National Institute of Standards and Technology
Incorporating Standards Education into Digital Forensics Curricula (Federal Award ID Number 70NANB17H321)
Award Period: 09/01/2017 - 12/31/2019
Technical Report for period 10/01/2018 – 03/31/2019
PI: Dr. Yan Wu
Co-PI: Dr. Sankardas Roy
Evaluator: Dr. Kristina Nell LaVenia
Bowling Green State University

1. Objectives vs. Accomplishments

Objective	Accomplishment
Designing curricula and offering it to students	2nd part of BGSU digital forensics course let students have hands-on-experience of how to evaluate a HWB device (bought from the market) using the NIST CFTT system.
Designing curricula and offering it to students	2nd part of BGSU digital forensics course let students have hands-on-experience of evaluation of deleted file recovery tools using the NIST standards.
Designing curricula and offering it to students	2nd part of BGSU digital forensics course made students familiar with the process of data acquisition of a smart phone and the analysis of artifacts via hands-on activities.
Evaluation of Students' Learning	Collected both quantitative and qualitative data from students who took the designed digital forensics course and cybersecurity course (in Fall semester of 2019).
Evaluation of Students' Learning	Analyzed the data collected and drew the preliminary conclusion.
Disseminate our results	Submitted a research paper sharing our experience of curricula design and evaluation of results to 7th IEEE International Symposium on Digital Forensic and Security (ISDFS 2019).
Disseminate our results	Planning for a workshop (in summer of 2019) to share our experiences.

2. Significant Developments
    a. Submitted a research paper summarizing our experience to 7th IEEE International Symposium on Digital Forensic and Security (ISDFS 2019).

b. Developing a Digital Forensics Course (CS 4320/5320) and offering it in Fall of 2018
    i. The 2nd part of the course has modules (whereas each module has hands-on activity) on evaluation of a HWB, evaluation of "deleted file recovery" tools (including challenges of retrieving a deleted file in widely used file systems, such as FAT and NTFS), and the process of smart phone data acquisition and subsequent analysis of forensic artifacts.
c. Students gaining experience of using the NIST CFTT system to evaluate a Hardware Write Blocker (HWB)
    i. We bought additional 5 counts (on top of 4 that we already had) of HWB devices (**Ultrablock Tableau Forensic SATA/ IDE bridge)** for the study. Each student group (2-3 students in one group) was given one HWB for running experiments during the lab sessions.
    ii. As a hands-on-activity students ran the NIST CFTT system's evaluation framework for a HWB. They successfully collected the test results.
d. Students gaining experience of how to evaluate a Deleted File Recovery (DFR) tool per the NIST standards for a DFR tool.
    i. Students learned design of multiple file systems (FAT and NTFS as concrete examples). They became familiar with challenges in deleted file recovery.
    ii. Students learned the NIST standards of a DFR tool. They were made familiar with intended core features and optional features of a DFR tool per the NIST standards.
    iii. Students evaluated DFR tools (e.g., Autopsy) per the NIST standards via hands-on-activity in lab. Then, they had to complete a comprehensive homework assignment on this topic.
e. Students gaining experience of the process of data acquisition of a smart phone and the analysis of artifacts
    i. Students used our newly bought tool-suite Magnet Axiom to perform data acquisition of a smart phone (in particular, Android phones).
    ii. Given a set of smart phone artifacts (SMS logs, photos, call logs, etc.) students analyzed a criminal case/scenario with the Magnet Axiom tool and prepared a (comprehensive) forensic report.
f. Evaluation Rationale and Purpose: We set out to understand if students, who enrolled in computer security and/or digital forensics courses, would demonstrate higher self-efficacy at the end of the semester, compared to their self-efficacy at the beginning of the semester.
g. Evaluation conclusions. 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.

3. Challenges
    a. Number of students in Digital Forensics course (1st offering at BGSU) is low (8 students; 6 undergrad students and 2 MS students).
    b. BGSU forensic lab is not yet ready, which is currently expected to be ready by July of 2019. Recently, there has been good progress in physical construction and furniture/equipment purchase. So far, the regular computer lab has been used as the forensic lab (with few forensic hardware devices recently purchased and with lab computers installed with forensic software, e.g. Kali Linux, relevant VMs, etc.). We plan to use the new lab for CS 4320/5320 in Fall of 2019.
    c. We could not find readily available forensic images to evaluate a DFR tool. We had to design and built such (file system) images ourselves.