Experience of Incorporating NIST Standards in a Digital Forensics Curricula*

Sankardas Roy
Computer Science Department
BGSU
Ohio, USA
sanroy@bgsu.edu

Yan Wu
Computer Science Department
BGSU
Ohio, USA
yanwu@bgsu.edu

Kristina N. LaVenia
Leadership Studies Department
BGSU
Ohio, USA
klaveni@bgsu.edu

***Abstract*—Recently, Bowling Green State University (BGSU) has started to offer a Digital Forensics specialization program for Computer Science undergraduate students. We (the authors of this paper) actively took part in developing and evaluating the curricula for this program. The overarching goal of the specialization program is to build a digital forensics workforce for the state and the nation. Realizing the importance of standards of digital forensics tools in real-life forensic examinations, we made an effort to incorporate lessons on standardization in the curricula. In particular, so far we incorporated National Institute of Standards and Technology (NIST) standards for three digital forensics topics (Hardware Write Blocker, Deleted File Recovery, and Mobile Forensics) in the curricula. We faced many challenges over the journey but also attained some success. In this paper we share our experience to the community. We believe this account may be helpful to others who are about to begin such a journey.**

***Index Terms*—Digital Forensics (DF), curricula development, NIST standards, Computer Forensics Tool Testing (CFTT), Hardware Write Blocker (HWB), Deleted File Recovery (DFR), Smart Phone Forensics.**

I. Introduction

FISMA (Federal Information Security Management Act) 2002 is a US federal law in which the importance of information security was recognized and promoted. Around FISMA, a variety of standards documents are created and disseminated by NIST (National Institute of Standards and Technology) to guide everyday IT activities. Among them, NIST Cybersecurity Framework released in early 2014 has motivated industry to adopt security standards. It is critical that security professionals are prepared with the skill sets needed for tomorrow's workforce.

Information security and digital forensics are two such areas in which security professionals should be trained. These areas have much in common: the information security covers live prevention of attacks, while digital forensics covers post-mortem mechanisms. Digital forensics is used in government, industry, and law enforcement to help us investigate computer systems and data in order to analyze and present information for criminal cases. Digital forensics also helps in determining how unauthorized users hacked into a system and in gathering related information.

The (Ohio) State Attorney General's Center for the Future of Forensic Science on the BGSU campus offers forensics science specialization programs in a couple of areas (Biology, Chemistry, and more). Considering the omnipresence of electronic devices (computer, mobile phones, and the likes) in our daily life, a specialization program in Digital Forensics (DF) would naturally complement other programs in forensics science. The Computer Science (CS) department at BGSU has recently developed a DF specialization program, which was planned to start from the fall semester of 2017. Wu and Roy were actively involved in the planning of the digital forensics curricula and the digital forensics lab from the very beginning.

Wu and Roy have received a NIST award in 2017 September, which is about incorporating NIST CFTT (Computer Forensics Tool Testing) standards in BGSU digital forensics curricula. One main goal of the project is to identify the key areas of digital forensics program, which are most important to be standardized, and wherever applicable, to develop lecture slides, case studies and modularized lab (i.e., hands-on activity) materials. The project focuses on three particular digital forensics topics, namely Hardware Write Blocker, Deleted File Recovery, and Mobile Forensics. Lavenia (who is a specialist educator) has joined the project as the evaluator of the developed curricula.

Finally, in 2018 Fall, the BGSU CS department has started offering a Digital Forensics Specialization program for students with CS major. As part of this program, in 2018 Fall, Roy has taught course CS4320: Computer and Mobile Forensics, whereas Wu has taught course CS3320: Introduction to Computer Security. In these courses, Roy and Wu have implemented and used the "standards education" modules mentioned above. Lavenia has designed specialized surveys for students in both the courses to measure students' self-efficacy. We as a team have also designed surveys to measure students' advancement in technical knowledge about standards. In summary, the data shows students have made some progress when they completed the courses.

*This work was partially supported by the US National Institute of Standards and Technology (NIST) under the grant number #70NANB17H321. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the above agency.

978-1-7281-2827-6/19/$31.00 ©2019 IEEE

In this paper we share our experience on the aforementioned front with the community, which may help others who will take a similar endeavor in the future.

II. Background

A. Digital Forensics Specialization Program at BGSU

Since Fall of 2018 the BGSU CS department has started digital forensics specialization to fulfill the emerging requirements for Cybersecurity/Digital Forensics experts. The requirements of this specialization include 12 credit hours of courses, which are CS 3210: Introduction to Software Security OR CS 3320:Introduction to Computer Security, CS 4320: Computer and Mobile Forensics, CS 4330: Network Security and Forensics, and CRJU 4400: Law, Evidence Procedures in Forensic Science. CS 3210 involves the introduction to software security and secure programming guidelines, basic security issues of programming languages, C and C++, and secure coding. As entrance courses and prerequisite to the other two DF courses, CS 3320 involves the fundamental knowledge in computer security such as confidentiality, integrity and availability; Basic security mechanisms such as access control, authentication, cryptography and software security; Overview of data logs audit and analysis; Introduction to spyware and malware. CS 4320 introduces computer forensic procedures: identification and collection of potential evidence; reverse engineering; analysis and reporting. Hands-on experience with forensics tools. Forensic mechanisms for mobile devices. Analysis of synthetic and real datasets. CS 4330 provides a comprehensive understanding of network forensics analysis principles, helps students learn to identify network security incidents and potential sources of digital evidence and demonstrate the ability to perform basic network data acquisition and analysis using computer-based applications and utilities. CRJU 4400 provides an overview and examination of the legal aspects of physical evidence including rules of evidence, procedural rules, and the role of expert witnesses. Overall, this DF specialization is designed to provide Computer Science students necessary knowledge and tools from both practical Digital Forensics courses and relevant law regulations.

In the meantime we are planning for a Digital Forensics lab. Supported by Arts and Sciences college, Department of Computer Science was given a dedicated lab space and necessary equipment to supplement the designed Digital Forensics curricula. The DF lab will have 30 personal computers, necessary networking equipment, basic digital forensic hardware, and a set of software tools to fulfill the needs of the designed DF courses.

B. NIST CFTT standards for digital forensics tools

NIST's CFTT division has set standards for digital forensics tools. The goal of CFTT project is to "establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware." They expect to provide the interesting information for toolmakers, users, or for any interested parties with various goals [1]. Other than the CFTT downloadable testing environment, they also provide Computer Forensic Reference Data Sets (CFReDS) as a repository of images for investigation, training, and testing purposes.

Our NIST grant supports us on developing the DF curricula and incorporate NIST DF standards into them, in the form of lecture, hands-on labs and exercises. We will introduce the details of the curricula and evaluation data in the following sections.

III. Building the Digital Forensics Curricula

Below we report on our efforts to incorporating standards education in BGSU curricula of cybersecurity and digital forensics. In particular, we have incorporated NIST standards in three modules of the digital forensics curricula as follows.

A. Hardware Write Blocker (HWB)

Typically, HWB works as a bridge between the host computer and the storage disk. It prevents "write" commands (which may modify data/evidence) from reaching the storage disk but allows information on the disk to flow to the forensic tool (or the OS) on the host computer.

1) Pre-course Plan: One main goal is to make students familiar with NIST's Hardware Write Blocker Device (HWB) Specification [2]. This document lists four categories of commands (to access a storage device), such as modifying, read, information, and other non-modifying. These commands can originate from the host computer via the BIOS, operating system, file system operations or the forensic tool in use. The minimum requirement for a HWB is to ensure that no modifying command can pass through. It is essential for the students to learn how to evaluate a HWB device conforming to the standards.

2) Implementation: For the sake of concreteness, below we present details of one sample lab exercise in the HWB module and we also list the tools/supports that are needed to run this lab.

Tools/supports needed: (i) NIST CFTT Federated Testing Linux system. This bootable system can be freely downloaded from the CFTT portal.(ii) HWB devices. We bought 9 counts of this device whose price was about 400$ each; (iii) Hard disks. We bought 30 counts of hard disks whose average price was about 30$. (iv) Host computers: We already have regular desktop computers in the labs on which students run the VM using VirtualBox. An example setup of the HWB device (which is under evaluation) is illustrated in Figure 1.

A sample lab exercise: The students are assigned the following tasks (derived from Federated Testing instructions).

Task 1: Use the Federated Testing ISO file to start a VM on VirtualBox on a desktop computer.

Task 2: On the welcome page of Federated Testing Forensic Tool Testing Environment, click on "Test a hardware write block tool". Then, walk over the following steps to test a HWB. (a) Go to "Hardware Write Block Home" page and click on " Get Started". (b) Insert one flash drive to computer which you will use as Log Drive for this test. (c) Follow the instruction to mount the Log Drive. (d) Go to "Generate test

Fig. 1. The lab setup: The HWB device (which is under evaluation) is placed in the middle of the hard disk (which is under protection) and the host computer (running NIST CFTT Federated Testing System).

cases and start testing". (e) Select a hardware write block type. Choose the "hard drive" option. (f) Describe the write blocker. Put in detailed information on manufacturer and model name, and so on. Select the drive type as SATA. Choose USB3 as the type of connection between test computer and HWB. (g) Select the FT-HWB-SATA option and 'Run test case'. Get results. (h) Generate a test report; a test report copy will be written in the Log Drive. (i) Open the test report in a Windows computer, and copy the content of the report to a new word document. (j) Go to the log file in the Log Drive (something like hwbtestlog.txt) and find the detailed test results. Now focus on a specific write command (e.g., opcode 30h). During the test, this command (30h) was issued to write to one sector (say S) of the hard disk. Check the (reported) content of the sector S before the test and after the test. Briefly verify whether they are "unchanged.

3) Limitations and Future Plan: (i) In BGSU CS computer lab, for security reasons, machines do not have "boot from CD" option. As a way out, we have used a VM, which is loaded with Federated Testing system. Mostly, this solution worked for our students, except occasional collapse of the VM screen, which we addressed by rebooting the VM (possibly multiple times). (ii) The NIST CFTT exercise on HWB was informative to students and it was easy to do. Most of the students have successfully completed it and also generated an independent report on evaluating a HWB. However, students did not understand/appreciate the detailed evaluation report on specific commands (e.g., opcode 30h) that HWB blocks. We plan to add curricula modules in the next offering to make students familiar with this plus add more lab exercises to experiment with this.

B. Deleted File Recovery (DFR)

A DFR tool attempts to discover data that is not part of any active file on a storage disk, which is helpful in forensic analysis. If the data is recovered in its original form, we may get additional useful information.

1) Pre-course Plan: We mainly focus on incorporating the Active File Identification & Deleted File Recovery Tool Specification [3] in the DF course. The NIST document lists the requirements a DFR tool needs to satisfy. The first, Requirements for Core Features, are those features that should be present in all tools. The second is the Requirements for Optional Features. Core Features include (i) The tool identifying all deleted objects whose entries are accessible in residual metadata. (ii) The tool constructing a recovered object for each such entry. (iii) Each recovered object including all non-allocated data blocks. The NIST document lists two Optional Features, which are active file listing and content estimation of a recovered object.

2) Challenges: NIST only provides a list of specifications/criteria for a DFR tool to meet. However, NIST does not provide sample file system images to evaluate the DFR tool on any of this criterion. We have to design such file system images on our own.

3) Implementation: For the sake of concreteness, below we present details of one sample lab exercise in the DFR module and we also list the tools/supports that are needed to run this lab.

Tools/supports needed: (i) DFR tools in Autopsy/SleuthKit (TSK) suite (ii) file system images in which some of the files are deleted using various tools, representing different scenarios.

A sample lab exercise: We have prepared two FAT images, which contain a few files (some of which were created and deleted). The students are given these images.

In Figure 2, File 1 is aa.txt (containing only char a's), File 2 is bb.txt (containing only char b's), File 3 is cc.txt (containing only char c's) and File 4 is dd.txt (containing only char d's). First, we created File 1, File 2, and File 3 in a FAT system (Image 1: fat.raw), where each one is of size 1 MB. These 3 files have filled in most of the space in the file system. Then, we deleted File 1 and File 3, and we created File 4 of size about 1.6 MB, which gets fragmented (due to space crunch). In Image 2 (fatDeletedOrOverwritten.raw), see File 4 overwrites whole of File 1 and part of File 3.

The students are assigned the following tasks to evaluate the TSK tool's performance whereas it attempts to recover the file cc.txt.

Task 1: Use *istat* command to see the cc.txt meta-data information on fatDeletedOrOverwritten.dd image.

Task 2: Now verify that cc.txt is not completely overwritten by dd.txt.

Task 3: Now try to recover cc.txt file using the *icat* command

Task 4: Now answer the following. Does TSK tool support NIST CFTT Core Features?

4) Limitations and Future Plan: (i) Thus far, we have only been able to design DFR tool evaluation exercises only for the NTFS and FAT system. There are many other file systems (e.g. ext3, ext4, etc.) to evaluate a DFR tool on. (ii) So far we designed exercises focusing on the "Core Features" of a DFR tool per NIST CFTT. There are many "Optional Features" of

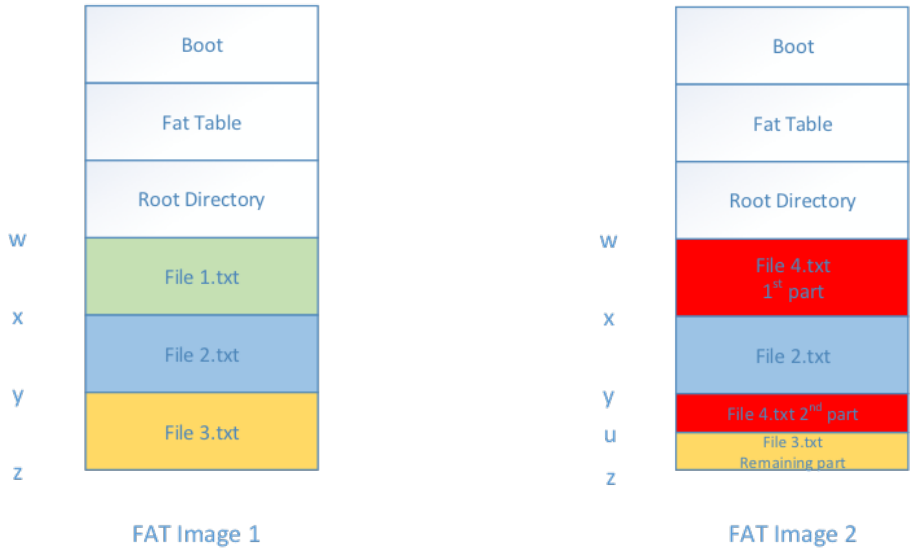

Fig. 2. The FAT images to evaluate the DFR tool: The left image is fat.raw whereas the right image is fatDeletedOrOverwritten.raw.

a DFR tool to experiment on, which we plan to do in the next offering.

C. Mobile Forensics

Forensics professionals frequently need to extract data from mobile phones as part of the investigation.

1) Pre-course Plan: To ensure basic training of digital forensics students, we need to make them aware of the standards related to evaluating a mobile forensics data extraction tool. To cover each standard, we design multiple labs, and include them in the DF curricula.

2) Challenges: NIST only provides a list of specifications/criteria for a mobile forensics tool to meet. However, NIST does not provide sample mobile phone images to evaluate the forensics tool on any of this criterion. We had to collect such mobile phone images from other sources, such as a NSF-funded digital forensics project at UIUC. We need multiple such phone images in the future to evaluate a mobile forensic tool.

3) Implementation: For the sake of concreteness, below we present details of one sample lab exercise in the mobile forensics module and we also list the tools/supports that are needed to run this lab.

Tools/supports needed: (i) The mobile forensics tool in Magnet Axiom suite, (ii) smart phone images containing suspicious artifacts (e.g., contacts, call logs, sms, maps, browser history, etc.) representing a real-life criminal investigation case.

A sample lab exercise: The students analyze a mobile phone full image with Magnet Axiom tool suite. We have received the image from UIUC course/material on digital forensics. The tasks are as follows.

Task 1: Get the phone image mob.dd which is a full-image of a smart phone.

Task 2: Open Magnet Axiom Process with credentials.

Task 3: Add Case Details to Magnet Axiom Process while selecting the mob.dd file to analyze

Task 4: Analyze evidence and view all artifact categories.

Task 5: Look into the SMS, contacts, call logs, maps and browser information for the investigation, and build your case. Write a summary of your findings.

4) Limitations and Future Plan: (i) So far we could run mobile forensic tool evaluation exercise only for a particular model of smart phone. In the future, we need to make/collect smart phone images for multiple phone models to expand the domain of evaluation. (ii) So far we designed exercises focusing on the "core criteria" of a mobile forensics tool. There are many "auxiliary criteria" of a mobile forensics tool to experiment on, which we plan to do in the next offering.

In the future, we aim to incorporate NIST standards in additional modules (i.e., beyond the aforementioned three), such as Forensic File Carving, Forensic Media Preparation, Disk Imaging, String Search, Software Write Blocker, and more.

D. Setting up a digital forensics laboratory

So far at BGSU we have been using a make-shift digital forensics lab sharing few desktop machines and other facilities in the regular computer lab. This created many challenges for us who have offered cybersecurity and digital forensics courses recently. However, this experience has made us aware of the precise requirements of a digital forensics lab and a reliable setup. In fact, we have shared our experience with the IT support staff of BGSU; we have worked together to chalk out a physical layout of a digital forensics lab with detailed configuration of desktops, software/hardware tools, computer networking setup (especially due to the requirement of making a digital forensics lab isolated from other part of the network). For instance, we are to extend our academic license from a few digital forensic companies (e.g. Magnet

Axiom, etc.). Moreover, we are to buy more counts of standard hardware (e.g. HWB, etc.). In fact, BGSU has started building a dedicated digital forensics lab since January of 2019 which should be ready in a few months.

IV. Evaluation of Students Learning

A. Rationale and Purpose

We set out to understand if students, who enrolled in computer science courses designed to teach computer security and/or digital forensics, would demonstrate higher self-efficacy at the end of the semester, compared to their self-efficacy at the beginning of the semester. Specifically, we hypothesized that students would experience stronger computer science self-efficacy after taking these courses. This expectation was based on the project teams expertise in working with college students enrolled in computer science courses, as well as the current job opportunities for students studying computer science; there is strong market demand for experts in computer security and digital forensics. Thus, we expected that students who are able to learn more about these high-demand topics in the field of computer science would experience increased confidence in their own abilities as computer scientists. We also hypothesized that students enrolled in these courses would not experience increased general academic self-efficacy, given that the focus of the courses was specifically tailored to improving computer security and digital forensics skills, and not general academic skills.

Research Questions: The purpose of this exploratory study was to investigate the following research questions:

1. Is there a statistically significant increase in students general self-efficacy after participating in a semester-long computer security course?
2. Is there a statistically significant increase in students computer science self-efficacy after participating in a semester-long computer security course?
3. After learning about computer security, and NIST standards in particular, what do students think about the importance of standardization?

B. Setting & Population

This study was conducted at a mid-sized public university in the Midwest United States. Participants (n = 20) were undergraduate (n = 16) and graduate (n = 4) students enrolled in two computer science courses during fall 2018. All students enrolled in these courses (n = 23) were invited to participate in our study. Participants were primarily male (99%) and Caucasian (70%).

C. Research Design & Instrumentation

This study employed a single-group pre-test/post-test design. We administered the following measures (pre and post) as part of this study:

1) General self-efficacy: We administered the New General Self-Efficacy Scale [4] at both pre- and post-test online using Qualtrics, the universitys online survey tool. The NGSE is an eight-item questionnaire with response options scored on a 5-point Lickert-type scale from strongly disagree (1) to strongly agree (5). Questions on this measure include items such as: 1) I will be able to achieve most of the goals I have set for myself and 2) When facing difficult tasks, I am certain that I will accomplish them.

2) Computer Science Self-Efficacy: We administered the Self-Efficacy in Learning Computer Science Scale [5] at both pre- and post-test online using Qualtrics, the universitys online survey tool. The SELCSS is an eight-item questionnaire with response options scored on a 7-point Lickert-type scale from strongly disagree (1) to strongly agree (7). Please note: We used a 5-point scale for this measure because in our online questionnaire, the two self-efficacy measures were presented back-to-back. We wanted to make the response options easier for students to read and score. Questions on this measure include items such as: 1) "I believe I will receive and excellent grade in the computer science class" and 2) "I am certain I can understand the most difficult material in the computer science class."

3) Qualitative Questionnaire for Students Understanding of NIST Standards and Network Security Protocols: This questionnaire was administered to students in the computer security course (n = 20). One of the projects Principal Investigators developed the following questions to probe students understanding and support for standards/standardization:

1. We have learned that a number of Cryptography algorithms are made NIST standards. So in your opinion, is it important to standardize those algorithms? And why?
2. We have learned that a number of Network Security protocols are made standards. SO, in your opinion, is it important to standardize those algorithms? And why?

D. Data Analysis

Data analysis for the quantitative data included calculation of means, standard deviations, and t-tests for related samples. Data analysis for the qualitative feedback involved one of the projects principal investigators, along with the projects evaluator, examining student feedback and identifying comments that indicate a) whether or not the student agrees that standardization is important, and b) why students believe this to be true.

E. Results

For the quantitative analyses, we observed no change in students general self-efficacy at the end of the semester (see Table I). However, we did observe a positive, statistically significant change in students computer science self-efficacy (see Table II).

For the qualitative analyses focused on Importance of Standards: Students (n = 20) answered questions related to the importance of NIST standards. Student comments related

TABLE I
COMPARISON OF COMPUTER SCIENCE STUDENTS' GENERAL SELF-EFFICACY PRE TO POST (N = 20).

Instrument	Mean	SD	t	p
NGSE pretest	1.45	0.51	-0.281	0.780
NGSE posttest	1.50	0.61		

Note: NGSE = New General Self Efficacy Scale.

TABLE II
COMPARISON OF COMPUTER SCIENCE STUDENTS' COMPUTER SELF-EFFICACY PRE TO POST (N = 20).

Instrument	Mean	SD	t	p
SELCSS pretest	1.65	0.67	-2.305	0.026*
SELCSS posttest	2.20	0.83		

Note: SELCSS = Self-Efficacy for Learning CS Scale.
$^{*}p < 0.05$.

to importance of NIST standards: We share (Table III) excerpts from comments that are typical responses students gave regarding whether (yes, n = 17) and why NIST standards are important. Note: Highlighted text indicates key words demonstrating support for standardization, and understanding of rationale for standards use.

TABLE III
EXAMPLES OF STUDENTS' QUALITATIVE FEEDBACK ON IMPORTANCE OF NIST STANDARDS (N = 17)

It is important for a cryptographic algorithm to comply with NIST standards mostly because it **protects** people from attacks.
Yes, following a standard **ensures all criteria are met**.
Yes. Having a standardized hard to crack set of cryptography algorithms is very important in order to better **regulate and ensure security** standards in different systems. Without these algorithms, valuable assets can be at risk, and **lazily implemented algorithms can be easily broken in** to by attributes
It is important to standardize these algorithms **sufficient encryption strength** is an integral part of cyber security. If these algorithms don't meet the standard, there is no way of determining **their adequacy and reliability**, making the system vulnerable to attackers.

Note: Three students who responded to these questions either did not believe standards are important, or offered rationale that was not clear and/or correct. Only a few excerpts are offered here due to space limitations.

F. Summary

The research team set out to understand whether teaching students about the use of professional industry standards for computer science might be associated with changes in students self-efficacy as well as students support for the use of these standards. We are encouraged that in spite of our small sample size, we did find positive, and statistically significant, improvements in students computer science self-efficacy. Moreover, nearly all students who responded to qualitative questions on the importance of standards indicated that they did support use of the standards as well as a clear rationale for why using standards is important for computer security. Resource constraints did not allow for recruitment of a matched comparison group. The project team would like to replicate this study in future semesters with the inclusion of a comparison group of computer science students and a larger sample size overall. We believe results of this study offer support for teaching students enrolled in computer science programs about NIST standards use and implementation.

V. CONCLUSION

The development of a digital forensics specialization program from scratch was challenging for us at BGSU. Yet it was an enriching experience. In this paper, we have discussed a few of the problems that we encountered. Furthermore, we have incorporated NIST standards in digital forensics curricula to better prepare the future workforce. Deliverables of the our NIST project include a set of lectures and hands-on activities to help students gain specific skills in various aspects of Digital Forensics discipline. The student evaluation data demonstrates effectiveness of delivering the designated knowledge and skills.

ACKNOWLEDGMENT

This work was supported by NIST [grant number #70NANB17H321]; The authors wish to thank the following graduate students for their work on this project: Shiva Bhusal, Sunil Shrestha, and Thamali Madhushani Adhikari Mudiyanselage.

REFERENCES

[1] Software Quality Group: Computer Forensics Tool Testing Program (CFTT), https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

[2] Hardware Write Blocker Device (HWB) Specification (Version 2.0, May 19, 2004), https://www.nist.gov/sites/default/files/documents/2017/05/09/hwb-v2-post-19-may-04.pdf

[3] Active File Identification Deleted File Recovery Tool Specification (March 24, 2009), https://www.nist.gov/sites/default/files/documents/2017/05/09/dfr-req-1.1-pd-01.pdf

[4] Chen, G., Gully, S. M., Eden, D. (2004). General self-efficacy and self-esteem: Toward theoretical and empirical distinction between correlated self-evaluations. Journal of Organizational Behavior, 25(3), 375-395. doi:10.1002/job.251

[5] Lin, C., Liang, J., Su, Y., Tsai, C. (2013). Exploring the relationships between self-efficacy and preference for teacher authority among computer science majors. Journal of Educational Computing Research, 49(2), 189-207. doi:10.2190/EC.49.2.d