ISSN: 2473-4901
v9 n6008

A Chip Off the Old Phone: Inquiry Learning as a Synthesis Capstone in a Digital Forensics Setting

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department, Saint Vincent College
Latrobe, PA 15650

Abstract

Students need experience with exercises that are not explicitly laid out step by step and are not guaranteed to work. While there is a case to be made for automated and prepackaged exercises and labs with known achievable results in introductory courses, as students progress towards field experiences and employment, they need to gain confidence in confronting the unknown, or anomalies, that they will be subjected to in the wild. This paper will detail an experiment in introducing a discovery lab module into an advanced digital forensics course. The purpose of this module was to place students into an open-ended situation where they were to develop an approach and process to extract data from a non-functional phone. The goal of the lab module was for students to develop a scientific and methodical approach to solving the problem without being provided with specific instructions. Six areas were identified as research questions to measure student success within the project: (1) Can students find source material to guide themselves; (2) Can students develop a proposed methodology; (3) Can students research a device and identify storage chips; (4) Can students remove a chip from a circuit board; (5) Can students extract data from a chip; and (6) Can students identify points of error in their process and possible fixes to those areas.

Keywords: Inquiry Learning, Forensics, Cybersecurity, Scientific Method

1. INTRODUCTION

Every day there is something new. This is a common cliché in many disciplines, but it really is a way of life in cybersecurity. The adversarial nature of the discipline inherently creates an environment of never-ending change as technology, user bases, and attackers are always in churn. Adaptability is a trait that is paramount in a cybersecurity professional. It should be a primary goal of the cybersecurity professor to develop the traits of adaptability in their students.

As a technical discipline, cybersecurity relies on a bedrock foundation of existing domains of knowledge and skillsets that students master as they progress to the workforce. However proficient a student becomes with those existing skills and bodies of knowledge, they will forever be chasing the practical question of how to apply those to a new, unique, unknown situation and environment.

Discovery-based Inquiry learning is an approach that has been integrated into classrooms of many disciplines at various levels of education. The guided inquiry approach "has proven to be more effective than other lab approaches using cookbook procedures or discovery approaches (de Jong, et al., 2013)." Developing critical thinking and problem-solving skills through inquiry learning can be an effective approach to bridging the worlds of protected classroom environments of limited variables and messiness and the real world of volatility and the unknown (Irwanto, et al., 2018) (Sitnikova, et al., 2013).

The purpose of this paper is to describe a lab module in chip-off forensics based on inquiry learning and the outcomes that allowed students to gain confidence in developing a process for confronting a task without a known set of instructions.

Background

Mobile and Internet of Things (IoT) devices have become ubiquitous in our society. As such, they often contain a vast treasure trove of data related to the owner, user, and possibly the extended environment in which the device has been located. As relatively new arrivals in our technical world, there are many issues related to the retrieval of data from these devices that technicians and investigators have had to constantly confront. These issues range from the lack of standardization, the variety of manufacturers, the orphaning of products from company failures, and a focus on a "first to market" mentality leaving security concerns as an afterthought. These issues are only a few of the many. In 2021, the Bureau of Labor Statistics determined that the market for computer forensic examiners would grow at a rapid rate of 33% in the decade between 2020 and 2030 (BLS, 2021).

Mobile forensics is the branch of digital forensics that aims at investigating the digital evidence recovered from a cell phone that can provide a wealth of information in a forensically sound manner (Sathe, et al. 2018). While standard forensic techniques and best practices are established, the pace of change in the industry necessitates that an examiner be adept and adroit in adapting to new and unique situations.

Due to the nature of mobile and IoT devices, in many cases, they can become inoperable. Through damage, lost passwords, or lack of interoperability access to data contained on the device by way of convenient graphical interfaces or network connectivity may be lost. In some of these cases, the only way to retrieve data may be through an invasive process. With traditional computing devices, such as a laptop, desktop, or server systems, stored data can be accessible with the removal of a traditional hard drive or M.2 Solid State Drive (SSD) storage device. Many IoT or mobile computing devices do not conatain removable storage components. Chip-off forensics is an advanced digital data extraction and analysis technique that involves physically removing flash memory chips from a device and then acquiring the raw data using specialized equipment (FLETC, 2023). As recently as 2019, a survey of IoT vendors reported that nearly 60% stored unencrypted data on the device (Maayan, 2019). Thus, the careful removal of a memory chip can allow data extraction through a separate interface.

As a capstone experience for an advanced mobile forensics course, a chip-off data extraction scenario presents a compelling set of challenges for a student. As a basis for a discovery, inquiry-based, learning activity, it demands that a student combine multiple skill sets to develop and follow through with an investigative process previously unknown to them. In doing so, the student develops independent and critical thinking skills along with creative problem-solving approaches.

The purpose of this capstone module was to place students into an open-ended situation where they were to develop an approach and process to extract data from a non-functional phone. The goal of the lab module was for students to develop a scientific and methodical approach to solving the problem without being provided with specific instructions. Six areas were identified as research questions to measure student success within the project: (1) Can students find source material to guide themselves; (2) Can students develop a proposed methodology; (3) Can students research a device and identify storage chips; (4) Can students remove a chip from a circuit board; (5) Can students extract data from a chip; and (6) Can students identify points of error in their process and possible fixes to those areas.

2. LITERATURE REVIEW

The central pedagogical approach adopted in designing the chip-off forensic lab is inquiry learning. In inquiry learning, students follow a process in which investigations are the primary motivation. In this approach, information is not offered directly to students, it needs to be extracted from an interaction with a task and experience in the real world or with a model of the phenomenon (de Jong, et al. 2014). This investigation process is guided by a research question or hypothesis that requires the interpretation of results and the formulation of conclusions, and the outcomes need to be communicated to others (National Science Foundation, [2000]). The guided inquiry approach "has proven to be more effective than other lab approaches using cookbook procedures or discovery approaches (de Jong, et al., [2013])."

A primary goal of higher education is fostering the spirit of lifelong learning. The dynamic nature of cybersecurity, and specifically Digital Forensics truly demands this as students must prepare to be independent learners throughout the length of their careers. Independent thinking and creative problem-solving are chief among these traits.

Independent learning consists of several components. These include cognitive, metacognitive and affective skills (Cukurova, 2014). Cognitive skills comprise critical thinking and creativity, both being essential for addressing problems in a rapidly changing environment. Critical thinking is taken as "thinking self-correctively about one's own thinking …… (which) employs criteria and is sensitive to context" (Lipman, 1987). Both skills are essential for independent learning, as the former involves the generation of new ideas, whereas the latter involves assessing their respective quality (Treffinger et al., 2002).

Metacognitive skills are needed for planning, monitoring, and evaluation, which are important for problem-solving (Meijer et al., 2006). Problem-solving in the context of this project is seen as the ability to design, implement, and review a solution to a specific technical problem. The ability to reflect on the learning process enhances the learning outcome (Boud et al., 2013), helping the student to understand the reasons underlying their observations and to help change their actions in a positive direction (Nguyen et al., 2014).

There is value in frustration, however, we can not allow students to become so frustrated that they abandon a task. Affective skills enable positive self-regulation of emotions during learning (Vermunt, 1996). As the student experiences setbacks more frequently during independent learning as compared to traditional fully guided learning, one critical affective skill is adaptive motivation, which is the ability to self-motivate in the face of difficulties (Heyman and Dweck, 1992). The external factors that support independent learning can be termed broadly as an "enabling environment", which includes a proper facility, well-trained teachers, and sufficient resources.

3. THE PROJECT

The chip-off lab exploration project took place over a three-week period as a capstone to an advanced specialization elective course in digital forensics. The exercise was broken into three categories: Discovery and development of a proposed process, journaling effort in executing the process, and formal documentation of the efforts in an appropriate report format.

Several pieces of equipment and materials were made available to students. A collection of cell phones was made available. The phones included a wide range of ages, manufacturers, and operating systems. The expectation was that each of the phones was no longer operational. Students were advised that each of the phones provided was disposable. The expectation was that the process was a destructive one and no efforts were made to reassemble a deconstructed device.

For aid in deconstruction and chip removal, a re-work station was provided. The X-Tronic 5040-XR3 includes an infrared preheating plate, hot air gun, and precision soldering iron with digital temperature control. Initially, for data recovery, the ALLSOCKET eMMC153/169 USB NAND memory reader was provided. At the end of the project, a Z3x Easy Jtag box with eMMC Socket Pro was acquired to expand the possible range of NAND chips that could be analyzed.

Stage 1 – process discovery

Students received an overview of the project. The goal was to retrieve any data from an inoperable device, a cell phone. No direct instructions on how to retrieve data would be provided. The time for the project was three weeks. Students were allowed the use of a restricted access special projects lab workspace.

The initial stage was broken into two parts. The first was a required annotated bibliography. Each student was required to provide at least three sources that could help guide them in developing a process for their methodology of retrieving data from their phone. The assignment was collaborative in that the turn-in for the sources was a discussion board shared on the course management system. For each source, the student would include a link to the article followed by a summary that included identification of purpose, the intended audience, the type of article (tutorial, research paper, blog, etc.), content, and an opinion on why and in what capacity the article would be useful. As an incentive for participation, duplicate sources were not allowed. If a student procrastinated, they would be forced to dig deeper to find sources that had not already been shared on the discussion board.

The second part of the first stage required students to submit a proposed methodology that they planned to follow in extracting data from their device. Students were required to submit a proposal including initial research on the device that they had chosen, followed by a step-by-step process based on the specifications of the device. Students could not proceed to the next stage without an approved proposal.

Stage 2 – deconstruction and attempted data recovery
It was determined that prior to this project only two of the fifteen students had previous experience soldering. None of the students had any experience in deconstructing circuit boards. Two sessions were held to provide basic instructions on how to operate the re-work station – the soldering iron, hot air gun, and warming plate. As an interim step, students were provided with a second device, an older "flip phone" to dismantle. As an encouragement, an extra assignment was inserted into this stage to give a small amount of credit for student effort to train themselves on the equipment. This extra assignment also allowed for a first run-through of developing the techniques required for the full project write-up. Treated as a dry run, students were required to journal their efforts in deconstructing the flip phone. This included taking pictures, providing some background research on the phone model, and their efforts identifying and extracting a memory chip from the circuit board. A second discussion board was created for "Tips on Chips" where students could share insight as they learned more about chip extracting through experience.

Once students were comfortable with their ability to deconstruct a phone and remove a memory chip without "visible" damage, they moved forward to attempt data recovery from their primary device. The expected work product and artifacts from this stage included rough journaling notes and images from multiple stages of deconstruction. Comments and informal observations were highly encouraged.

Stage 3 – formal lab report
The final stage of the project required students to provide a formal "lab report" of their efforts. While no exact template was provided, a "standard" format was recommended. An eight-part outline was presented to students as a suggested framework. This framework included: Abstract, Introduction, Literature Review, Methodology, Procedure, Analysis, Discussion, and Conclusion.

4. RESULTS

Course enrollment was capped at fifteen students. The chip-off data retrieval project was presented in a period of three weeks inclusive of six class meetings during weeks twelve through fifteen of a sixteen-week semester. Of the fifteen students enrolled in the course, fourteen students completed the project.

RQ1 – Can students identify quality sources to guide and direct their efforts in chip-off forensics?

This question was evaluated based on the annotated bibliography assignment. A three-category rubric was utilized in evaluating submissions. Sources were rated based on content and direct applicability in directing the actions of the student in their effort to retrieve data. One student failed to submit any source. Eight students were able to provide three sources with valuable instruction. Of the six remaining, three provided two sources, with the remaining three providing only one. It was noted that of the six that did not receive a three in the rubric, each provided duplicate sources that had already been shared on the message board. Based on the fourteen that completed the assignment, 71.5% were able to find two or more unique sources to guide them in chip-off forensics.

RQ1	3	2	1
Students	8	2	4
	57.1%	14.3%	28.6%

RQ2 - Can students develop a proposed methodology to guide and direct their actions in chip-off forensics?

This question was evaluated based on an assignment requiring students to submit a proposed methodology/process prior to any physical activity with a device. Fourteen students submitted proposed process documents, with three students submitting two days late. A three-category rubric was utilized in evaluating submissions. Methodologies were evaluated based on the completeness of scope, and the detail of steps. One student did not complete the assignment. Six students received a three for their proposal that identified multiple stages of disassembly, cleaning, and data retrieval. Five students received a two based on deficiencies in identifying either multiple stages or lack of detail in describing multiple steps. Three students received a score of one on the rubric evaluation having submitted proposed procedures that lacked specificity in steps and a lack of identification of stages to the process. Based on the fourteen that completed the assignment, 78.5% were able to produce a methodology/procedure that identified multiple stages to the process and combined a sufficient amount of detail to the steps to anticipate a reasonable chance of successfully completing the chip-off forensic project.

RQ2	3	2	1
Students	6	5	3
	42.9%	35.7%	21.4

RQ3 – Can students research a device and identify proper memory chips on a mobile device?

Evaluation of this question was taken in two stages. Initially, it was anticipated that students would be able to research and obtain technical specifications of the devices they had chosen. Unfortunately, this proved exceedingly difficult with the resources available and in the timeframe allotted. Identification of the type and manufacturer of memory was to be included within the initial proposed methodology assignment. No students were able to find this data in advance of the disassembly of their devices.

Subsequently, the search for and identification of memory chips became a discovery operation during the deconstruction of the devices. Once students began to isolate the circuit boards of their phones, they were confronted by many heat shields protecting, but obscuring, the chips. The process of identifying became a game of trial and error. Through anecdotal evidence of informal conversation and observation, only a handful of students (three by informal count) were able to identify a memory chip prior to removal. All of the fourteen students who completed the assignment were able to extract a memory chip, but for most the identification only came after removal. Some explanations from students included the inability to read markings on the chips as the printing was very light, very small, and often faded due to the heat treatment in removing the heat shield protecting them.

RQ4 – Can students remove a memory chip from a circuit board?

Of the fourteen students who completed the assignment, all fourteen were able to extract a memory chip from a circuit board. This statement must be qualified, though, as later efforts in data extraction showed that most chips were damaged in some way during the extraction.

RQ5 – Can students extract data from a memory chip removed from a mobile device?

Of the fourteen students who completed the assignment, one was able to retrieve identifiable data from a chip. This student was able to access the file system from a Samsung Galaxy S5 (SM-G900V). Based on the fourteen students completing the project, this is a 7.1% success rate.

RQ6 – Can students identify points of error and possible fixes in their project?

This question was evaluated based on the discussion section of the final lab report submitted by students. A three-category rubric was utilized in evaluating submissions. Student responses were evaluated based on the identification and description of possible sources of error in their actions or equipment, and proposed solutions to the identified source of error if the lab were to be repeated. Ten students were able to identify at least two sources of error and possible solutions. Three students provided either a mix of two sources and one solution or one source of error with two solutions. One student only provided one source of error with one possible solution.

RQ6	3	2	1
Students	10	3	1
	71.4%	21.4%	7.1%

5. DISCUSSION

Student attitudes

There are many areas of computer science or cybersecurity where results are very obvious. It can be a world of binary options; a program compiles or experiences a "Fatal Error", a device connects to a network or it does not, a firewall blocks unwanted traffic or it does not. Judging the success of this project on the ability of a student to retrieve data utilizing a chip-off technique from a disabled cell phone by whether the student actually retrieved data or not would be valid if the environment was a forensics lab for law enforcement. However, this project was conducted in an elective undergraduate course. The purpose of the lab was not data retrieval. If data was retrieved, it was a bonus. The true purpose of the exercise was to instill a sense of exploration and adaptability in the students. This is not a binary measurement.

Initially, student reaction to the project was mixed. Several students expressed a level of discomfort with the idea of not being handed a set of instructions. Several students were intimidated by the idea of having to work with a soldering iron for the first time. It was important as the instructor to instill a spirit of exploration and the idea that, maybe for the first time for many of them, the expectation was that they would fail. Retrieving data was a long shot, and it was an acceptable result for them if they were not able to retrieve any data. This was unsettling for some, and confusing for others. Again, in computer science and cybersecurity, in most cases, there is a very clear sign of success, and most students are accustomed to achieving that success. It took some explanation to assuage the fears of these students. The layout of the project helped with this. A clear framework of deliverables and the inclusion of multiple stepping-stone assignments allowed students to earn their grades and show progress, even if the end result was not successful data recovery.

Once into the process, attitudes notably and visibly changed. Students were notably excited to play. The idea of being able to "break" and take apart phones was very attractive to the students. Following the demonstration and short training exercise with the soldering station, students were waiting in line to work with it.

It was encouraging to see further research being carried out by students. Once chips began to be removed, several students began to dig further into the types and pin patterns to identify them. More encouraging was to see the research and effort students put into trying to determine the reasons that they were unable to retrieve data.

Student success

As expected, very little data was recovered. It was a bit of a eureka moment when one student did find success at the very end of the project. It was the proof of concept that it could be done.

Of the fourteen students, eleven took the opportunity of a second attempt. Enough phones were available to afford them the chance. Students were allowed a second chance only if they were able to present at least one possible cause of failure from their first attempt, and a potential solution in how they would change their process.

There were two sources of error that students determined were the most likely cause of failure. The first was the temperature of the hot air gun and soldering iron in chip removal. In practicing with the re-work station, most students immediately went to a higher temperature setting near 400C. This allowed them to quickly remove any heat shield and then the memory chip in a short amount of time. As students dug deeper into more in-depth tutorials and technical specifications, they discovered that lead-free solder will melt around 217C. Further investigation found best practices related to preheating the circuit board slowly up to 180C before bringing the chip to the 220-230C range for removal. This process could take up to ten minutes. The slow building of temperature and the overall lower top end of temperature will lessen the chance of damaging/erasing any data on the chip.

The other primary source that students identified of error was in cleaning the chip properly. BGA (ball grid array) connections are very tightly arranged and could be prone to shorting if any excess solder bridges the "pins". As novices with a re-work station, hot air gun, and soldering iron students were feeling their way in practicing the physical dynamics of the process. A magnifying glass and a digital microscope were added to the toolset to enable students to closely inspect their chips for any excess solder.

While every student was able to find at least one NAND memory chip with BGA 153/169 pattern, this was the only pattern for which they had a reader. During the deconstruction process, multiple other chip types were recovered for which no data recovery could be attempted at that time without a specific reader for that chip type.

Student reflection

Comments from students related to the exercise were very positive. As noted, for most students this was the first time that they had an experience with a soldering iron. For most, their work has not included any experience with hardware down to this level. Having been introduced to this tool, there is now a project scheduled for the cybersecurity club to build radios from kits to introduce more students to circuit building.

Students were also very happy to tear apart phones. Again, it was expressed that for most of their student careers, little had been included that allowed them to dissect equipment. Some had built their own gaming computers, but even that process is very component-driven with little need for even a screwdriver anymore. Really tearing into a phone was akin to breaking into a "black box" in real life for them. They knew what was inside, but had never really seen it for themselves. "Getting in there" was a highly satisfying experience of confirmation.

As stated previously, some students expressed trepidation when confronted with the notion of

"Here's a dead phone, figure out how to get some data off of it… and no, I don't have any instructions for you… you'll have to figure that out yourself…" By the end of the project, all students stated that they felt more confident in confronting an unknown task. In addition, each student also responded that they were more comfortable with, and more likely to use, a "scientific method" approach to problem-solving when confronted with an unknown task based on their experience with this exercise.

Professor insight

As the professor of the course, it was also a bit intimidating to implement a project that had not been fully tested and had a very high probability of failure. However, it was one of the more rewarding and positive experiences I have had.

The project necessitated a bit of discovery from both students and the professor. The requirements of the professor presented as more of a mentoring task than a direct teaching process. It was very important to foster a positive atmosphere. Most students at the advanced stage of their degrees are not accustomed to having projects not succeed. Defining success away from data collection and towards process creation was essential. Not every task can be completed quickly and easily, and sometimes progress is good enough.

6. CONCLUSIONS

At the rock face of cybersecurity in the real world, practitioners will be presented with something new every day: new adversaries, new environments, and new technologies – things that they have not trained for or on. For many students, their experience in a classroom has focused on the basics of knowns within the discipline. Gaining knowledge about and experience with these known areas of cybersecurity is essential to being able to get started with a career in the field. However, very quickly, the new cybersecurity practitioner will be knee-deep in the volatility of change and the unknown.

Creating experiences for students that include process-oriented guided inquiry can provide a foundation of confidence and frameworks to work within the unknown. These projects help to bridge the gap between the sheltered and expected learning environments of the classroom and the volatile real world where nothing is cookie-cutter.

Creating a positive environment of discovery is a noble goal. Providing the opportunity for students to confront unknown tasks on their own is crucial in tying together the known skillsets of their education, synthesizing the essentials, and applying them beyond the scope of the classroom. With a growth in confidence in approaching the unknown, and a proven framework to direct inquiry, the real world can be just a little less intimidating.

7. REFERENCES

Boud, D., Keogh, R., & Walker, D. (Eds.). (1985). Reflection: Turning Experience into Learning (1st ed.). Routledge. https://doi.org/10.4324/9781315059051

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile forensics: advances, challenges, and research opportunities. IEEE Security & Privacy, 15(6), 42-51.

De Jong, T., Linn, M. C., & Zacharia, Z. C. (2013). Physical and virtual laboratories in science and engineering education. Science, 340(6130), 305-308.

De Jong, T., & Lazonder, A. W. (2014). 15 the guided discovery learning principle in multimedia learning. The Cambridge handbook of multimedia learning, 371.

FLETC (2023). JTAG ChipOff for smartphones training program.. (n.d.). https://www.fletc.gov/jtag-chipoff-smartphones-training-program#:~:text=Chip%2Doff%20forensics%20is%20an,raw%20data%20using%20specialized%20equipment.

Heyman, G. D., & Dweck, C. S. (1992). Achievement goals and intrinsic motivation: Their relation and their role in adaptive motivation. Motivation and Emotion, 16(3), 231–247. https://doi.org/10.1007/bf00991653

Irwanto, Saputro, A. D., Rohaeti, E., & Prodjosantoso, A. K. (2018). Promoting Critical Thinking and Problem Solving Skills of Preservice Elementary Teachers through Process-Oriented Guided-Inquiry Learning (POGIL). International Journal of Instruction, 11(4), 777-794. https://doi.org/10.12973/iji.2018.11449a

Lipman, M. (1987, November 30). Critical thinking: What can it be? resource publication, series 1 no. 1. ERIC. https://eric.ed.gov/?id=ED352326

Maayan, G. D. (2019, June 13). The data behind internet of things: Threats, ethics, and regulation. DATAVERSITY. https://www.dataversity.net/the-data-behind-internet-of-things-threats-ethics-and-regulation/

Nguyen, Q. D., Fernandez, N., Karsenti, T., & Charlin, B. (2014). What is reflection? A conceptual analysis of major definitions and a proposal of a five-component model. Medical Education, 48(12), 1176–1189. https://doi.org/10.1111/medu.12583

NSF - National Science Foundation. (n.d.). nsf99148 Foundations, Volume 2: Inquiry: Thoughts, Views, and Strategies for the K-5 Classroom. www.nsf.gov. Retrieved July 22, 2023, from https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf99148

Sathe, S.C., & Dongre Jawade, N. (2018). Data acquisition techniques in mobile forensics. 2018 2nd International Conference on Inventive Systems and Control (ICISC), 280-286.

Sitnikova, E., Foo, E., Vaughn, R. (2023). The Power of Hands-On Exercises in SCADA Cyber Security Education. 8th World Conference on Information Security Education (WISE), Jul 2013, Auckland, New Zealand. pp.83-94, ff10.1007/978-3-642-39377-8_9ff. ffhal-01463661

Treffinger, D. J., Young, G. C., Selby, E. C., & Shepardson, C. (2002, November 30). Assessing creativity: A guide for educators. National Research Center on the Gifted and Talented. https://eric.ed.gov/?id=ED505548

U.S. Bureau of Labor Statistics (BLS). (2022, September 8). Information security analysts : Occupational Outlook Handbook. U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Vermunt, J. D. (1996). Metacognitive, cognitive and affective aspects of learning styles and strategies: A phenomenographic analysis. Higher Education, 31(1), 25–50. https://doi.org/10.1007/bf00129106