CAL POLY

California Cybersecurity Institute

Digital Forensics Challenge

Senior Project Final Report

Zoe Lie (zlie@calpoly.edu)

Sydney Mendoza (smendo12@calpoly.edu)

Introduction

Project Overview

Each year, the California Cybersecurity Institute (CCI) puts on a weekends challenge called the California Cyber Innovation Challenge (CCIC) for middle school and high school students from all across California. This year in 2019, the challenge will be held on June 21st - June 23rd and the theme of the weekend is securing healthcare information and medical devices. Our team's task is to create the Digital Forensics Challenge (DFC) portion of the weekend. The DFC is a five hour competition in which the students get a case where digital and physical evidence will need to be collected, verified, and analyzed. Then a criminal case will have to be presented on a timeline the following day to the judges. The students will be scored on the evidence that they found, how well their presentation is, and if they figured out who was behind this crime(s).

Digital Forensics Challenge - Storyline

The storyline of the challenge is a ten day long crime. The students come into the challenge on the final day and have to work backwards, but this section outlines the story in chronological order.

In order to understand the crime, it is important to know some background information about the characters. This crime revolves around two people, Mark Turner and Aidan Harkirk. The background is important to completely understand the motive for the crime. Mark was married to Aidan's daughter, Sydney Turner. Sydney was killed in a car crash by the drunk driver Daniel McAffee Jr. Since Daniel's father, Daniel McAffee Sr., is a rich doctor, he paid for his son to get off with no charges.

The first day of the crime starts off with email conversations between Mark and Aidan. This email chain is talking about Sydney's funeral, however, the conversation is in a cipher. So, at this point the students will not know they are discussing a funeral and instead think that the two are talking about baked goods in a restaurant.

The second day there is more email communication in the cipher text between Mark and Aidan. They are at the funeral and Daniel Sr. shows up to it. This is where they begin to start planning their revenge against him.

On the third day, the two actually plan their revenge. They are going to hack into Daniel's bank information and make it look like Daniel is stealing money from Saint Martin's hospital where he works, when in reality Mark and Aidan are the ones stealing the money. However, all this is still in the cipher so the students will not know what they are actually saying.

The fourth day is where Mark sends a phishing email to Daniel's work. This email is disguised as a financial email to the hospital and if Daniel were to click the link and enter his credentials, then Mark will be able to get all his banking information. However, Daniel did not fall for the phishing email, so Mark and Aidan moved to their next plan on the fifth day of setting up a vampire tap in Daniel's office. This way, Mark will be able to tap into Daniel's network traffic in order to find his banking information. This is an outline of the big crime that the students will need to solve.

On the sixth day when they are home, they are looking into Daniel's network traffic when they get a knock on their door from their neighbor, Sarah Stothers. It is important to understand a little background on Sarah. She is living next door with her boyfriend Justin Walker. During these last five days, she finds out that Justin is cheating on her. This is all outlined in text messages between Sarah and her best friend Vicky Gilburt. So, Sarah goes over to the her neighbor’s house to try to get help. She wants to leave Justin but knows that if she tries to confront him, he will not let her leave. So she goes over to her neighbor’s house because she wants Justin out of the house for a few hours so she can pack up all her stuff and leave. At first, Mark and Aidan do not help her because they are a little busy with framing Daniel for money laundering. However, when she is over there, she notices something suspicious on Marks computer. He was running Wireshark to look at Daniel’s network traffic. Sarah takes a picture with her phone because she knows that it is suspicious to use wireshark.

The next day, Sarah texts Mark the picture that she has of Mark’s computer running Wireshark. She blackmails him into helping her by saying that she will go to the authorities if they do not help her. This just shows how desperate she is to get out of her relationship. She drops off a flash drive containing information about Justin. Mark notices that Justin has a pacemaker and that he is going in for a pacemaker update in a few days. He decides to write his own update to hospitalize Justin for a little bit in order to get him out of the house.

Two days later there is the pacemaker attack. This affects Justin and other people who have gotten the update as well. This is where the students come in to the crime and have to figure out what happened.

Client

Our client is the CCI. Partnered with the California National Guard and Cal Poly, San Luis Obispo, the CCI’s mission is to protect California from future cyber threats. The CCI hopes to achieve this goal by training, doing research for the government, academia, military, law enforcement, first responders, and private entities [1]. Since the CCI is partnered with Cal Poly, they mostly train and educate the next generation cyber workforce with the same learn by doing motto.

More specifically our main points of contact from the CCI are Danielle Borelli, the Director of CCI who is the person in charge of putting on the CCIC, Jessica MacMillan, the set designer and story creator for the DFC, and James Poirier, the technical resource for the DFC. These three people are the ones that we report to with our ideas, products, or questions.

Stakeholders

Not only will the CCI use our product in their state-wide recognized competition, but the students will also get to use our product during the competition. The challenge that we create is important to the students who are participating in the competition because it is a great opportunity for them to learn about cyber security and how to better protect themselves against attacks.

Framed Insights and Opportunities

Throughout Winter quarter, Zoe and Sydney had bi-weekly meetings with the whole team working on the CCIC. These meetings consisted of giving updates in our progress with forensics image and seeing what changes we had to make with the competition.

We also had meetings throughout the quarter only with Jessica to finalize the story line. These meetings were usually pretty extensive since we would go through the criminal storyline step by step, figure out the evidence needed to show that step in the story, and determine what was possible to create. These meetings had a few iterations which consisted of completely changing the storyline to make the competition a little more realistic, consistently adding new evidence, and adding new components to make this year's competition more challenging and better than the previous years.

Our Spring quarter bi-weekly meetings consisted of presenting the progress for each prototype of the forensics image that we created. From these presentations we were able to show the progress of the image and get feedback from Danielle, Jessica, and James about what looks great and what needs to be improved for the next prototype.

One thing that we were asked to add for the final prototype was checkpoints. Danielle wanted a way to measure how far along students were during the competition and track which evidence they found. Jessica, James, and our team sat down for about two hours trying to figure out how this could be possible. One suggestion was to add yellow codes to the top of all the evidence, but we quickly realized this would not work for emails or text messages. Then, we came up with the idea to just explicitly include "CHECK POINT #: WORD" in all the evidences including messages, emails, and documents. The students will then put the checkpoint and the word associated with that checkpoint into a form. This way we can be able to keep track of where the students are during the competition and see exactly what evidence they found. Each checkpoint they find will count towards two points of their final score.

On May 24th, we had our first walk through of the competition with our final prototype. During this meeting, the whole team had the chance to walk through what the whole day of the competition. This consisted of the team going through the escape rooms to find the physical evidence, Zoe and Sydney going through what the digital evidence will be found in the competition, watching the trailer and giving feedback for that.

Project Goals and Objectives

For our project, it was important to set up overall goals with our client that we want to achieve. These goals ensure that we are on the same page as the team from the CCI and that we are completing this product exactly how they want. We also have objectives which are smaller tasks to help us complete the goals in the long run.

Goals:

1. Understand Autopsy/UFED Reader and how evidence is found to create a case
    a. Objective 1: Do the Windows and and Android forensics trainings. This will teach us how to use Autopsy and UFED reader to obtain evidence and create a case.
    b. Objective 2: Create a "mini" case. This just helps us get familiar with how to hide evidence in a fair way that students will be able to find. Also solving this mini case using Autopsy will be great extra practice to make sure all the aspects of the forensics image are correct.
2. Create a product in the end that is challenging enough for the highly competitive students participating in the CCI and meets our clients at the CCIC's expectations.
    a. Objective 1: Meet with our client bi-weekly to report our progress and ask questions. This will ensure that we our meeting our client's expectations and delivering a product that they approve of.
    b. Objective 2: Make multiple prototypes that get tested by the team at the CCI. This will ensure that the challenge is difficult enough for the students attending the competitions since the members of the CCI have seen the competition the past two years.

Project Outcomes and Deliverables

The overall goal of this project is to create the Digital Forensics Challenge before the competition on June 21st. Our project will have two parts to it: the Android image and the Windows image. Both of these images will be a vital part in collecting digital evidence to solve the crime.

Formal Product Definition

Customer Requirements

The team at the CCI expects documentation of the challenge and a challenging Android and Windows image. First, the documentation consisted of reporting the storyline of the challenge, where the evidence is hidden in the images, and how we created the actual Windows and Android images. Second, the CCI asks us to provide a working yet difficult Android and Windows image that will be used to collect digital evidence in the competition. Another requirement the team from the CCI gave us was for the students to be able to solve or get close to solving the whole challenge in four hours.

Design Development

Our first image design concept acted as a run through of the storyline to notice the plot holes or evidence that we were missing. We originally planned to have the character Aidan have all the digital evidence on his computer, however after this first development, it made more sense to have his accomplice, Mark, be the one holding all the evidence since he is the more technically knowledgeable one of the pair. We also did not have the evidence for the phishing email, all the documents or ways to hide all the passwords. Also at this point, we did not have the

Android phone so all the communication between the character Sarah and Aidan were over emails and we could not include the communication between Sarah and Vicky.

During our next development of the image, we developed the Windows image owned by Mark. At this point, we still did not have the Android phone, so to show the conversations between Sarah and Vicky, we made instant messages hidden on a flashdrive. However, the conversations between Sarah and Mark were over email and were found on Mark's computer. In this version of the image, we had all the evidence to hide, however, the way we hid it and the passwords we used to protect it needed to be more difficult in the next implementation.

Final Design Concept

The final design concept included both an Android and Windows image. The Android image contains texts messages from Sarah to Vicky and from Sarah to Mark. These messages are how the students will connect Mark to the pacemaker attack. There are also the phone call history and web searches that add stronger evidence to the case. The Windows image still contains all the evidence from the previous prototype with better passwords and more creative ways of hiding the passwords. We also decided to include a new piece of evidence that was supposed to be a "manifesto" of Mark to make the crimes seem like more of a big deal and shows his confliction of doing the crimes.

Digital Forensics Challenge - Evidence Map

This section maps out the different evidence and how/where we hid it in both the Android and Windows images as well as in physical evidence.

- Android Image
    - Text messages between Sarah and Vicky talking about Sarah's relationship with Justin.
    - Text messages between Sarah and Mark talking about her blackmailing them.
    - The picture that Sarah uses to blackmail Mark and Aidan.
- Windows Image
    - Email conversations between Mark and Aidan in a cipher text. The are talking about getting revenge on Daniel Sr.
    - Password protected cipher word document.
    - The phishing email sent to Daniel at Saint Martin's hospital.
    - The email conversation between Mark and Aidan saying that they are moving to the next plan of using a vampire tap.
    - Email conversations between Mark and Aidan about making an update for the pacemaker and framing it on Sarah.
    - The actual pacemaker update file and executable.
    - A password protected Sydney Manifesto zip which contains a word document of Mark confessing all the crimes and the conflicts he is having with it, the funeral arrangements for Sydney, and her obituary.
    - A password protected bank zip with all of Daniel's fake bank transfer receipts, Wireshark packet captures, a text file with two more passwords in it. One for his "Sydney Manifesto" zip and one for the cipher document.

    - A batch script where you have to enter Mark’s Windows user password in order to get the password for the bank zip.
- Physical
    - The flash drive of Daniel Sr.’s actual bank information and the court case new paper having to do with his son Daniel Jr.
    - The flash drive containing Justin’s information including photos of him, his calendar, his Facebook url, and his Instagram url.

Exporting The Forensics Images

Exporting the Windows image took a little bit of time to figure out. We played around with using FTKImager, but in the end chose to use qemu-img on a Windows Machine to convert the VMware file to a E01 file. Here are the steps we used:

1. Export the VMware image from VMware Workstation Pro. Open your VMware image, go to “File”, and then “export to OVF”.
2. Use qemu-img on a Windows machine to convert the vmdk file to a E01 file. Here is the command we used:

   ```
   qemu-img.exe convert -f MarkTurner.vmdk MarkTurner.E01
   ```

Exporting the Android image was more straightforward because we had Bruce Pixley to help us use his software and license for that software. There were three programs we had to download in order to extract the data. They were USB Over Ethernet Client, UFED Physical Analyzer 7, and UFED 4 PC. The USB Over Ethernet Client was used for us to connect to Bruce’s license. Next, we used UFED 4 PC to do an Advanced Logical extraction of the Android data. To do this we just had to plug in the Android phone to our laptop and select Advanced

Logical extraction. By doing the Advanced Logical extraction, we were able to select everything that we wanted to extract like text messages, phone calls, internet searches, and calendar. After, we were able to open the extracted files with UFED Physical Analyzer 7 to make sure we got all the data we were looking for. Then from the Physical Analyzer, we were able to export it to a UFED Reader file. This is the file that the students will be getting in the competition.

Testing

Each prototype was thoroughly tested by Sydney, James, and others at the CCI. The prototypes were looked at based on if all the passwords could be cracked, all the evidence could be collected, and the whole challenge could be solved or be close to being solved in four hours. Table 1 below shows the positive results and what needs to be changed during the testing of each prototype. From each iteration of the forensics images, we used the negative results as what to improve for the next prototype.

Prototype	Positive Results	Change For Next Prototype
1	● After this first run through of the ten day challenge we were able to notice some plot holes in the storyline and figure out which evidence we still needed.	● One of the plot holes we found in the story line was to hide all the evidence on Mark's computer rather than Aidan's since Mark is the more technical one and the person mostly behind the crime. ● A second thing we noticed we need to change for the next time is having all the evidence and putting it in the correct place.
2	● We had all the evidence during this prototype and we were able to make creative ways to hide the passwords for different files.	● After this prototype, we realized there needs to be less "fluff" emails since the emails stored in Windows 10 are more complicated than the way they are stored in Windows 8. ● We also learned that we needed more password protected files to

		make the challenge a little more difficult.
Final	● We added more password protected files and more difficult passwords that will not be able to be cracked with rainbow tables in the alloted time. ● We also did not add as many “fluff” emails to make it easier to find them. ● We added “checkpoints” throughout the images to score the students during the competition. ● We also hid the evidence documents in more sub folders and added more fluff in folders. ● We also made an Android image for the communication for one of the characters.	● Nothing. This was the final version of the challenge.

Table 2: Testing Prototype

Management Plan

It was important to our clients at the CCI to create a milestone table with a deadline of when we were to complete each milestone. This milestone table will ensure that the overall project gets completed a few weeks before the competition in June and that the whole CCI team will know what is going on during the competition so they will be able to answer teams' questions. Each milestone is described in Table 2 below along with the target deadline and status of completion.

Milestone	Description	Target Deadline	Status
Finalize Storyline	Solidifying all the characters, the big crime, and the small crime	2/19/19	complete
Evidence Map	Following the storyline, map out what evidence will need to be shown for each situation	3/7/19	complete
Communication Timeline	Along with the Evidence map, create a communication timeline that shows the exact date and time that who says what and what is planted on the laptop or phone image	3/24/19	complete
Prototype 1	First Prototype of the 10-day crime. This allowed us to figure out what evidence was still missing and what holes there were in the plot line	4/19/19	complete
Prototype 2	Second Prototype to include all the evidence and hide passwords in a way that make the challenge more chronological	5/10/19	complete
Final Image	The last image included the phone as well as the laptop image which worked out kinks from the previous prototypes to make sure everything was solvable yet difficult to find	5/24/19	complete

Table 2: Milestone Deliverable Table

Team Responsibilities

In order for our team to work efficiently and deliver our product in time, it was important to us and our clients to split up team responsibilities. Delegating specific roles within our group will not only serve to help the overall organization of our task, but it will also allow us to gain specialization in the various facets of our product.

Sydney was in charge of everything that had to do with the Windows image. She did the Windows forensics training, learned how to convert a vmdk file to an encase file, and created the 10-day challenge on a Windows image. Creating the 10-day challenge consisted of doing all of the first two prototypes on the Windows virtual machine since we did not have the Android phone to work with until later. Sydney was also a main point of contact with the team at the CCI to answer questions about what would be possible for the challenge and to give updates about the progress of the challenge. Lastly, she was in charge of writing the final paper for this project.

Zoe's responsibility was to create the Android image after we got the phone for the final version.

References

[1] About the CCI. (n.d.). Retrieved from https://cci.calpoly.edu/about

[2] The 2019 California Cyber Innovation Challenge. (n.d.). Retrieved from https://cci.calpoly.edu/events/ccic/2019