CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 3, No. 2
October 2024
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2024 Review Board

Teaching Case

Digital Forensics and Incident Response (DFIR): A Teaching Exercise

Jennifer L. Breese
jzb545@psu.edu
Penn State Greater Allegheny
Penn State University
McKeesport, PA, U.S.

Maryam Roshanaei
mur45@psu.edu
Penn State Abington College
Penn State University
Abington, PA, U.S.

J. Andrew Landmesser
jal620@psu.edu
Penn State Brandywine
Penn State University
Media, PA, U.S.

Brian Gardner
bkg113@psu.edu
Penn State Schuylkill
Penn State University
Schuylkill Haven, PA, U.S.

Abstract

Cybersecurity requires practical knowledge related to protecting electronic information systems and, more importantly, hands-on skill sets for students. To prepare cybersecurity students for effective workforce contributions, experiential practice in a modern, secure environment is essential. An ideal and cost-effective way to provide this environment for both institutions with funding limitations and students with starved resources is to establish a live virtual isolated lab environment that acts as a sandbox for performing cybersecurity-related exercises, including ethical hacking, penetration testing, offensive and defensive security, information risk assessment and management, and malware analysis. This teaching exercise provides suggestions and resources, including free training by reputable cybersecurity companies offering services to the broader industry community, as excellent options to include in student coursework. Additionally, this teaching exercise offers three lessons and a full learning module to include in a variety of introductory cyberforensics, information systems, and other related disciplines to both provide hands-on learning and engage students pursuing a major in cyber studies.

Keywords: cybersecurity, digital forensic incident response, cyber education, LinkedIn Learning

Recommended Citation: Breese, J.L., Landmesser, J.A., Roshanaei, M., Gardner, B., (2024). Digital Forensics and Incident Response (DFIR): A Teaching Exercise. *Cybersecurity Pedagogy and Practice Journal;* v3 (n2) pp 21-34. https://doi.or/10.62273/EPXU4458

Digital Forensics and Incident Response (DFIR): A Teaching Exercise

Jennifer L. Breese, Maryam Roshanaei, J. Andrew Landmesser and Brian Gardner

1. INTRODUCTION

Rapid technological advancements have led the entire world to shift towards the digital realm, which increased exponentially during the COVID-19 pandemic. The transition has resulted in the emergence of cybercrimes and security breach incidents that threaten the privacy and security of users and organizations overall. Alghamdi (2020) examined the use of digital forensics in countering cybercrimes, which has been a critical development in cybersecurity. Security vulnerabilities and breaches have galvanized the developments in digital forensics, requiring data extraction from digital devices to be used as evidence in both criminal and civil legal proceedings. To understand the importance of digital forensics, Lallie et al. (2021) thoroughly discusses current trends, potential threats, and opportunities of digital forensics in cybersecurity with a focus on the impact of COVID-19 changes to the overall security landscape. Research has also identified specific threats to digital forensics, which include technical, operational, and personnel-related challenges (Easttom et al., 2022; Lallie et al., 2021; Srinivas & Kumar, 2019; Whitman & Mattord, 2021). Both statistics and analytics have shown that the exponential growth of cyber threats and attacks necessitate a corresponding need for forensic experts and forensic researchers for automation procedures in the digital realm (Joseph & Norman, 2018). According to Cyberseek (2021), cybersecurity workforce preparation is an integral part of closing the skill gap required for combating threats found in mobile apps, networks, and phishing in mobile applications.

Cybersecurity expertise requires a solid understanding of policies related to protecting electronic information systems, but again more hands-on skill sets for students is an important focus. Job descriptions related to cybersecurity, even at the entry-level, state a need for three to seven years of prior cybersecurity-related experience. To prepare cybersecurity students, hands-on practice in a modern, secure environment is essential, and the best way to provide this is to establish a dedicated physical and live virtual lab environment. The physical lab is typically a dedicated room/classroom that houses its own servers and dedicated workstations to learn physical/logical networking and perform digital/computer forensics. Normally this setup can be too costly, even for institutions with larger resources to deploy. Again, the isolated lab environment can provide a safe, fully virtualized, and sandboxed platform to perform ethical hacking, penetration testing, offensive & defensive security, information risk assessment & management, malware analysis, etc. While a physical lab is cost prohibitive, live virtual lab environments that include free training from reputable cybersecurity companies are great options to include in student coursework. Although some of these free options do not have broad certification recognition in the employment market, they could still be a differentiating factor when included in a student's resume submission and on their LinkedIn profile.

Providing learning opportunities and garnering interest in lower-level courses are key to developing a robust student pipeline in Cybersecurity Analytics and Operations (CYAOP). We are utilizing materials provided by NIST (National Institute of Standards and Technology) and other free online courses offered by industry providers to develop foundational modules for learning, interest, and excitement among our student population, potentially even drawing additional students to Information Sciences and Technology (IST) and CYAOP majors.

What is Cyberforensics?

Marcella (2021) describes cyberforensics as the discipline focused on identification, preservation, examination, and analysis of digital evidence using scientifically accepted and validated processes. Digital evidence can come from many diverse sources, including personal computing devices, networking devices, servers, cloud computing environments, and Internet of Things (IoT) devices such as vehicles and surveillance cameras with most personal computing and IoT devices networked to cloud resources. According to NIST (2022), hundreds, if not thousands, of individual digital forensic techniques might need to be used in a complete digital forensic examination. NIST identifies several useful models, each with a different emphasis, for digital forensic examinations. Further, these digital

forensic standards differ depending on the scene, nature and type of evidence being handled. For the successful prosecution and admissibility in court, certain accepted procedures must be properly followed. Digital forensic examiners use different methods and tools to accomplish the same job during digital investigations and with the changing world of digital technology these tools and methods are variable to change (Mabuto & Ventor, 2011). Beardall (2023) navigated the symbiotic relationship between cybersecurity and digital forensics, exploring the key role of digital forensic methodologies play in addressing cyber incidents while also recognizing the issues with the lack of investigative standardization.

2. PROJECT PURPOSE

The goal of this teaching exercise is to develop an instructional learning tool in cyberforensics to enhance the learning experience of students pursuing a degree in Cybersecurity Analytics and Operations (CYAOP), Information Sciences and Technology (IST), or an equivalent degree. The instructional learning module provides materials on many of the latest digital forensics frameworks and their related subjects. This teaching exercise also provides skills that students need to fully comprehend the security strengths and weaknesses of digital forensics, including mobile devices, platforms (e.g., Apple iOS and Android), and their functionalities. The instructional learning module and tool includes a step-by-step, hands-on approach that uses many current industry tools and techniques to help gain a basic understanding about Digital Forensic Investigation Response (DFIR) with additional elements to demonstrate mastery.

The development of this exercise has been a trial-and-error process through a collective of four campus faculty from the overall seven campus cyber consortium of the Penn State college campus community. Additional steps were added to the exercise to create a coordinated set of modules that can be used across the overall curriculum. These additions have served to connect other course knowledge progressions rather than a one-day or a one-off session for student learning.

3. BACKGROUND

NIST (2022) provides best practices in digital investigation techniques based on computer science methods from peer-reviewed sources, academic and classroom materials, and technical guidance from professional organizations. NIST describes options for acquiring and analyzing data from a mobile device that are explored in this case leveraging the Paraben Electronic Evidence Examiner (E3) platform. NIST (2022) also specifies a seven-step process with the first three focused on data collection and the last four on data interpretation.

1. Step one protects collected evidence from modification typically using write blocking.
2. Step two performs data acquisition as an image copy of the original data.
3. Step three in data collection ensures the integrity of the acquired data typically using cryptographic hashing techniques.
4. The fourth step (also the initial one in data interpretation) attempts to recover any deleted data. NIST discusses three commonly used techniques for data recovery of metadata-based file recovery, file carving, and deleted record recovery.
5. The next step performs navigation through the acquired data typically supported by validated forensics software tools.
6. The sixth step identifies and extracts data relevant to the investigation using criteria of interest like specific text of date-time intervals.
7. The last step in data interpretation analyzes all the extracted data artifacts to develop a narrative and timeline of events for inclusion in a final report.

What are mobile forensics and why is it important?

Mobile forensics is a subset of cyberforensics focused on analyzing digital evidence from mobile devices in a forensically sound manner. Since mobile devices are networked with other digital devices, evidence from mobile devices can often provide clues to additional digital resources to investigate. Most mobile users conduct email and social media interactions from their mobile devices. With social media applications encouraging users to share personal data, mobile users often leave significant personal data on their mobile devices without being aware (Casey, 2011). Investigators must have the skills needed to overcome challenges including potential remote device wiping, encryption, and physical imaging of various file systems. While there are many aspects of DFIR to consider in the ever-changing DFIR IoT landscape as discussed by Beardall (2023) this exercise focuses on mobile forensic discovery and analysis.

Pennsylvania State University (PSU) Commonwealth Campuses of Abington, Brandywine, and Greater Allegheny received 2022 software grants for Paraben Electronic

Evidence Examiner (E3), an all-in-one platform for adding forensic data through a collective interface for analysis and improving student understanding of mobile device forensics via hands-on lab exercises. The Paraben Unified Police Support (PUPS) grant helps resource constrained organizations, including educational institutions, to enhance the ability to process digital evidence with software and training costs for the E3 Fundamental Fast Track and Mobile Fast Track for one year including access to the Paraben Online Training Academy and access to all the courses and labs (see https://paraben.com/dfir-le-grant/ for details on grant application). Once Paraben E3 licenses are granted, students download Paraben E3 platform installer from https://paraben.com/paraben-downloads/ to install on individual computers. If opening E3 without Admin privilege, E3 prompts for Admin login but you can click No to continue in E3 without Admin privileges; however, some types of evidence will be unavailable. Once the Activation wizard opens, select the Internet License option and click Activate. Once the Connect to Web License Server dialog displays, enter the generic student user login and password supplied by Paraben then click Connect. E3 opens a dialog with four options of 1) Acquire Device, 2) Import Data, 3) Add Evidence, or 4) Open Case. If you close the dialog, you can still perform these functions from E3 menu options.

Paraben also provides a free online version of their DFIR tool for download with limited capabilities; educational tutorials on the site are also useful (see https://paraben.com/free-dfir-tools/ for the free download) (*free download*, n.d.). The free download is available after a trial is completed. Paraben also has a YouTube channel that provides educational videos on the use of the tool at https://www.youtube.com/user/ParabenForensics (YouTube, n.d.).

Our previous hands-on labs in our undergraduate cyberforensics courses of Information Sciences and Technology (IST) 453 Legal, Regulatory, Policy Environment of Cyber Forensics, and IST 454 Computer and Cyber Forensics utilized only free forensics tools primarily available in Kali Linux distributions. Kali Linux provides Autopsy as the GUI tool for Sleuth Kit under the Forensics menu option, carving tools like *scalpel*, and *guymager* under Forensic Imaging Tools to support multiple image file formats. With the importance of mobile forensics in current investigations, this software grant enabled our students to gain experience specifically with Android and iPhone devices. Paraben also issued lab instructor and student lab manuals for Android and iPhone devices. However, the student manuals assumed a greater level of Paraben tool-specific training than our students have the experience to walk through self-guided, so we added more specific detailed Android lab steps for our undergraduate students. These steps are detailed further in section 5 titled 'Teaching Exercise Learning Steps' under Additional Steps/Suggestion(s). Also, the Paraben Android and iPhone student labs used an existing Paraben evidence file starting at step four in the NIST seven-step digital forensics process. Students need to understand in the advanced levels how to extract the data file which is not provided by Paraben as the data file is furnished. Fortunately, we provided an earlier course lab focused on the first three NIST steps that included manually performing Linux filesystem acquisitions using the *dcfldd* command with required options. *dcfldd* is an enhanced version of disk dump command that includes features useful for forensics and security including hashing input data during transfer to ensure data integrity and logging of output.

This case was developed for a module initially for IST 453 Legal, Regulatory, Policy Environment of Cyber Forensics and has been adopted in other courses, specifically Security Risk and Analysis (SRA) 221 Overview of Information Security, and IST 454 Computer and Cyber Forensics. This teaching exercise initially provides five steps to developing a module on student learning and includes a free three-hour DFIR (Digital Forensic Incident Response) training and certificate through Cyber Triage (*Online incident response training with Brian Carrier, 2022)*. The Cyber Triage certificate titled *Intro to DFIR*: Divide and Conquer may not be widely recognized in industry but attempts to be tool agnostic focusing on breaking down the large investigative questions into smaller questions. Smaller questions can be answered through the artifacts uncovered in an investigation.

The ability to add sections to the module exists; however, skipping steps is not recommended or advised. Again, additional steps and labs have been adopted in various courses for the development of advanced student knowledge.

1. Textbook background chapters for reading and comprehension are assigned, and open access articles can be substituted as a student cost-effective alternative.
2. Students are required to complete the free DFIR training through Cyber Triage. The training, which takes approximately three hours, instills the ability to frame an

investigation before the students complete the exercise. Students are asked to submit the completed certificate issued through the industry provider through the Learning Management System Dropbox for credit. Further, students can and should add the DFIR training to their LinkedIn to differentiate them from peers in similar fields when they enter industry.

4. STUDENT/PROGRAM BENEFITS

The material in parts or in the additional exercises seeks to facilitate the following for students' success:

1. Provide students essential and valuable skills along with the opportunity to explore offensive security and ethical hacking methodologies.
2. Ensure that the projects will prepare students for the workforce and allow students to work from their own location with minimal computer requirements.
3. Give students in-depth theory and practical knowledge of different digital forensics, tools, platforms, and their functionalities.
4. Provide students with cost-effective and hands-on experience using open-source tools.
5. Support the incoming CYAOP major at our Commonwealth Campuses.
6. Increase instructor effectiveness in the classroom and in a hybrid course sharing environment.
7. Enhance overall faculty instructional effectiveness in SRA/CYBER/IST courses.

5. TEACHING EXERCISE LEARNING STEPS

NIST has several other mobile device image files that can be downloaded from the link below:
https://www.cfreds.nist.gov/mobile/index.html

The questions below were asked of the students in the IST 453 course based on the image file provided by the guest speaker, Brett Creasy, from the cyberforensics management team at *bit–x–bit* and led to a further understanding of suggestions by NIST (2020).

1. What is the theme of the criminal investigation?
    a. What data did you review to determine this?
2. What general areas (location) was the phone used in?
    a. What data might you review to determine this?
3. Are there any 3rd party apps installed on the phone?
    a. Where might you look to determine this?
4. If a raid was performed on the hotel they are staying in, what specific additional electronic device would be of interest in the investigation?
5. What are some of the interesting terms you uncovered in your review of the information (ex: What were some of the terms Brett mentioned in his speech? Do some additional research if needed).
6. What other information did you uncover? (ex: Were there "cover" names that seemed strange or odd in the conversations?)

The specific image file for this exercise used has since been removed from the NIST site. Many images are placed on the site and subsequently removed by educators; there are currently (as of 2023) twenty images and some access to archived images are available. Although we are unable to provide the original link to the cited image for this exercise, the NIST site cited above has images for download to create your own step and develop similar questions for discovery as those mentioned above. The upload for analysis is the free Cellebrite Reader software https://cellebrite.com/en/cellebrite-software/cellebrite-reader/. Cellebrite is a digital forensics tool that preserves the integrity of evidence data throughout the investigation process, which is known as validation. Cellebrite as a tool is designed to assist in the validation of forensic evidence so that it holds admissibility in court and decreases the time spent acquiring data from a mobile device by leveraging an aimed approach (Wilson & Chi, 2018).

Additional Steps/Suggestion(s)

The opportunity to provide additional step(s) to the "module" was created through an educational institution grant from Paraben Corporation, who provided licenses at no cost to our often resource-challenged students. This grant made it possible to create instructions suited for college students with little or no knowledge of the DFIR process or software.

Paraben

The Paraben E3 Android evidence file uses a scenario with an Android device confiscated from a 16-year-old user involved in a possible drug ring incident at a local high school. After installing Paraben E3 and activating using Internet licenses, students download the **SCH-R740C-AndroidEDU1.0.ds** evidence file from a shared course location, confirming the SHA256 hash of the downloaded Paraben E3 Android evidence file.

After starting Paraben E3, students click "Add Evidence" and enter a case name. In the **Add New Evidence** wizard, students select "Paraben Tools" from the category list and then select "E3 mobile data case file/DS case file" from the source type list. Finally, students navigate to the downloaded **SCH-R740C-AndroidEDU1.0.ds** evidence file containing data acquired from the Android device. Since Paraben E3 cases can have multiple evidence files, students are asked to name this new evidence before E3 provides the Case Content in leftmost frame allowing students to navigate evidence by double-clicking on items to drill-down in case hierarchy. Selecting any specific item in the case hierarchy displays that item properties in rightmost frame of E3.

The original Paraben student lab manual simply lists questions to answer by finding from the evidence file. We requested that our undergraduate students answer these questions in the context of a complete forensic report as output from the NIST-recommended forensic process. We wanted to confirm that our students could complete step seven of data interpretation by analyzing all the extracted data artifacts to develop a narrative and timeline of events relevant to the case scenario from the evidence. Students are instructed to answer the following eight questions derived from the original Paraben E3 Android student lab manual within their created forensic case report for the lab scenario investigation:

1. Mobile device information: What is the model of this device? Is a subscriber identity module (SIM) card present in the device? What is the device International Mobile Equipment Identity (IMEI)? What firmware is the device running?
2. Is there an email account set up on the device? If so, what is the email address? How many contacts are on the device?
3. Is there a Secure Digital (SD) card present in the device? How many photos are on the device? Are any photos relevant to the case?
4. How many Apps are there on the device? Which Apps have relevant information to this case? How can you obtain information from these Apps?
5. How many Short Message Service (SMS) are there on the device? How many Multimedia Messaging Service (MMS) are there on the device?
6. Does the device contain any user-entered calendar entries? If so, do any relate to this case?
7. What internet searches have been executed on the device?
8. Who is the owner of the device? Is the owner involved in the drug ring? If so, what role does the owner play?

6. CONCLUSION AND FUTURE ADDITIONS

Instead of being a one-day, one-off course, this exercise has been an attempt to create a cohesive module within the overall curriculum that connects with other course knowledge progressions. According to NIST (2022), digital investigation techniques require knowledge of how tools function and how they are limited. Forensic tool functionality and limitations are impacted by the types of devices being investigated, with increased focus on mobile devices being used to conduct and collaborate illegal activities and to build timelines at locations of key events. Students need hands-on exercises conducting digital forensics on mobile devices with industry tools to better prepare them to provide accurate, timely investigations including internal organization investigations upon graduation. The Paraben education grant was instrumental in allowing our participating Penn State University Commonwealth Campuses to bring this experience with mobile device forensic tools and to reduce the learning curve with these tools after graduation. As we continue to improve our lab activities based on receiving future Paraben education grants, some areas that we plan to enhance include supporting direct Android data acquisition from an Android virtual machine and conducting iPhone mobile device forensics.

7. REFERENCES

Alghamdi, M. I. (2021). Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities. In (Ed.), Cybersecurity Threats with New Perspectives. IntechOpen. https://doi.org/10.5772/intechopen.94452

Beardall, D. (2023). Unveiling the Digital Shadows: Cybersecurity and the Art of Digital Forensics. *Cyber Operations and Resilience Program Graduate Projects*. 5. https://scholarworks.boisestate.edu/cyber_gradproj/5

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet: Academic press.

Cyberseek. NIST. (2021, November 19). Retrieved July 25, 2022, from https://www.nist.gov/itl/applied-cybersecurity/nice/cyberseek

Easttom, C. (2022). Digital Forensics, Investigation, and Response (4th ed.). Jones & Bartlett Learning.

Free Digital Forensic Tools. Paraben Corporation. (n.d.). https://paraben.com/free-dfir-tools/

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Joseph, D. P. & Norman, J. (2019). An Analysis of Digital Forensics in Cyber Security. *Advances in Intelligent Systems and Computing First International Conference on Artificial Intelligence and Cognitive Computing*:701–708. https://doi.org/10.1007/978-981-13-1580-0_67

Marcella, A.J. (Ed.). (2021). Cyber Forensics: Examining Emerging and Hybrid Technologies (1st ed.). CRC Press. https://doi.org/10.1201/9781003057888

Mabuto, E. K., & Venter, H. S. (2011). State of the Art of Digital Forensic Techniques. In *Information Security South Africa 2011 Conference Proceedings*.

National Institute of Standards and Technology (NIST) (2022, May). Digital Investigation Techniques: A NIST Scientific Foundation Review, NISTIR 8354-DRAFT. U.S. Department of Commerce: Gaithersburg, MD. Retrieved from https://doi.org/10.6028/NIST.IR.8354-draft

Online incident response training with Brian Carrier. Cyber Triage. (2022, April 15). Retrieved July 5,2022, from https://www.cybertriage.com/training/

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, 178-188. https://doi.org/10.1016/j.future.2018.09.063

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.

YouTube. (n.d.). *Paraben Forensics*. YouTube. https://www.youtube.com/user/ParabenForensics

Wilson, R., & Chi, H. (2018). A framework for validating aimed mobile digital forensics evidences. *Proceedings of the ACMSE 2018 Conference*. https://doi.org/10.1145/3190645.3190695

APPENDIX A
Using Mobile Forensic Software Survey - Pre

Using Mobile Forensic Software Survey - PRE

* Indicates required question

How do you feel about Learning Mobile Forensic Software?*

Choose

What is your intended major?*

- ○ IST
- ○ Cybersecurity

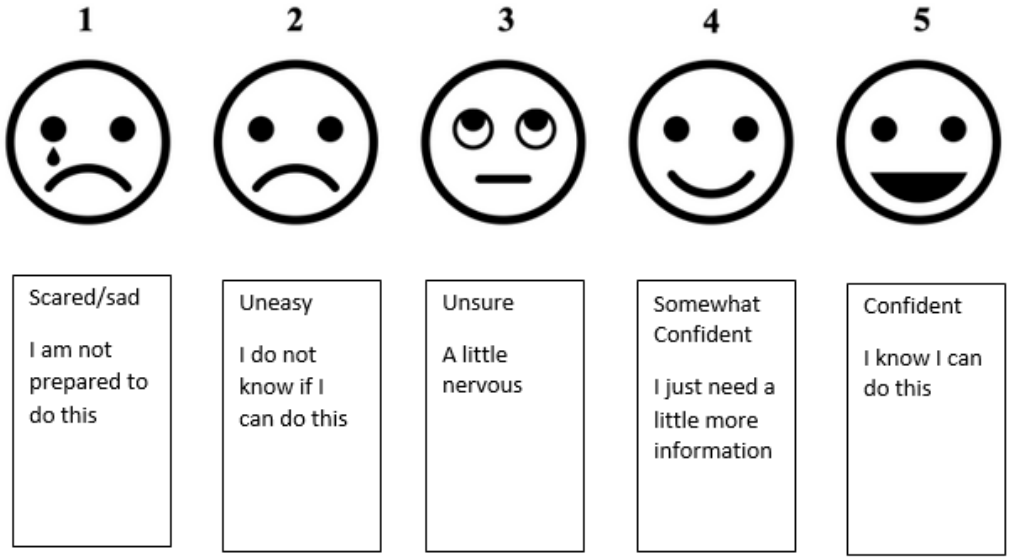
Are you pursuing an SRA minor?*

- ○ Yes
- ○ No
- ○ Maybe

What academic semester are you in currently?*

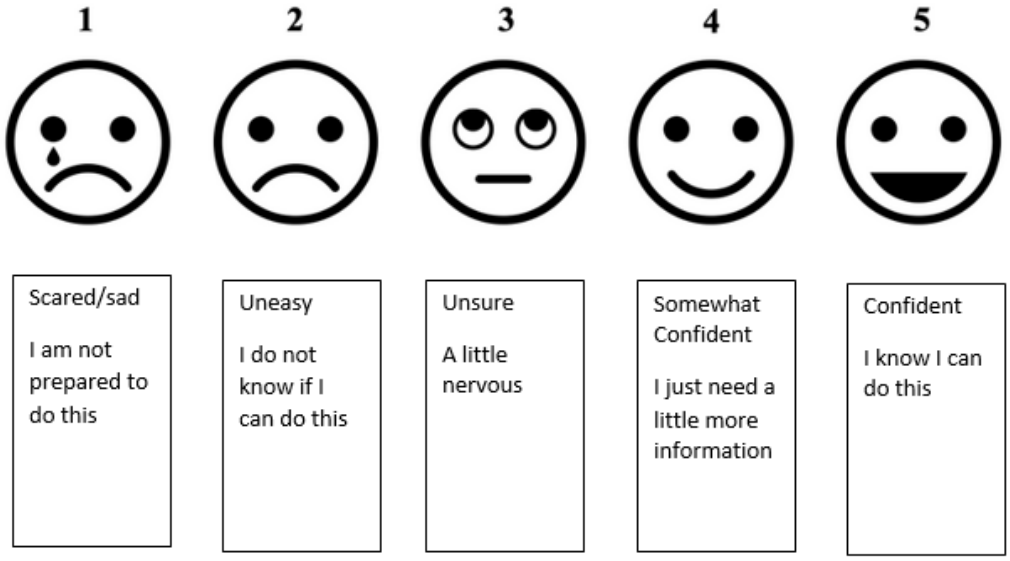
- ○ 3rd
- ○ 4th
- ○ 5th
- ○ 6th
- ○ 7th
- ○ 8th
- ○ 9th or higher

Do you feel prepared based on your PREVIOUS COURSES to complete a mobile forensic investigation?*



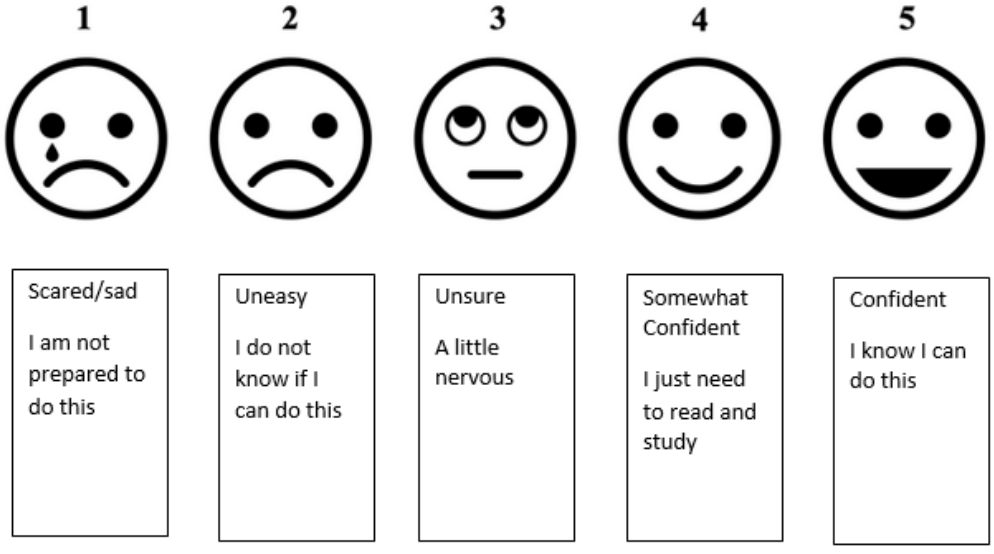
Choose

How comfortable do you feel using mobile forensic software to complete an investigation?*



Choose

What was your comfort level with the course material BEFORE the use of mobile forensics software was introduced?*



Choose

Did you complete the DFIR two-hour training yet?*

- ○ Yes
- ○ No

What can be done to increase your comfort level completing mobile forensic investigations?*

Your answer

APPENDIX B
Using Mobile Forensic Software Survey – Post

Using Mobile Forensic Software Survey - POST

* Indicates required question

How do you feel about Learning Mobile Forensic Software?*

1	2	3	4	5
Scared/sad I am not prepared to do this	Uneasy I do not know if I can do this	Unsure A little nervous	Somewhat Confident I just need to read and study	Confident I know I can do this

Choose

What is your intended major?*

- ○ IST
- ○ Cybersecurity

Are you pursuing an SRA minor?*

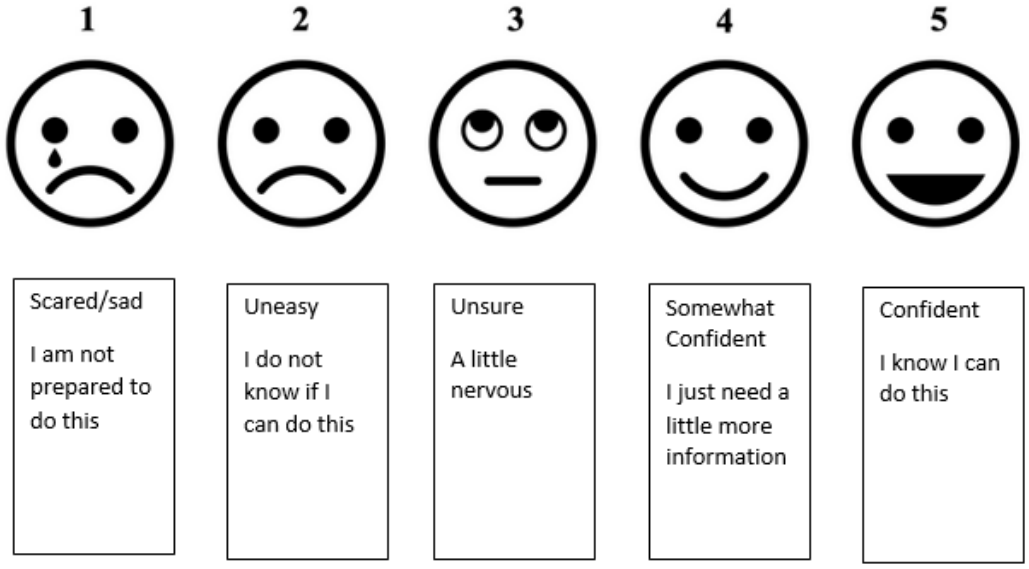
- ○ Yes
- ○ No
- ○ Maybe

What academic semester are you in currently?*

- ○ 3rd
- ○ 4th

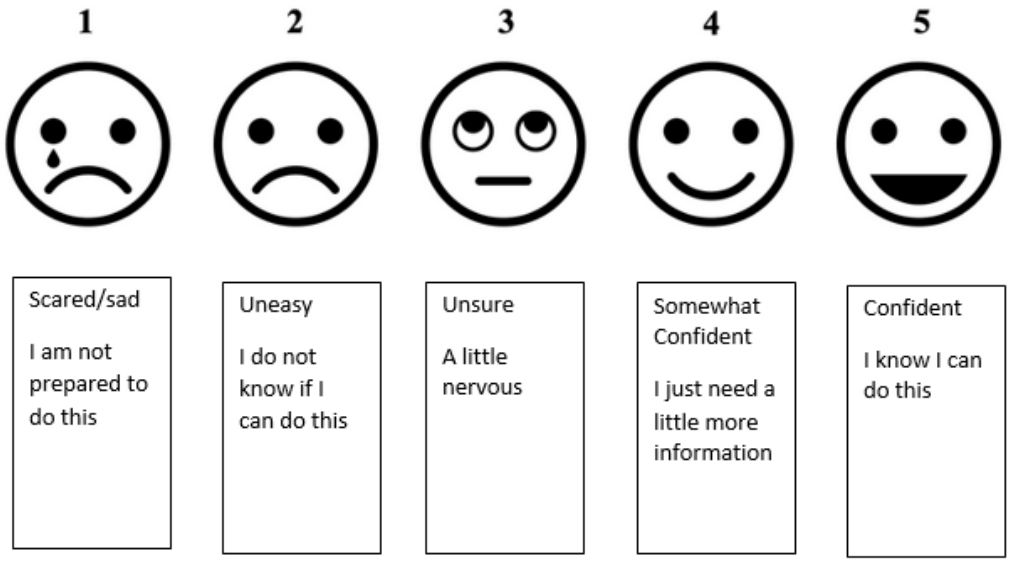
- ○ 5th
- ○ 6th
- ○ 7th
- ○ 8th
- ○ 9th or higher

Do you feel prepared based on the CURRENT COURSE INFORMATION to complete a mobile forensic investigation?*



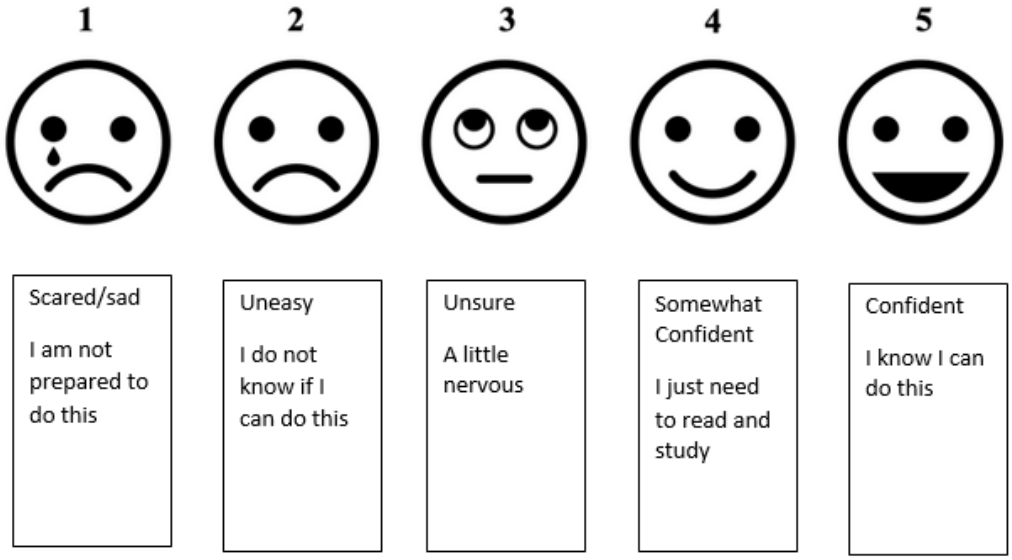
Choose

How comfortable do you feel using mobile forensic software to complete an investigation?*



Choose

What was your comfort level with the course material BEFORE the use of mobile forensics software was introduced?*



Choose

Did you complete the DFIR two-hour training yet?*

- ○ Yes
- ○ No

What can be done to increase your comfort level completing mobile forensic investigations?*

Your answer

Which program are you more comfortable using:

- ○ Cellebrite
- ○ Paraben
- ○ Other: _____