On Developing Lab Materials for the Course CECS 7237 (Advanced Computer Forensics)

Jorge L. Rosado-Padilla
ME Software Engineering
Dr. Jeffrey Duffany
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract - Due to the rise of new technology advances, cyber activities are unfolding in unexpected forms. There are lots of professions such as law enforcement and IT specialists evolving in function of multiple conflicts, threats and complexities of cyber anomalies and uses of digital information in misleading ways. Therefore, the use and development of digital forensic tools is been growing rapidly in the last few years and we expect them to continue rising. Software such as FTK Imager and Autopsy are useful tools of this kind. As part of the Advanced Forensics course offered at the Polytechnic University of Puerto Rico, students get a practical and research approach by using several digital forensic tools in order to solve digital forensic issues. This article discusses the laboratory component of this course and the creation of a laboratory manual for guided exercises using FTK Imager and Autopsy tools.

Introduction

Graduate students pursuing the Certificate Program in Computer Forensics (GCCF), Masters of Computer Engineering or a Masters in Computer Science and those working in the area of Information Technology (IT) must develop practical and analytical skills in several applications in order to diagnose, identify and provide solutions to threats and cyber-security issues in general. Digital Forensics emerges as an in important field of this type of incident responses. At the Polytechnic University of Puerto Rico (PUPR), the Advanced Computer Forensics (CECS 7237) course offered in the curriculum of graduate studies includes a research approach. It is indeed relevant to master state-of-the-art techniques to achieve a full comprehension of complex problems arising in the cyber environment [1].

Based on this, I developed a more detailed lab sequence that will benefit students through practical examples and exercises using FTK Imager and Autopsy software. These tools provide a practical experience at no cost in image forensics, cloud forensics and several levels of analysis to different digital devices (such as USB drives and cellphones). In this article I discuss the extent of my project, future approaches and research by using the Lab manual and its relevance to the aforementioned course.

Background

As a graduate student I must state it is rewarding to create pedagogical materials to put in practice in the real world. Going beyond theory and research creates a more empathetic approach towards completing graduate studies. There was a necessity in the Computer Engineering and Computer Science Department at PUPR to develop a lab manual for the Advanced Computer Forensics course. It was my personal interest to develop such materials, to give them a structure and put the sequence in a laboratory manual format. I also found interesting to create content that the University can use. This is a project with beneficial intent towards future students.

Problem

The Advanced Computer Forensics course is currently taught using the Lab Manual for Guide to Computer Forensics and Investigations, Fifth Edition, 2015, Andrew Blitz, Course Technology, Cengage Learning. At first glance it is a useful tool, but it does not present enough visual reference to perform practical tests. It is challenging to provide graduate students with a detailed laboratory manual explained in a basic yet meticulous manner. That is the reason to develop and test a different lab manual, testing its sections, editing for best and in-depth explanations, and providing an answer key to each review section. A better explained manual will benefit the student's academic experience and will guide their practice in a well-organized way. In other words, this is a proposal for autodidactic practice. As this is a manual for the Advanced Computer Forensics course,

these materials are meant to be coordinated with the introductory course CECS 7235 – Computer Forensics to limit some of its overlapping contents. Finally, the manual is based on the free tools mentioned in the Equipment and Materials section, meaning that there is no need to buy or subscribe to any program license in order to complete each lab.

Equipments and Materials

Nowadays there are multiple options to perform computer forensics analysis such as EnCase, FTK Forensic Toolkit, Magnet Axiom among others. Unfortunately for most students, these alternatives are expensive. With the following applications they can analyze several complex digital scenarios from a forensic perspective and doing so for free. They also provide the advantage of being lightweight in capacity; enough for the students to be able to install them on their own computers. Now we will describe each software and its uses at first glance.

FTK Imager

As AccessData's website states, FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence. One of the major advances for students and professionals is that this is a free tool that allows to create, preview and mount images and folders from different devices such as USB or DVDs, seeing its exact content as is on the original drive. It is part of a larger suite called FTK or forensic toolkit. See figure 1 [2].

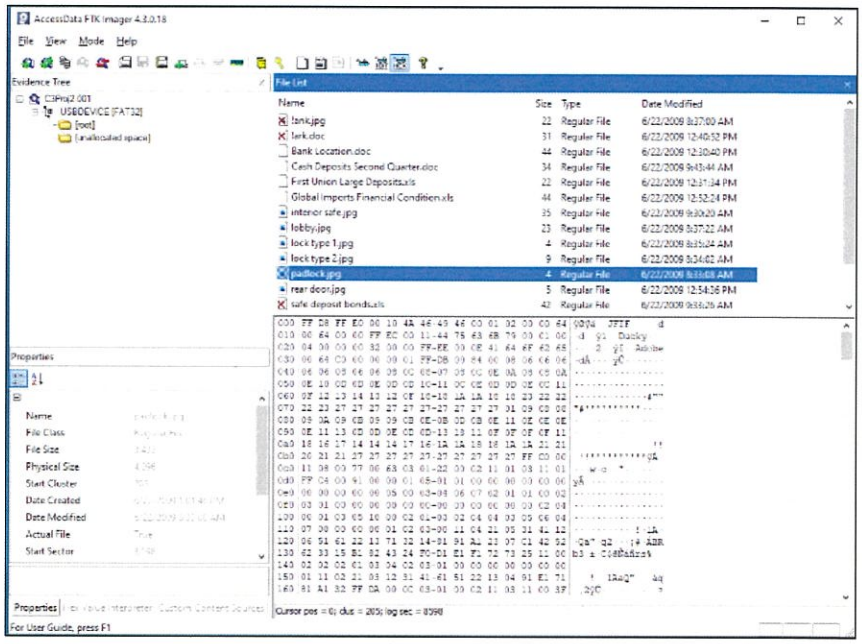

Figure 1 - FTK Image data display

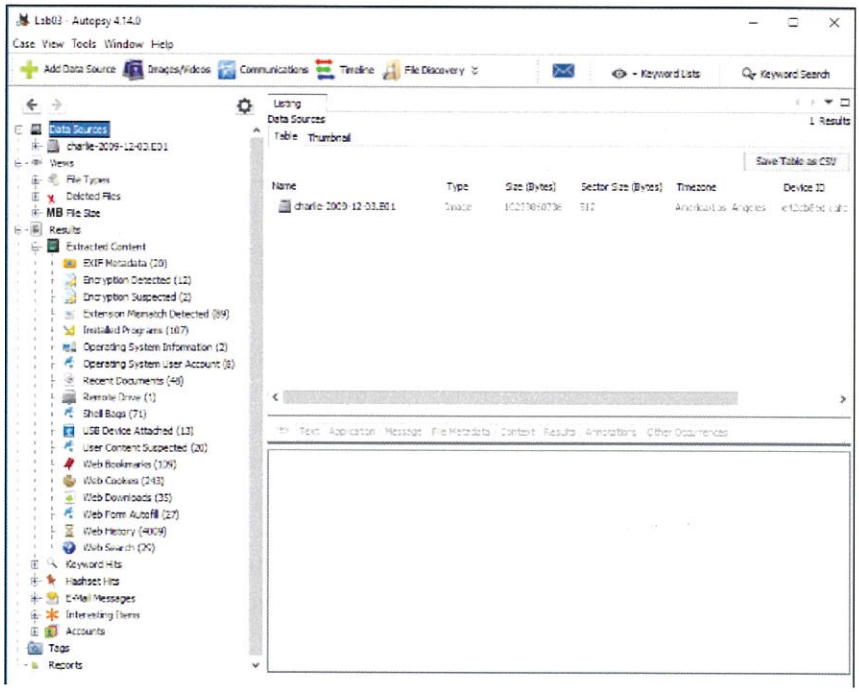

Figure 2 - Autopsy data display

Autopsy

This is also a free tool where users can analyze images, logical files, disk images, unallocated space image, among other sources. It is a GUI for the Sleuth Kit, which is a collection of command line tools that allows for image analysis and file recovery even after the user has erased it. This program supports common file systems including NFTS, FAT32/ExFAT, HFS+, ISO9660, Ext3/Ext4 and UFS. Its several functions and modules are developed to allow the user to perform data analysis in an intuitive and friendly manner. Some of the modules provide: keyword search, timeline analysis and e-mail analysis and Android analysis. It also features a reporting tool enabling reports to be generated in a variety of formats such as HTML and Excel spreadsheets. See figure 2 [3].

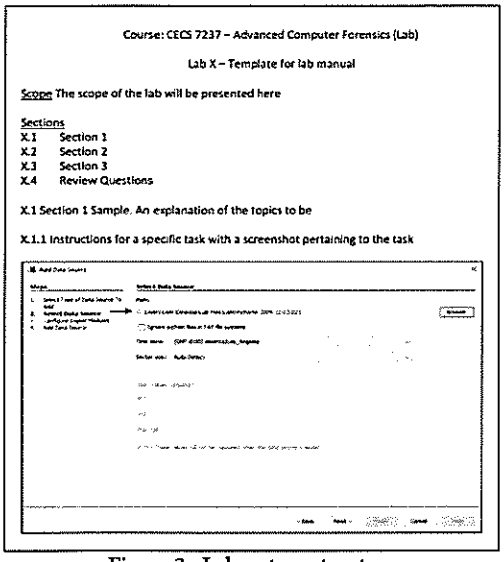

Figure 3 - Laboratory structure

Methodology and Discussion

The structure of this Lab manual suggests 10 Labs or "tutorials" as follows. In Lab 0 there are tool installation instructions for FTK Imager and Autopsy. Labs 1 to 5 were designed and tested as a sequence: Labs 1 and 2 are simple imaging and analysis to get the student used to the tools that they are going to be using. Labs 3 to 5 are the tool-specific tutorials. From Lab 6 to 9, these are self-contained; each focusing in a technology cloud mobile and e-mails. Even though they are self-contained, these assume previous knowledge on how to use the tools from the first five Labs. Thus, providing a logical progression of difficulty. Finally, Lab 9 is a full scenario where the student or user must apply their knowledge from previous labs in order to find and discuss a solution to a hypothetical digital forensic problem.

Going into detail of the laboratory contents, each is divided into multiple sections: Title, Scope, Section menu, Contents and Review questions. The title identifies the laboratory. The scope defines the objective or skills that the student will acquire after completing the lab. The sections are the structure for presenting the contents (figure 3).

Review questions (figure 4) are at the end of labs 1 to 9 in order to put the tutorial into real practice. Each lab's completion is aimed to be 1 hour, including the questions section. The questions aim to test the concepts that are presented in the lab. They are varied, including searching for a specific flag on the image being examined and searching the Internet for manufacturer documentation on software to learn more about its features.

The images that are used on these labs come from various sources. The main one is the materials available from Lab Manual for Guide to Computer Forensics and Investigations, Fifth Edition. Images from this source were used in labs 3 to 8 [4]. The second source of images was Digital Corpora. This is a website that provides resources to be used in forensics education research. The mobile image used for lab 6 and the image for the lab 9 scenario were taken from here [5].

Now we will explain each laboratory in its relevance and progression characteristics:

• **Lab 0 – Tool installation tutorial**: With this Lab the student will get the necessary equipment to work with through the rest of the manual and other CECS 7237 coursework. As mentioned in the Equipment and Materials section, both FTK Imager and Autopsy software are free downloadable tools. Furthermore, students can download these programs in their own computers so there is no need to access them through the University's network.

• **Lab 1 – USB Image Capture:** The purpose of this lab is to teach students the basics of imaging exploration using FTK Imager. The student uses a personal USB for the image capture. By doing so, each student will get a different experience when completing the lab analysis.

• Lab 2 – USB Image Exploration: In this lab the student analyzes the image captured in the previous lab. This is done using Autopsy. It introduces the student to the basis of creating a case and adding a data source on Autopsy. It also encourages the student to learn about the way autopsy manages its analysis by exploring all the modules available.

• **Lab 3 – Examining Images:** In this lab the student starts to learn

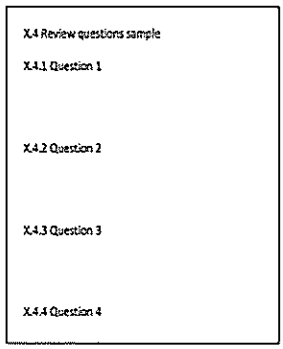

Figure 4 - Review questions sample structure

about the features of FTK Imager while exploring a FAT32 and NFTS file system images. These are two of the file systems commonly used by Windows interface. The student will be able to add evidence to FTK Imager, browse and export regular and deleted files from the image. The lab also encourages students to learn about the MFT (master File Table) and how file timestamps work.

• **Lab 4 and Lab 5 – Analyze Image of a Hard Drive, part I and part II:** In these labs the student

will examine an image using Autopsy. It presents the student with an overview of the Autopsy interface and explain its UI elements. It also explains how to create or open a new case and add its data source. Autopsy provides keyword indexing. Then the student can search for a keyword and the software will return all the instances where the keyword appears in the image. This becomes handy for e-mail analysis. The student will learn to use Autopsy's report generating feature of the findings in the image. The student will learn to use Autopsy's timeline function, where all the events in the image are sorted on a timeline.

- **Lab 6 – Mobile Forensics:** Here, the student will have a chance to examine mobile devices' images with the forensic software that we use on the course. We will pay special attention to the Android Analyzer module on Autopsy. The student shall examine calls, contacts and messages acquired from a google Pixel 3 device, running Android 9. The student is encouraged to explore around the device image in order to explore how different accounts like Facebook and WhatsApp are identified.
- **Lab 7 – E-mail Forensics:** It focuses on e-mail forensics. We start with a section on analyzing e-mail headers. The student will remark the importance of e-mail headers and how to read them to learn about the path an e-mail takes before arriving to its destination. Then we move to Autopsy and the student will search an image for e-mail evidence, including attachments. Special focus is placed on using Autopsy's Communication Visualization feature.
- **Lab 8 – Cloud Forensics:** It teaches how to analyze files from three of the most popular cloud providers: Dropbox, Google Drive and One Drive. The lab is focused on the local files each cloud provider leaves present on a hard drive and how we can extract data from them.
- **Lab 9 – Digital Forensic Scenario:** In this lab the student is presented with a simple scenario to solve about an information leak on a fictional company. This scenario can be solved with the set of skills learned in the Lab manual.
- Answer Key: Provides the answers for self-study, so students can verify the responses given to each set of review questions following labs 1 to 9. Each answer sheet is going to be printed out and given to all students at the beginning of class.

Conclusion

With the immense adoption of technology that we are seeing these days, the use of digital devices for keeping track of all aspects of our everyday life grows. This in turn means that more and more people are using digital devices that first were perceived as useful and now society considers them as essentials. The need for skills in forensically analyzing these devices grows with each passing year. In the lab manual that was developed, students were provided with a practical overview of different aspects of digital forensics. The set of skills that were built on this lab aims to help the CECS 7237 course in its research component through a methodic way of thinking that will improve the academic experience of each student.

Future Work

After completing this project, the purpose of creating this laboratory manual is finished in an initial phase. There is more that can be done to give students a whole autodidactic approach to digital forensic tools. As we deal with an advanced course requiring advanced methods of analysis, one can suggest the use of commercial forensic software to explore scenarios with more complex and challenging situations emphasizing real life panoramas. This proposal comprises several long-term objectives: (1) to statistically test the effectiveness of this laboratory manual with a group of students; (2) to engage PUPR to acquire more applications on this metanalysis area of study; (3) to publish this manual in a digital platform in accordance to the technological and academic resources the University already have; (4) to include FTK Registry Viewer and OSForensics in the lab assignments of CECS courses; and, (5) to integrate software and procedures used by digital crime labs in the island.

References

[1] A. Cruz and J. Duffany, "Development of a Graduate Certificate Program in Computer Forensics," 10th Latin American and Caribbean Conference for Engineering and Technology, Panama City, Panama, 2012. [Online]. Available: https://pdfs.semanticscholar.org/e7d4/37717cd09fded2ad2f1530823b143c3445be.pdf?_ga=2.11966258.783497083.1588724042-2104436147.1588724042

[2] AccessData, "Homepage." Accessed April 28, 2020. [Online]. Available: https://marketing.accessdata.com/

[3] The Sleuth Kit, "The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools." Accessed April 28, 2020. [Online]. Available: http://www.sleuthkit.org/index.php

[4] A. Blitz, *Lab Manual for Guide to Computer Forensics and Investigations*, 5th ed. Boston, MA: Course Technology, Cengage Learning, 2015.

[5] Digital Corpora, "Homepage." Accessed April 28, 2020. [Online]. Available: https://digitalcorpora.org