computer Emergency Response Team (NeCERT), FBI InfraGard, High Technology Crime Investigation Association (HTCIA), local and state government, etc. Many of these groups have monthly or quarterly meetings in which the group requests focused training on a particular subject. NUCIA helps meet this need by either providing training directly from faculty, procuring a subject matter expert, or in some cases mediating a dialog between a student and the group to provide the group with a faculty advised student presentation and the student with an opportunity to obtain unique research feedback in a friendly, low stress environment.

2.5. Training Sessions at Conferences and Workshops

Finally, NUCIA provides training at certain conferences and workshops. In some cases, such as the Working Connections IT Conference, some equipment is provided at a remote location (much of NUCIA's specialty equipment is somewhat mobile as it is kept in a large, wheeled toolbox). In other cases, such as the NeCERT conference, the proximity of the conference to the university allows use of the physical lab environment. Bringing conference attendees to the lab, allows for a rich, immersive experience and can procure dialog with local parties that would otherwise be lost.

3. Need for the lab

As with much of computer security, Digital Forensics can be thought of as equal parts science and art[7]. The science can arguably be taught in lecture and via books. One might argue that the art must be experienced. Traditionally this aspect of education is gained through on-the-job training. In order to create graduates that are more ready for the workplace, and in order to reinforce lecture topics students needed an environment to cultivate such learning.

To support students in the information assurance program where general university lab facilities may not fit the need, specialized Security Technology Education and Analysis Laboratories (STEAL) were formed. STEAL aims to provide a constructivist learning environment by being a Rich Environment for Active Learning as explored in [8], and in order to maximize student learning several different pedagogical methods needed to be employed.

The creation of the lab required support from several parties. The university and PKI pledged support in not only the usage of the room, but also in providing contemporary client computers. NUCIA supports the lab not only through funding for servers, LCD monitors, and specialized software, but also through the invested time of faculty who maintain and utilize the shared lab. Access to the labs is restricted via proximity card, but this does not preclude non information assurance people from using labs, it only ensures notification and provides a control mechanism to prevent research and class interruptions. In fact, there has been great success in using scheduling software [9] in order to prioritize lab usage requests.

4. Lab design

Several design choices were made during the creation of each lab and insight on those choices is provided in this section for others to take into consideration when designing their own labs.

4.1. Physical Air Gap

A design choice was made to keep the labs isolated (aka "air gapped") [10,11]. The isolation provides piece of mind to the network operations staff in the building as well as the students and faculty running security related experiments in the lab, and allows students to experience what it would be like to work in a controlled facility after graduation.

The isolation also creates some interesting issues with lab management. For example there is no Internet connectivity so downloading software, research through the Internet and connecting Virtual Private Networks for academic CTF events is problematic. While any student may bring media into the lab, similar to controlled facility operations, only certain parties are designated with privileges to sanitize and bring media out of the lab. Also, in addition to academic honesty and ethics forms signed for every class, students with lab access must also sign lab usage and ethics forms every semester.

4.2. Purpose Driven Labs

In order to facilitate the digital forensic education, the need for differing types of lab environments was realized. Currently, NUCIA is supplied by PKI and the university with three different STEAL spaces: STEAL1, STEAL2, and STEAL3. Each has a unique and important role.

STEAL1 is primarily a research lab. Composed of seven *pods*, students, faculty members, or particular outside third-party partners are able to reserve the use of a pod at any time. The greater purpose behind STEAL1 is to provide an environment that is always available to everyone. Students are often encouraged (and occasionally required) to do their assignments in this lab. In addition to homework, students are encouraged to take on personal-learning projects, and to use this flexible, isolated environment to learn ideas or methods not able to be covered in a traditional classroom. The lab environment provides the venue for learners of any kind to make real-life type mistakes, and to have no consequences for those mistakes.

STEAL1 also hosts a variety of *minilabs* designed to bring students up to speed in a particular area, re-enforce lecture concepts, or better prepare students for more difficult activities. Minilabs are largely a self-paced resource-based learning activity designed in such a way that all the tools needed for a lesson are readily available in the STEAL environment. Students can simply pick any minilab at their leisure and work through the lesson in 30-40 minutes. While there are typically questions for thought at the completion of a minilab, they are not actually part of any curriculum and are not graded. The minilabs are configured hieratically: one minilab may require another as a prerequisite. Additionally, some classes may require the knowledge that should be gained from performing a minilab as a prerequisite for an assigned lab activity.

Over the years of its existence, it has been found that several students have spent the majority of their free time in the lab, using its resources for homework as well as personal research and investigation.

STEAL2 is primarily a presentation and instruction lab. It was decided during the labs conception that a "nicer" space was needed within the same isolated environment, one that could be utilized for special demonstrations to classes as well as community, government, and military partners. Consisting of more than 50 workstation PCs and 30 "executive" style chairs, it provides a place that a group can comfortably participate in security discussions, demonstrations, and exercises.

STEAL3 is a student office and lounge. In addition to STEAL lab assistants, graduate assistants, teaching assistants, and students hired for research activities related to information assurance all share a common working area. This environment fosters discussion, whether intentionally or by way of natural interactions. STEAL3 allows the information assurance students a place they can call their own, work comfortably on projects as groups, and simply interact. The motive behind this space is growth of close professional relationships between other students and nearby faculty, relationships that will last beyond the degrees and into "real-life." While not electronically isolated like STEAL1 and STEAL2 (and thus not used for many types of research), this environment has proven just as necessary in providing students with the resources and environment they need to be successful.

4.3. Grouped Pods

The seven pods in STEAL1 (see Figure 2) each consist of five machines: three mid-ranged workstations and two high-end workstations/low-end servers. They are situated along the perimeter with a central conference table for brainstorming sessions. Each pod is equipped with a 2xN KVM and set up for one or two individuals to multiplex between the five workstations. This facilitates both individual and paired activities for lab assignments, personal experimentation and in some cases homework.

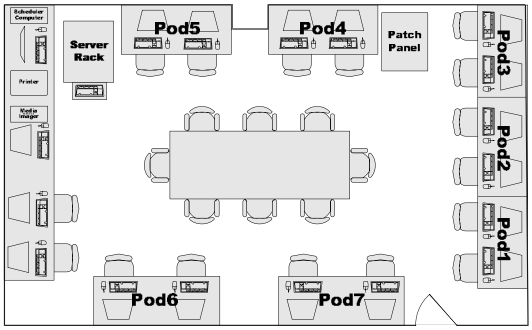

Figure 2: STEAL1 Floor Plan

The eight pods in STEAL2 (see Figure 3) each currently consist of six machines: five workstations and one thin client. Pods in this lab are configured in an “L” shape with four stations and a 4xN KVM in order to facilitate group activities. The pods were then carefully placed to allow the vast majority of the lab occupants to readily see the two instructor projection screens. It is not uncommon to teach the vast majority of a security related class using this lab instead of a traditional classroom. Additionally at any given time, the lab may be used for boot-camp style training, or for other related exercises that require the physical space available in the lab. This lab is designed to foster group learning in either several groups of about four or a single larger group of up to about 50.

STEAL3 cultivates a different pedigree of candid discussion for students and faculty that are not bound by the typical time boundary that a scheduled class or lab activity presents. In many ways STEAL3 may not be considered a laboratory, and it is definitely configured differently from STEAL1 and STEAL2. It is fully connected to the Internet, has no KVMs and the cabling is not hardwired leaving the furniture completely reconfigurable. In different contexts the entire space can be thought of as several pods of size 1 or as a single large pod. It’s connection to outside networks preclude STEAL3 from participating in STEAL network shared by the other two labs.

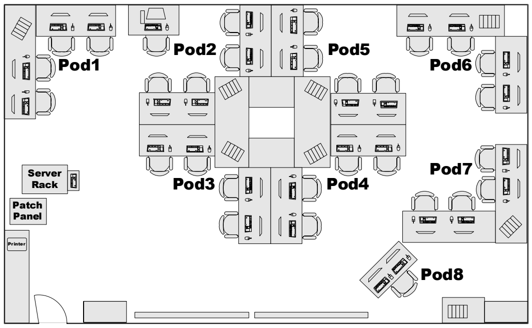

Figure 3: STEAL2 Floor Plan

4.4 Network Topology

The above mentioned pods in STEAL1 and STEAL2 are all hardwired from a networking rack in each lab. The rack is physically located in each lab to both help ensure the isolated nature of the lab and to allow ready access for students who are attempting to learn networking topics or that need to physically reconfigure part of a lab for research. The network core consists of several layer 2 and 3 devices located in each lab and connected directly via fiber. Connecting both labs into a unified, yet still isolated network allows for sharing of resources between the labs which reduces the amount of management required. Additionally it uniquely permits certain activities such as isolated lab-to-lab CTF exercises.

In the labs’ default configuration, each pod is assigned its own subnet. The internal DHCP and DNS servers assign addresses and names that correspond to machine IDs. The network core is configured to limit multicast traffic between pods which reduces capture volume from other pods when sniffing. In the main, the lab is left for configuration as needed.

At any given time these racks may also host other miscellaneous network devices used for experimentation such as hubs, network taps, protocol analyzer, Cisco PIX firewalls, a Public Switched Telephone Network (PSTN) emulator, etc.

5. Lab Logistics

At times the labs are in constant contention between different potential users. Given the mission of each lab, priorities are assigned and access is granted in different ways. The unique nature of the labs create certain logistical issues that need to be addressed.

5.1 Controlled access

All three labs have controlled access. STEAL1 and STEAL2 via proximity card, and STEAL3 via traditional key. Access to all labs is granted as needed and the access list is checked each semester. Lab entry is logged centrally with the university. Any student can request access to STEAL1, while STEAL2 access is limited fairly strictly to NUCIA faculty and lab assistants.

Once in the lab, the STEAL network provides several central services. Among these services are a traditional Windows based Domain, a central Linux based server, and a large storage repository. These core services are hardened and designed to have high network availability. Access to these services is granted through individual accounts for each user which allows for private storage for active research projects and accountability for the lab resources.

5.2 Media and Usage Policy

The lab isolation creates an interesting situation where an air gap needs to be crossed in order to bring software into the STEAL network. Generally stated, the policy allows any media to be brought into the lab, but no writable media to be taken out of the lab. This policy is outlined during class and/or lab orientation and students sign to acknowledge the understanding of the policy. The policy is posted in the lab and available on the external lab website. To meet certain homework needs, there are internal printers or homework results can be stored in special directories on the shared storage for the corresponding faculty member to later acquire or grade in the lab.

5.3 Dedicated Personnel

The complexity of the STEAL environment and the shear volume and diversity of usage warrants dedicated management. A traditional model of having a single faculty lab manager along with one or more student lab assistants has worked well. Lab assistants generally sit in STEAL1 and have regular, posted working hours. In addition to maintaining the lab, lab assistants are familiar with the content in minilabs and many of the class assigned activities in order to help students in a variety of classes when required. It is up to the lab assistants to help reconfigure the lab environment, perform the network administration activities, create and maintain client images, and enforce the STEAL policies.

5.4 Internal Website

An internal website is maintained by the lab manager and lab assistants. The website is centrally located for ready access from any client in either STEAL1 or STEAL2. Students can find documentation on how to utilize lab services, network diagrams, frequently asked questions, and all of the available minilabs content is on this site. This gives students access to the self paced learning in a variety of subjects and the opportunity to find answers to questions in the absence of a lab assistant.

5.5 Lab Software

One of the critical advantages that STEAL offers to the Digital Forensics domain is lab software.

5.5.1 Industry Agreements. In addition to the typical agreements such as Microsoft's Academic Alliance through the university, NUCIA has struck agreements with PKI partners Guidance Software and AccessData that allow all STEAL client computers to have EnCase and FTK installed. This allows students to experience contemporary tools that are not typically available at the university setting. Pairing software such as EnCase Enterprise with the dynamic and diverse hardware set available in STEAL allows for a very rich experimentation platform. It also allows STEAL to provide a testing environment where local law enforcement and industry members can try full version products with faculty specialists nearby.

5.5.2 Virtualization. Many institutions are moving or considering moving to using virtualization for learning in many topical areas including Digital Forensics [6,12,13]. In some cases VMWare or VirtualPC are used in the STEAL environment, but in large the machines are used directly. The close proximity to networked storage and the high speed network allow the re-imaging of client machines to happen very quickly. In some cases, such as using Symantec Ghost to image Windows XP with a full array of forensic software loaded, all pods of both labs can be completely re-imaged for a forensics class in less than 5 minutes. Some genres of experimentation simply don't work in a virtualized environment, and some genres require such an environment; STEAL can provide both.

The lab actively maintains *working loads* (such as Symantec Ghost images) for the client machines for approximately 30 different "cleanly" installed operating systems, and many more custom loads so support various lab exercises, minilabs, class activities and research projects. Similar VMWare virtual machines are also maintained.

5.5.3 Air Gap Workarounds. In order to provide functionality that some users have come to expect in lab situations, several workarounds have been implemented to make the lab more efficient. Two examples are given here: default web locations and Fedora Core yum service.

Many applications automatically visit certain web locations. Internet Explorer is set to visit a particular web address when it is first executed. Various software packages access different time (NTP) servers. Some software simply rely on the existence of particular popular web sites (e.g. www.google.com) to assess web connectivity which affects software functionality. Network analysis can show that simply creating "dummy" DNS records, IP addresses, web sites, and in some cases providing redirection can drastically improve the lab experience. For example, without altering the default configuration of a "cleanly" installed Windows client, the default home page for Internet Explorer will yield an internal STEAL web page.

Package management in Linux has always had its complexities. Over the years, automatic package managers such as apt, urpmi, and yum have gotten better. Contemporary package managers can determine the dependencies and automatically download all the software needed to install a particular package. Unfortunately, this software feature assumes that access to the remote software repository is available.

By mirroring the entire repository and having the internal DNS records for the original repository point to an internal repository, standard Linux clients can successfully use package managers to automatically install software. This mirror is performed via an Internet connected machine and then imported into the STEAL environment on regular intervals. As a fringe benefit this also allows for the repositories to be used long after the particular OS version that is no longer maintained by the original creators.

5.6 Lab Hardware

The STEAL maintains a variety of standard and specialized equipment, both for general information assurance education, and for specific topical areas such as Digital Forensics.

5.6.1 Machines All of the machines are of similar pedigree. Keeping the hardware configuration to a minimum allows the lab to maintain a very diverse software set without worrying much about peculiarities such as particular drivers. Almost all of the pod machines are on a three year rotation and are provided through PKI partners IBM, SUN and DELL.

5.6.2 Network The STEAL1 and STEAL2 pods each have network junction boxes that are hardwired to their respective network racks. Students gain real-world experience by actively participating in the physical installation of the lab hardware. All of the core network devices were donated by PKI partners Foundry Networks and Force10.

5.6.3 Unique Hardware Some research projects call for very specific hardware, exploring the forensic acquisition possibilities for an Apple computer, or a popular MP3 device, for example.

The forensic endeavors are supported by a variety of dedicated equipment both for individual experimentation and large group activities. This equipment ranges from hardware IDE-to-firewire write blockers for every client in STEAL2, to a single forensic USB-to-USB bridge, a forensic card reader and adaptable hardware imaging kits for all types of media.

To facilitate rapid reconfiguration, all machines in the lab are configured for Pre-boot eXecution Environment (PXE), as well as networked power strips. The power strips are managed on a separate VLAN that is connected to the central server. The combination of the PXE and the networked power strip allows the machines to be powered on, PXE booted to a automated Symantec Ghost client and essentially automatically imaged. The granularity of the power strips also allow individual pods, or any subset (such as monitors only) to have their power source toggled.

All the unique, individual machines and specific hardware purchased for specific projects were purchased by NUCIA through money acquired through partnership activities or grants.

5.7 External Lab Scheduler

Using a central self scheduling service external to the labs has been quite effective. Parties wishing to use a pod in STEAL1 can schedule the pod right up until real-time if the pod is still unoccupied. If a pod that is needed has already been scheduled, the software allows for email notification to the other party so collisions can be worked out. Similarly, faculty members have the ability to reserve STEAL2 for activities.

The scheduling service also provides several peripheral benefits such as the ability to monitor overall lab usage and provide a daily/weekly calendar for display.

6. Conclusions

A combination of academic, industry and government entities work together to make STEAL a success. The unprecedented partnerships with key forensic software vendors places NUCIA in a unique position to service the surrounding community and to create exemplary graduating students. The assembly of all three parts of the Nucleus of Digital Forensic Research (Figure 1) make the University of Nebraska at Omaha a logical place for Digital Forensic Research to flourish.

The STEAL environment has proven to be an effective environment for many different pedagogic models: constructivism, resource and problem-based learning, collaborative learning, and narration. The current state of the labs serve as a working example of how a Rich Environment for Active Learning [8] can be applied to digital forensic education and easily expanded to information assurance education.

7. Citations

[1] G. Palmer, "A Road Map for Digital Forensic Research", Utica, NY, November 6, 2001.

[2] C. Eagle, J Clark. "Capture-The-Flag: Learning Computer Security Under Fire", Proceedings from the Sixth Workshop on Education in Computer Security (WECS6). Monterey, CA. July 12-14, 2004.

[3] iCTF: International Capture the flag Competition. Hosted by the University of California Santa Barbara. Homepage:
http://www.cs.ucsb.edu/~vigna/CTF/

[4] CIPHER: Challenges in Informatics: Programming, Hosting and Exploring. Hosted by the RWTH Aachen University. Homepage:
http://nets.rwth-aachen.de/~lexi/cipher.php

[5] M. Bishop, "Teaching Context in Information Security", Proceedings of the Sixth Workshop on Education in Computer Security. Monterey, CA. July 12-14, 2004. pp. 29-35.

[6] G Kessler, "Online Education in Computer and Digital Forensics: A Case Study", Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS07). Waikoloa, Hawaii. Jan 3-6, 2007.

[7] Bishop M. Computer Security: Art and Science. Addison-Wesley. Third printing, August 2003.

[8] R. Grabinger, J Dunlap, "Rich Environment for Active Learning: A Definition," ALT-J Association for Learning Technology Journal, Issue 3, No. 2. 1995. pp 5-34.

[9] Online Resource Scheduler software. Homepage:
http://ors.sourceforge.net/

[10] J. Hill, C. Carver, J Humphries, U Pooch. "Using an isolated network laboratory to teach advanced networks and security", SICCSE BULL. 2001. pp 36-40.

[11] M. Bishop, L. Heberlein, "An Isolated Network for Research", 19th National Information Systems Security Conference. Baltimore, MD. Oct 22-25, 1996. pp 349-360.

[12] A. Arnes, P. Haas, G. Vigna, R Kemmerer, "Digital Forensic Reconstruction and the Virtual Security Testbed ViSe", Proceedings of the SIG SIDAR Conference on Detection of Intrusions and Malware and Vulnerability Assessment 2006 (DIMVA). Berlin, Germany. July 13-14, 2006.

[13] J. Hu, D. Cordel, C. Meinel, "A Virtual Laboratory for IT Security Education", Proceedings of the Conference on Information Systems in E-Business and E-Government (EMISA). Luxembourg, Oct. 6-8 2004. pp 60-71.

[14] R. Vaughn, D Dampier, "The Development of a University-based Forensics Training Center as a Regional Outreach and Service Activity", Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS07). Waikoloa, Hawaii. Jan 3-6, 2007.

Additional information may be found at:

http://nucia.unomaha.edu/
http://nucia.unomaha.edu/steal/labs.php
http://www.pki.nebraska.edu/default.html
http://www.unomaha.edu
http://www.guidancesoftware.com/
http://www.accessdata.com/