2019

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

DATA FORENSICS SOLUTIONS FOR HIGHER EDUCATION ENVIRONMENT: SCORING FRAMEWORK FOR OPTIMAL CONFIGURATION

Caitlin Mabe

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2019

Approved by

Advisory Committee

Dr. Jeffery Cummings	Dr. Lucas Layman

Dr. Elizabeth Baker, Chair

Accepted By

Dean, Graduate School

TABLE OF CONTENTS

ABSTRACT

DATA FORENSICS SOLUTIONS FOR HIGHER EDUCATION ENVIRONMENT: SCORING FRAMEWORK FOR OPTIMAL CONFIGURATION. Mabe, Caitlin, 2019. Capstone Paper, University of North Carolina Wilmington.

The Information Security department at the University of North Carolina Wilmington has the responsibility of providing expertise when an incident occurs involving UNCW data. Depending on the incident, it may require data forensic investigation to preserve and extract digital evidence. In order to perform this type of investigation, procedures for data preservation and extraction need to be established. These procedures must ensure data integrity, be compliant with other Information Security procedures, provide a chain of custody, have the ability to hold up in court, and it is recommended that the procedure be easy for Information Security personnel to follow. Hardware and software will also be utilized during a data forensic investigation. The hardware and software must uphold data integrity and be compatible with multiple types of data storage devices as well as multiple operating systems. Additionally, the hardware needs to have a secure configuration and the software should support multiple investigation cases.

This capstone project explores all the possible options for data forensic procedures, hardware, and software and evaluates each option based on a set of criteria. The criteria were chosen based on research of industry knowledge and best practices and is the basis for the scoring framework, which is the key to finding the optimal solution. This capstone uses the scoring framework to determine the optimal data forensic solution for UNCW. In addition to assisting UNCW, this scoring framework will also be able to aid other higher education institutions in finding their optimal data forensic solution.

CHAPTER 1: INTRODUCTION

Information security plays a vital role in an Information Technology department and can be defined as "the protection of information and its critical characteristics (confidentiality, integrity, and availability), including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology" (Whitman and Mattford, 2014). Protection of information is necessary due to inevitable security incidents that occur in any company, including higher education institutions. Regardless of the type or size of an incident, it is important to know exactly the course of action needed to handle the incident (*Incident Management and Response*, Educause). Appropriate handling of an incident will rely on organizational concerns and dedicated infrastructure to be established.

There are some incidents, such as data misconduct, that may warrant the need for data forensic investigation in order to retrieve evidence. To complete this type of investigation, appropriate policies, procedures, hardware, and software are required to protect the data to ensure data integrity. A data forensic investigation will launch an electronic discovery (e-discovery) process which may include all or some of the following phases: Identification, Preservation, Collection, Processing, Review, Analysis, Production, and Presentation (*EDRM Model*, Duke Law). It is important for a data forensic and e-discovery process to be in place before an e-discovery request is received for litigation because "[f]ailure to respond or to respond in a timely manner to an e-discovery request can result in adverse inference jury instruction and/or fines and penalties" (*E-Discovery Toolkit,* Educause).

Organizations, in general, may approach data forensics and e-discovery in different ways, such as conducting everything in-house or outsourcing to a vendor (Prounis, 2013). Cost is a

main concern for private organizations, whether in monetary value or time, and these organizations have to compare each option to determine which will provide a greater return on investment (Prounis, 2013). These same options of in-house or outsourcing are also available to higher education institutions and thus, in contrast to private organizations, their main concerns are teaching, research and learning which cater to different types of employees, faculty and staff, as well as students. Therefore, data is being accessed, processed, and created by multiple types of users, with some being personal data on personal devices. This has to be taken into consideration when it comes to data forensics and e-discovery in higher education. Data forensic operations will need to be specific as to what data is appropriate for investigation; this is where data governance is of importance for higher education institutions. Having established data governance will outline what is appropriate university data and "assists in maintaining data integrity, controlling access, and securing data storage" (*The Compelling Case for Data Governance*, 2015).

The Information Security department at the University of North Carolina Wilmington is in need of a data forensic and e-discovery process for appropriate university data, specifically in reference to the preservation and collection (also referred to as extraction) phases. This process must include the use of an operating procedure for data forensics, hardware, and software or use of a third-party company. The data forensic procedure is necessary to guide individuals through completing these phases accurately and consistently. The use of hardware and software, or a third-party company, is also needed to properly protect and extract data. Thus, the use of a scoring framework to determine the optimal solution for higher education institutions would be helpful to guide UNCW in choosing the best data forensic investigation processes for their organization.

CHAPTER 2: PROBLEM CONTEXT

2.1 – Background Information

As would be the situation with a typical college or university, the Information Security department at UNCW has the responsibility of providing expertise when an incident occurs involving UNCW data: such as data misconduct, data breach, system compromise, computer viruses, etc. At times, this may require forensic analysis of data to investigate the root cause of an incident. The problem UNCW Information Security faces with this process is that there are no official written policies or procedures to follow with respect to data forensics. As a result, there is insufficient software and hardware to ensure proper investigation of data. UNCW Information Security currently makes decisions based on their best judgement of the steps that need to be taken during a data investigation based on the electronic discovery reference model (EDRM).

> "The EDRM diagram represents a conceptual view of the e-discovery process, not a literal, linear or waterfall model. One may engage in some but not all of the steps outlined in the diagram, or one may elect to carry out the steps in a different order than shown [in Figure 2.1 below]" (*EDRM Model*, Duke Law).

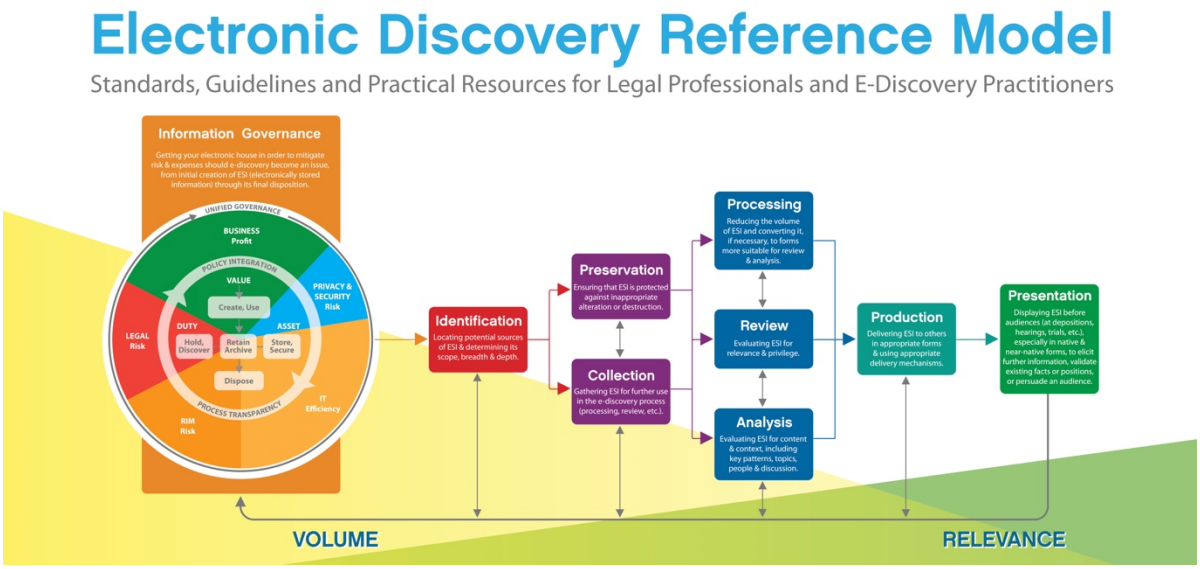


Figure 2.1 – Electronic Discovery Reference Model (Source: *EDRM Model*, Duke Law)

The concern for UNCW Information Security in an investigation is the preservation and collection (or extraction) phases of the e-discovery process, specifically with regard to data stored on UNCW owned devices (i.e. desktop computers, USBs, laptops, tablets, etc.). The process for preserving and extracting email or data stored on network locations is outside the scope of this capstone project; however, a request of that nature would be handled in an appropriate manner if requested by the proper authority. Preservation is an essential phase in the e-discovery process as it is the foundation to ensure data remains legally defensible (*Three Common Techniques for E-Discovery Preservation,* 2014; *Preservation Guide,* Duke Law). Appropriate preservation of data allows for data integrity and nonrepudiation. Once preservation of data is complete, extracting the relevant electronically stored information (ESI) to the investigation is the next step (*Collection Guide*, Duke Law). It is crucial that data also remains unaltered during extraction to warrant legal defensibility (*Collection Guide*, Duke Law). To complete these phases in an investigation, in conjunction with policies and procedures, software and hardware are used as tools to appropriately guide UNCW Information Security through the preservation and extraction process.

2.2 – Specific Issues at UNCW

UNCW Information Security currently does not have an official policy or procedure regarding data preservation and extraction for a forensic investigation. Security policies place emphasis on guiding behavior for who, what, and why; while security procedures focus on when, where, and how (Dunham, 2018). While developing a procedure is part of this capstone project, creating an official policy is beyond the scope. However, UNCW Information Security is currently in the process of drafting an incident response policy which has the potential to act as the overarching guide for the data preservation and extraction procedure. The data forensic

procedure for data preservation and extraction will need to include details on when it would be used, possible locations for data, and the steps for consistent execution (Dunham, 2018).

UNCW Information Security needs to identify appropriate hardware and software to perform adequate data preservation and extraction. The current hardware proved to be insufficient during an incident in early Fall 2018. When responding to the incident, the plan was to use the available mobile hardware to perform forensic preservation of data on a hard drive while out in the field. The mobile hardware was not suitable for this use, and the security team had to take possession of the hard drive in order to complete the task in their own secure location with other equipment.

Proper forensic software to appropriately extract data under investigation is a limitation for UNCW Information Security. They previously had one of the top leading industry tools, EnCase, to use for data investigations. However, it was not a beneficial tool because of cost and user training requirements. Often, once an employee was trained and certified in the software, that individual became in high demand in the industry and left UNCW. Ultimately, the cost of EnCase outweighed any benefits. Thus, currently, UNCW Information Security is without any software to use for incidents that required preserving or extracting data. A manual process of copying the data from one location to another was adopted for preservation, then extraction was the manual process of searching through the data for relevant electronically stored information. This manual process introduces the risk of losing data integrity, and once integrity is lost, the data evidence would be inadmissible in court.

2.3 – Criteria for Data Forensic Procedure, Hardware, and Software

New hardware, software, and an official data forensic procedure is necessary for UNCW Information Security to perform proper data preservation and extraction going forward. Table 2.1

lists criteria for each segment based on industry knowledge and best practices. The criteria are necessary in order to develop the scoring framework for choosing an optimal solution.

Procedure Criteria	Hardware Criteria	Software Criteria
• Compliant with other Information Security procedures • Uphold data integrity • Provide chain of custody • Ability to hold up in court • Easy for personnel to follow	• Cost effective • Uphold data integrity • Compatible with multiple media storage devices • Secure configuration • Secure network integration	• Cost effective • Uphold data integrity • Compatible with multiple operating systems • Support multiple cases • Easy for personnel to use

Table 2.1 – Scoring Framework Criteria (Sources: *Quality Standards for Digital Forensics,* 2012; *EDRM* Collection *Standards,* 2014; Barbara, 2007; *Chain of Custody in Computer Forensics*; Wolfe, 2003)

The data forensic procedure needs to be in accordance with other overarching official policies and procedures and allow for maintaining integrity of the data under investigation. It will also be important to have a chain of custody in the procedure to further preserve integrity. The chain of custody is the documentation of evidence of who performed the data preservation and extraction, when it was done and who/when the evidence is transferred to another person (*Chain of Custody in Computer Forensics*). It would be recommended that the procedure be easy for an authorized member of UNCW Information Security to follow and perform the written steps.

The chosen hardware and software must also meet specific criteria. They will each need to uphold data integrity and be compatible with multiple types of data storage devices (i.e. SATA drives, SSD drives, USBs, etc.), as well as multiple operating systems (i.e. Windows, MacOS, Linux, etc.). The hardware will need to have a secure configuration that will prevent it from altering evidence. The software should be able to support multiple investigation cases in the

event of concurrent investigations. It would be nice for the hardware configuration to allow for secure network integration, so that individuals working a case can properly be identified with their UNCW credentials. This could help create a stronger chain of custody. Also, network integration could provide the option for forensic copies of data to be backed up to a secure server; this would pose as a recovery option if the data under investigation becomes altered or unavailable. Easy to use software is another criterion that would be nice to have so investigations can be done efficiently, without having to work with difficult software. Cost effective solutions would be an additional benefit, but this could be at the discretion of the department as to what would qualify as cost effective.

CHAPTER 3: AVAILABLE SOLUTION OPTIONS

3.1 – Data Forensic Procedure Options

The procedure for data preservation and extraction must provide enough detail to allow for consistent execution in order to reduce the possibility of introducing risks, such as "loss of availability, failure of data integrity, and breaches of confidentiality" (*Security Operations*, Educause). While sufficient detail is required for the operating procedure, it should not be too reliant on advanced expert knowledge as this could result in procedural gaps (Dunham, 2018). The procedure will have gaps if it is not able to be executed reliably by high and lower level employees of Information Security that have permission to perform the procedure. Technology and infrastructure can change often, so it is important that the procedure be reviewed and updated periodically to prevent it from becoming outdated or inaccurate (*Security Operations*, Educause).

There are two options for the data forensic procedure for data preservation and extraction: 1) keep the phases combined; or 2) split the phases into separate operating procedures. Either option will need to abide by the procedure criteria provided in Table 2.1.

3.2 – Data Forensic Hardware Options

The hardware options include purchasing a preconfigured forensic workstation or repurpose an existing standard workstation. There are a few companies that offer preconfigured forensic workstations that are built for the sole purpose of data forensics. These forensic workstations are securely configured to ensure data integrity and to be compatible with multiple types of media storage devices. Forensic Computers Inc. offers several forensic workstations available for purchase ranging from $4,000 - $23,000 (*Desktop Workstations - Workstations - Forensic Computers, Inc.*).

The alternative to purchasing a preconfigured forensic workstation is to repurpose an existing standard workstation that can be securely hardened to best fit the needs for an organization. This option can still uphold data integrity, be compatible with multiple types of media storage devices and be securely configured.

Regardless of the type of workstation chosen, the purchase of a mobile imaging device is recommended in order to conduct secure data preservation out in the field. This mobile imaging device will allow for immediate action while still providing a secure environment for preserving the data to ensure data integrity. Tableau makes a portable imager, TX1 Forensic Imager, that is well suited for in-the-field data preservation. This imager is also network-enabled to offer 10GB Ethernet connection for fast network imaging performance (*Tableau TX1 Forensic Imager - Forensic Computers, Inc.*).

3.3 – Data Forensic Software Options

There are many different licensed industry software available for purchase that can be used for data investigations. When licensed software is purchased, the expectation is already there that it will perform at a certain standard to uphold data integrity, be compatible with multiple operating systems and have the ability to support multiple investigation cases. AccessData is a company that offers different types of forensic software; their Forensic Toolkit (FTK) software would be a suitable solution. “FTK is an award-winning, court-cited digital investigations solution built for speed, stability and ease of use” (*FTK – Digital Investigations*).

The alternative to purchasing software is to use open-source software. Open-source software is free to use, but it still has the ability to uphold data integrity. Some open-source software can also be compatible with multiple operating systems and support multiple investigation cases. Autopsy (open-source) from The Sleuth Kit and FTK Imager (free) from AccessData are two pieces of appropriate software that can be used together to meet the needs of an organization. FTK Imager is a tool that captures data “in a forensically sound manner by creating copies of data without making changes to the original evidence” (*FTK Imager 4.2.0*). Autopsy is simple to install, cost effective, and fast in providing results (Carrier).

3.4 – Data Forensic Third-party Company Options

The last option would be to use a third-party company for data investigations, leaving an organization only responsible for data preservation. Just as with the workstation options, the purchase of a mobile imaging device is recommended when choosing to go with a third-party company to allow for secure data preservation. This will allow an organization to have control over this phase of an investigation, then the preserved data forensic image would be analyzed by the third-party with their own hardware and software. The use of a credible third-party would be

able to ensure data integrity and complete investigations in a timely manner. There are a number of companies that cater to data forensics. Guardian Forensics & Data Recovery, Forensicon, Atlantic Data Forensics, and Kroll are just a few examples of companies that perform investigations. In general, these types of companies are used to outsource the data extraction and examination process from preserved data to gather relevant data needed for court.

3.5 – Scoring Framework for Optimal Solution

The chosen option of either a single data forensic procedure for data preservation and extraction, or separating the phases into two procedures, is up to the discretion of the department. The optimal solution for the procedure will be based on how operations are conducted in the department to best fit within the workflow.

The scoring framework in Table 3.1 shows the scorecard for evaluating each hardware and software option based on the predetermined criteria. Some criteria may hold more weight than others based on their importance to the department, but a default weight of 1 is given for all criteria. A total score of each hardware and software configuration is tallied in Table 3.2. The configuration with the highest total score is the optimal solution.

Hardware	Cost-effective	Uphold data integrity	Multiple storage devices	Secure configuration	Secure network integration	Hardware Score
	Weight					
	1	1	1	1	1	
Preconfigured Workstation & Mobile Imager						
Repurposed Workstation & Mobile Imager						
Third-party Company & Mobile Imager						
Software	**Cost-effective**	**Uphold data integrity**	**Multiple OS**	**Multiple cases**	**Easy to use**	**Software Score**
	Weight					
	1	1	1	1	1	
Licensed Software						
Open-source & Freeware						
Third-party Company						

Table 3.1 – Scorecard Template

Configuration Total Scores			
	Hardware		
Software	Preconfigured Forensic Workstation & Mobile Imager	Repurposed Standard Workstation & Mobile Imager	Third-party & Mobile Imager
Licensed Software			
Open-source & Freeware			
Third-party			

Table 3.2 – Configuration Total Scores Template

CHAPTER 4: EXPLICATION OF CRITERIA AND SCORING FRAMEWORK MECHANICS

An in-depth understanding of the procedure, hardware and software criteria, beyond what was discussed in Chapter 2.3, is important for an organization to have in order to identify the best procedure option and to use the proposed framework accurately to find the optimal hardware and software solution. This chapter thoroughly will discuss the criteria and the scoring mechanics for the framework.

4.1 – Data Forensic Procedure Criteria

The procedure criteria are meant to guide an organization in writing a data forensic procedure(s) for data preservation and extraction. When writing this new procedure(s), an organization must take their other applicable procedures into account to ensure that the new procedure(s) is compliant and does not introduce any conflicts. The new procedure(s) will need to be written in a way to ensure that the data under investigation maintains integrity; without data integrity, an investigation could be put in jeopardy of losing its validity. A chain of custody process will need to be documented in the new procedure(s), so every member of the staff knows exactly how to record their work during an investigation. The new procedure(s) will be carefully written so that it covers all vital steps in the process of data preservation and extraction. It is important that the procedure(s) not have any missing information so that it can be held up in court, if necessary, without question of its validity. Lastly, the new procedure(s) needs to be easy enough for the appropriate staff to follow so it can be executed properly.

4.2 – Data Forensic Hardware Criteria

The hardware criteria are broken down into five categories which include cost-effectiveness, data integrity, multiple storage devices, secure configuration and secure network

configuration. Cost-effective hardware and software will vary from one organization to another, so it is important for an organization to know their budget in order to properly identify the most cost-effective solution. Upholding data integrity means to keep the data consistent and unchanged; this must remain true during an entire investigation. Multiple storages devices imply that the hardware is compatible with different types of storage in use throughout the organization. A secure hardware configuration indicates that there are specific settings in-place to ensure that the computer is not vulnerable to alterations that could affect data integrity. Finally, network integration would give the ability to access the forensic workstation remotely and move data across the network, to and from other locations. Introducing network integration must be done carefully to ensure access to the workstation and data remains secure.

Along with these hardware criteria, there is a piece of default hardware that is recommended to go with both the hardware and third-party options, and that is the use of a mobile imaging device for data preservation. This device will provide a secure environment, which is vital for keeping data integrity, to allow for immediate data preservation to be conducted out in the field.

4.3 – Data Forensic Software Criteria

Cost-effectiveness and data integrity are part of the software criteria as well. What is considered cost-effective software will vary depending on the organization, but whatever software is chosen, it must ensure that data remains consistent and unchanged. The software criteria for evaluating the options also include compatibility across multiple OS, the ability to create multiple, simultaneous cases and be easy to use for the staff. The software should be compatible with multiple operating systems, both mobile and desktop, to cater to all types of devices that may be part of an investigation. Operating systems include Windows, MacOS,

Linux, iOS and Android, among others. The software should also have the ability to create multiple cases in the event of simultaneous investigations of different matters. The knowledge and technical skill of the staff that will be using the software should be evaluated to assess the ease of use of the software.

4.4 – Scoring Framework Mechanics

The goal is to create a scorecard to help the organization choose the best solution for them. In order to identify the optimal solution, the framework template in Table 3.1 will be used to evaluate the specific hardware and software brands and third-party company the organization is considering. Each hardware, software and third-party company piece is evaluated based on the criteria listed above and given a score. The score is based on a 5-point scale with 1 being "Not Applicable", 2 "Least Appropriate", 3 "Slightly Appropriate", 4 "Moderately Appropriate" and 5 "Most Appropriate". As stated in Chapter 3.5, an organization may opt to weight some criteria differently depending on what is of most value and importance to their department, but a default weight of 1 is given for all criteria. An organization can select a criteria weight based on the level of importance ranging from 1 to 3 with 1 being "Low", 2 "Medium" and 3 "High". The scorecard should be filled out by security personnel responsible for data forensics and the person with budget information that has the purchasing authority.

The following chapter will apply the framework described above at UNCW. Specific hardware, software and third-party company options have been discussed in Chapter 3 and will be used as the selected options for UNCW when applying the framework. While these are the chosen options for UNCW, it is not exhaustive as there are additional hardware, software and third-party companies available that are not listed in this paper that may be more applicable to other organizations.

CHAPTER 5: APPLICATION OF FRAMEWORK AT UNCW

5.1 – Data Forensic Procedure

As stated in Chapter 3.1, there are two options for the data forensic procedure for data preservation and extraction: having a single procedure to include both phases; or splitting them into two separate procedures. Having a combined procedure for data preservation and extraction would provide only a single document to follow, review and update. This option eliminates possible risk of missing any steps since all the necessary details for preservation and extraction would be in one place. The person executing these tasks would not have to flip between two procedures. However, separating the preservation and extraction phases into different operating procedures also has advantages. There could be times when these two phases do not need to be completed in tandem; therefore, having them separate would be more beneficial. This would prevent anyone from inadvertently performing steps beyond necessary action for an incident. For example, UNCW Information Security may receive a legal hold notice requesting only preservation of data relating to an incident be completed, but not to perform any extraction of specific data.

To align with current workflows of UNCW Information Security, the decision was made to have data preservation and data extraction as two separate phases, as well as separate procedures. This will ensure that only the steps of a requested phase are completed if they are not requested to be done together. These procedures will be written to be in compliance with each other, as well as other UNCW Information Security procedures that may be relevant. The procedures will also be written to ensure data integrity, establish a chain of custody, and be adequately detailed in a way that all UNCW Information Security staff can execute them

consistently. Lastly, writing the procedures will follow the same approval process of current UNCW Information Security procedures to make sure they are accurate and complete.

5.2 – Data Forensic Hardware

There are two options for hardware: purchasing a preconfigured workstation or repurposing an existing standard workstation. With either option, the purchase of a mobile imaging device is recommended.

A forensic workstation from Forensic Computers Inc. would be very robust and more than meet the needs of UNCW Information Security. The disadvantage is the high price tag for one of these workstations; at a minimum, this option would cost $4,000. Also, this type of workstation may not provide the ability for hardware upgrades if desired in the future. Additionally, repurposing an existing Dell workstation has the ability to meet the requirements. This would be very cost effective because there would not be any cost for allocating the workstation. The only costs that may need to be invested into this option are the purchase of a new hard drive and possibly more RAM. For reference, a 1TB hard drive and 32GB of RAM would come in at around $300. The disadvantage of this option is that it would be a manual setup process to ensure everything is securely configured. Table 5.1 shows the hardware overview given to UNCW to help with their scorecard ranking.

Data Forensic Hardware Overview			
Workstation Options	**Description**	**Imager Options**	**Description**
Forensic Computers Inc. forensic workstation	• Cost ~$4,000 • Can uphold data integrity • Can support multiple storage devices • Has secure configuration • Slight possibility of network integration	Tableau TX1 Forensic Imager	• Cost ~$3,000 • Can uphold data integrity • Can support multiple storage devices • Has secure configuration • Has network integration ability
Repurposed Dell desktop	• Cost ~$300 (New HDD and additional RAM) • Can uphold data integrity • Can support multiple storage devices • Can be securely configured • Slight possibility of network integration		

Table 5.1 – Data Forensic Hardware Overview for UNCW[1]

[1] The Tableau TXI Forensic Imager was the only mobile imager option considered by UNCW. When researching for these devices, the Tableau TX1 Forensic Imager was the leading imager found. However, in application of this framework at other institutions, multiple mobile imagers may be researched and evaluated.

5.3 – Data Forensic Software

The software options include purchasing licensed software or using open-source software and/or freeware. AccessData's Forensic Toolkit (FTK), similar to the Forensic Computers Inc. forensic workstation, offers more than what UNCW Information Security actually needs of forensic software for an investigation based on history of previous incidents in the organization. The official cost of obtaining this software would be around $5,000 (Appendix A). This is not the most cost-effective option in comparison to using open-source software and freeware, such as Autopsy and FTK Imager. Yet, there are some drawbacks to using open-source software. Typically, there is not a company behind the software to offer official support and learning to use the software might take slightly longer since there may not be much documentation available. Fortunately, with Autopsy and FTK Imager, there is some documentation available. Table 5.2 shows the software overview given to UNCW to help with their scorecard ranking.

Data Forensic Software Overview	
AccessData's Forensic Toolkit (FTK)	• Cost ~$5,000 • Can uphold data integrity • Can support multiple OS • Can support multiple cases • Sufficient documentation to allow for ease of use
The Sleuth Kit's Autopsy & AccessData's FTK Imager	• Cost – Free • Can uphold data integrity • Can support multiple OS • Can support multiple cases • Some documentation to allow for ease of use

Table 5.2 – Data Forensic Software Overview for UNCW

5.4 – Data Forensic Third-party Company

The alternative option to setting up hardware and software for data forensic investigations at UNCW would be to use a third-party company. The use of a third-party company to complete investigations for UNCW Information Security could become very costly. Guardian Forensics & Data Recovery provides some standard rates on their website for different services for reference, ranging from hourly rates to per device to a lump sum cost (Appendix B). Using a company like this could end up being very expensive, and in addition, UNCW Information Security loses control over the investigation. However, one advantage would be knowing that the company is fully capable to properly handle forensic data to ensure integrity. Table 5.3 shows the third-party overview given to UNCW to help with their scorecard ranking.

Data Forensic Third-Party Overview	
Guardian Forensics	• Hourly rates from $200-250 • Flat rates, depending on service, from $175-2,500 • Can uphold data integrity • Can support multiple storage devices • Can support multiple OS • Can support multiple cases • Company will have secure configurations for investigations

Table 5.3 – Data Forensic Third-Party Overview for UNCW

5.5 – UNCW Scorecard

By considering all the stated information and using the overviews previously provided, the scores for the specified hardware, software and third-party company UNCW is considering can be found in Table 5.4. Some of the hardware and software criteria are weighted differently, using a range of 1 to 3, because they are of greater importance to UNCW. The Hardware Score and Software Score for each option is calculated by multiplying the criterion score by the criteria weight and then adding them across. For example, the Forensic Computers Inc. workstation and Tableau TX1 Forensic Imager option is calculated as (3*2) + (5*3) + (5*1) + (5*2) + (3*1) = 39.

Hardware	Cost-effective	Uphold data integrity	Multiple storage devices	Secure configuration	Secure network integration	Hardware Score
	Weight					
	2	3	1	2	1	
Forensic Computers Inc. workstation & Tableau TX1 Forensic Imager	3	5	5	5	3	39
Repurposed Dell workstation & Tableau TX1 Forensic Imager	5	5	5	4	3	41
Guardian Forensics (third-party) & Tableau TX1 Forensic Imager	3	5	4	5	1	36
Software	**Cost-effective**	**Uphold data integrity**	**Multiple OS**	**Multiple cases**	**Easy to use**	**Software Score**
	Weight					
	2	3	2	1	1	
AccessData FTK Licensed Software	2	5	5	5	4	38
Autopsy (open-source) & FTK Imager (freeware)	5	5	5	5	3	43
Guardian Forensics (third-party)	3	5	5	4	1	36

Table 5.4 – UNCW Scorecard

Table 5.5 includes the possible configurations and tallies their hardware/software scores by adding them together to provide the optimal solution for UNCW. For example, the Forensic

Computers Inc. workstation and Tableau TX1 Forensic Imager/AccessData FTK licensed software combination is calculated as 39 + 38 = 77

Configuration Total Scores				
		Hardware		
		Forensic Computer Inc. forensic workstation & Tableau TX1 Forensic Imager	Repurposed Dell workstation & Tableau TX1 Forensic Imager	Guardian Forensics (third-party) & Tableau TX1 Forensic Imager
Software	AccessData FTK licensed software	77	79	
	Autopsy (open-source) & FTK Imager (freeware)	82	84	
	Guardian Forensics (third-party)			72

Table 5.5 – UNCW Configuration Total Scores

5.6 – Optimal Hardware/Software Solution

With the knowledge stated in previous chapters that an organization may opt to weight some criteria differently depending on what is of most value and importance to them, UNCW Information Security decided to weight some criteria heavier than others due to the importance on those criteria to UNCW. With upholding data integrity being the most important criteria, obtaining cost-effective and securely configured hardware was slightly more important than the other criteria. This resulted in the Repurposed Dell workstation and Tableau TX1 Forensic Imager/Autopsy (open-source) and FTK Imager (freeware) being the highest scoring configuration to provide the optimal solution, 41 + 43 = 84.

After customizing the scorecard to fit their needs, UNCW was able to identify their optimal solution of repurposing a Dell workstation, with the addition of a Tableau TX1 Forensic Imager, and utilizing free Autopsy and FTK Imager software. The workstation will be securely

configured based on best practices that are pertinent from Center for Internet Security (CIS) Benchmarks for Windows 10 which will further ensure data integrity (*CIS Microsoft Windows 10 Enterprise (Release 1709) Benchmark*). The only expense necessary for the workstation is the purchase of a new 1TB hard drive which will cost around $50. There is currently 20GB of system memory installed which will be sufficient for this configuration. As previously stated, the Tableau TX1 Forensic Imager will allow for data preservation to be conducted out in the field to provide a secure environment and ensure data integrity. The Autopsy and FTK Imager software can maintain data integrity, are compatible with multiple operating system files types, can support multiple concurrent cases, and are simple to use.

The implementation of the framework at UNCW for new data forensic procedures for data preservation and extraction, along with the optimal hardware/software solution, was effective. UNCW was able to utilize the procedure criteria effectively to create the following standard operating procedures: Data Preservation for Investigation (Appendix C) and Data extraction for Investigation (Appendix D). A supporting document for recording chain of custody was also created (Appendix E).

UNCW repurposed a Dell workstation utilizing appropriate configurations based on CIS Benchmarks for Windows 10; see Appendix F for setup outline. Lastly, the FTK Imager and Autopsy software were installed easily and at no cost, while providing the exact features necessary for UNCW.

This implementation was proven successful when all parts were put into action during an investigation. All data was properly preserved and extracted, maintaining its integrity, to provide as evidence for the investigation.

CHAPTER 6: ASSESSMENT OF FRAMEWORK FROM CAPE FEAR COMMUNITY COLLEGE

The framework was presented to John Branner, Program Director of Healthcare Business Informatics and Business Analytics at Cape Fear Community College. Mr. Branner is also on the Advisory Board for the Center for Cyber Defense Education at UNCW. Branner was very impressed with the work developed in this project and was able to provide insightful thoughts and feedback on the data forensic framework, or as he liked to call it, the decision-making tool for a data forensic configuration.

What first struck Branner with the content of this project is that the procedure criteria and development of operating procedures seems to be more of a bonus segment that came as a result of this project and should not necessarily be considered part of the framework for identifying the optimal data forensic solution. This is because the scoring framework is solely focused on the hardware and software criteria. Branner suggested the possibility of carving out the procedure criteria from Table 2.1 and having it be its own standalone segment, so it does not get confused as being part of the scoring framework.

Secondly, Branner found the 5-point scale for scoring the hardware and software options to be slightly overwhelming and though that having a 3-point scale might be more suitable. The phrasing of terms used for the scale (Least Appropriate, …, Most Appropriate) was questioned; what would deem something as “appropriate”? An explanation that determining the level of appropriateness would be up to the organization using the tool provided clarity, however, it was suggested to possibly use a term that would provide clear definition on its own, perhaps the word “suitable”.

Thirdly, the question of how weight for the criteria is determined was asked. Currently, the default weight for all criteria in the scorecard is 1 and an organization can make criteria have a higher weight by assigning a higher number. For example, UNCW gave the following weights for hardware and software:

Hardware	Cost-effective	Uphold data integrity	Multiple storage devices	Secure configuration	Secure network integration
	Weight				
	2	3	1	2	1
Software	**Cost-effective**	**Uphold data integrity**	**Multiple OS**	**Multiple cases**	**Easy to use**
	Weight				
	2	3	2	1	1

Table 6.1 – UNCW Criteria Weights for Hardware and Software

These weights were merely given to weight the criteria that was most important to UNCW higher than others. Branner pointed out that this free-range is a flaw in evaluating. If an organization can just give any weighted number to a criterion, then they can manipulate the scorecard to give them a specific outcome instead of using the tool for its actual purpose. With this feedback in mind, the process of how to weight the hardware and software criteria was reconsidered. Ranking each criterion on a scale of 1 to 5, instead of everything being a default weight of 1, would force an organization to truly determine what is of most importance and least importance; 5 being most important and 1 least important. Upon application of this criteria weight ranking scale, it was successful in providing the same optimal solution for UNCW, see Table 6.2 and Table 6.3.

Hardware	Cost-effective	Uphold data integrity	Multiple storage devices	Secure configuration	Secure network integration	Hardware Score
	Weight					
	3	5	2	4	1	
Forensic Computers Inc. workstation & Tableau TX1 Forensic Imager	3	5	5	5	3	67
Repurposed Dell workstation & Tableau TX1 Forensic Imager	5	5	5	4	3	69
Guardian Forensics (third-party) & Tableau TX1 Forensic Imager	3	5	4	5	1	63
Software	**Cost-effective**	**Uphold data integrity**	**Multiple OS**	**Multiple cases**	**Easy to use**	**Software Score**
	Weight					
	3	5	4	2	1	
AccessData FTK Licensed Software	2	5	5	5	4	65
Autopsy (open-source) & FTK Imager (freeware)	5	5	5	5	3	73
Guardian Forensics (third-party)	3	5	5	4	1	63

Table 6.2 – Updated UNCW Scorecard

Configuration Total Scores			
	Hardware		
Software	Forensic Computer Inc. forensic workstation & Tableau TX1 Forensic Imager	Repurposed Dell workstation & Tableau TX1 Forensic Imager	Guardian Forensics (third-party) & Tableau TX1 Forensic Imager
AccessData FTK licensed software	132	134	
Autopsy (open-source) & FTK Imager (freeware)	140	142	
Guardian Forensics (third-party)			126

Table 6.3 – Updated UNCW Configuration Total Scores

Branner also suggested considering that the optimal solution not necessarily being highest scoring hardware and software configuration. Instead, an optimal solution can be selected by the organization if some configurations score within a specific range of each other. For example, if the two highest scoring configurations score within 3 points difference of each other, both configurations would be considered "optimal" and the organization can select which configuration they prefer. This suggestion does allow for more options to be available to an organization, but the benefit of having the highest scoring configuration be the optimal solution gives an organization an immediate decision without needing any further consideration.

Lastly, Branner recommended that when presenting this framework to an organization to use, provide them with a clear and simple introduction of the purpose of the framework and instructions on how to properly use the framework. Having a simple user guide or manual will take any guess-work out of how to use the framework. While CFCC did not implement the framework at this time, they could in the future.

CHAPTER 7: CONCLUSION

An organization's Information Security department, in a private corporation or a higher education institution, has great responsibility for the protection of information in the organization to ensure confidentiality, integrity, and availability. Data forensics is a segment that falls under that protection umbrella and an organization, including higher education institutions, should be properly equipped to handle incidents that require data forensic investigation; this includes having appropriate procedures, hardware, and software. The established criteria developed for evaluating procedures, hardware, and software in this project has been proven to be effective and successful. With the development of a scoring framework to determine the optimal data forensic

hardware/software solution, the decision-making process is streamlined by providing a straightforward way for an institution to find their optimal data forensics solution.

A higher education institution can successfully use this data forensic framework to find their optimal hardware/software solution by utilizing the guidelines and scorecard template provided in Appendix G. The guidelines provide information about the different hardware and software criteria to help an institution evaluate their options appropriately. The guidelines also provide instruction on how to weight the hardware and software criteria and then explains how to score the options. Based on what was successfully applied to UNCW and the recommendation from Mr. Branner at CFCC, there are two options an institution can choose from on how to weight the criteria. Option 1 is to give each criteria a weight ranging from 1 to 3 based on the level of importance with 1 being "Low", 2 "Medium" and 3 "High". Option 2 would be to rank the five criteria from 1 to 5 with 1 being the least important criteria and 5 the most important. The scoring process for the hardware and software options has remained on the 5-point scale instead of condensing to the 3-point scale as recommended by Mr. Branner. Using the 5-point scale gives an institution more options and flexibility with scoring when evaluations call for variations from a definitive yes or no answer.

REFERENCES

Barbara, John J. "Documenting Computer Forensic Procedures." *Forensic Magazine*, 10 Oct. 2007, https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures.

Carrier, Brian. *Autopsy*. http://www.sleuthkit.org/autopsy/.

Chain of Custody in Computer Forensics. InfoSec Resources, https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/.

CIS Microsoft Windows 10 Enterprise (Release 1709) Benchmark. 28 Aug. 2018, https://workbench.cisecurity.org/benchmarks/766.

Collection Guide. Duke Law. https://www.edrm.net/frameworks-and-standards/edrm-model/collection/.

Desktop Workstations - Workstations - Forensic Computers, Inc. https://www.forensiccomputers.com/workstations/towers.html.

Dunham, Ray. "Security Procedures & Your Overall Security Documentation Library." *Linford & Company LLP*, 14 Mar. 2018, https://linfordco.com/blog/security-procedures/.

E-Discovery Toolkit. Educause. Information Security Guide: Effective Practices and Solutions for Higher Education. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/ediscovery-toolkit.

EDRM Collection Standards. 16 Jan. 2014, https://www.edrm.net/frameworks-and-standards/edrm-model/edrm-stages-standards/edrm-collection-standards/.

EDRM Model. Duke Law. https://www.edrm.net/frameworks-and-standards/edrm-model/.

FTK – Digital Investigations. https://www.accessdata.com/assets/images/misc-content/FTK-6.3-WEB_.pdf.

FTK Imager 4.2.0. http://marketing.accessdata.com/ftkimager4.2.0.

Incident Management and Response. Educause. Information Security Guide: Effective Practices and Solutions for Higher Education. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/incident-management-and-response.

Preservation Guide. Duke Law. https://www.edrm.net/frameworks-and-standards/edrm-model/preservation/.

Prounis, Michael. "How Corporate Counsel Deal With E-Discovery." *Corporate Counsel Business Journal*, Oct. 2013, p. 35.

Quality Standards for Digital Forensics. 20 Nov. 2012, https://ignet.gov/content/quality-standards.

Security Operations. Educause. Information Security Guide: Effective Practices and Solutions for Higher Education. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-operations.

Tableau TX1 Forensic Imager - Forensic Computers, Inc. https://www.forensiccomputers.com/forensic-hardware/tableau/forensic-duplicators/tableau-tx1-forensic-imager.html.

The Compelling Case for Data Governance. Mar. 2015, https://library.educause.edu/~/media/files/library/2015/3/ewg1501-pdf.pdf.

Three Common Techniques for E-Discovery Preservation. Exterro. 2014. https://www.exterro.com/seomatic/seo-file-

link/aHR0cHM6Ly9nby5leHRlcnJvLmNvbS9sLzQzMzEyLzIwMTQtMTItMDQvNmYzZmsvNDMzMTIvNDY1MjgvV1AwMTZfVGhyZWVfQ29tbW9uX1RlY2huaXF1ZXNfZm9yX0VfRF9QcmVzZXJ2YXRpb24ucGRm/YWxs/aHR0cHM6Ly93d3cuZXh0ZXJnby5jb20vcmVzb3VyY2VzL2NvbW1vbi1lLWRpc2NvdmVyeS1wcmVzZXJ2YXRpb24tdGVjaG5pcXVlcy8=/0/WP016_Three_Common_Techniques_for_E_D_Preservation.pdf

Whitman, Michael E., and Herbert J. Mattford. *Management of Information Security*. Fourth, Cengage Learning, 2014.

Wolfe, Hank. "Setting up an Electronic Evidence Forensics Laboratory." *Computers & Security*, vol. 22, no. 8, Dec. 2003, pp. 670–72. *Crossref*, doi:10.1016/S0167-4048(03)00004-X.

APPENDICES

APPENDIX A – AccessData Quote

ACCESSDATA

Customer # [redacted]
Quote Number [redacted]
Expiration Date [redacted]
Created Date [redacted]

Approval Signature:_____

AccessData Group Inc.
588 West 400 South #350
Lindon, UT 84042 USA
Phone: 801-377-5410
Fax: 801-377-5426
www.accessdata.com
sales@accessdata.com

Bill To Name	[redacted]	Ship To Name	[redacted]
Bill to Company	University of North Carolina - Wilmington	Ship to Company	University of North Carolina - Wilmington
Bill To	601 South College Rd Wilmington, North Carolina 28403 US	Ship To	601 South College Rd Wilmington, North Carolina 28403 US

Product Code	Product	Quantity	List Price	Discount	Total Price
9901141	FTK Standalone - Perpetual License	1.00	USD 3,995.00	5.00%	USD 3,795.25
9901143	FTK Standalone - Perpetual License - 1 Year SMS	1.00	USD 1,119.00	5.00%	USD 1,063.05

Total List Price	5,114.00
Total Discount	USD 255.70
SubTotal	USD 4,858.30
Shipping and Handling	USD 7.00
Tax	USD 340.08
Final Amount	USD 5,205.38

Wire Transfer Information:
Wells Fargo Bank, N.A.
420 Montgomery Street
San Francisco, CA 94104
Routing #: [redacted]
Acct #: [redacted]
Swift Code: [redacted]

Any balance not paid within the terms stated will be subject to an 18% annual finance charge, at 1.5% per month.

Make checks payable to:
AccessData Group, Inc
Tax ID [redacted]

US Domestic REMIT TO:
AccessData Group, Inc
PO Box 413146
Salt Lake City, UT 84141-3146

ACCESSDATA SOFTWARE RETURN POLICY
AccessData offers a 30-day return policy on all software products.The following procedures apply to your return. 1. You must contact AccessData's Customer Support Team by telephone, fax or email within 30 days of the product ship date to notify them of your intent to return your product. 2. A 10% restocking fee (excluding taxes and shipping) will apply to all returns. 3. AccessData will issue you the appropriate refund upon receipt of the returned product(s). The original payment method will be used for the refund (i.e. credit card, check, etc). 4. The product must be returned unused to qualify for a refund, including all cables, manuals, software, dongles, and original packaging. 5. Your refund amount is calculated by taking the original purchase price (including any discounts) less the restocking fee. Refunds are not issued for shipping charges. 6. To initiate a return, the following contact information should be used: AccessData Group Inc., 588 West 400 South, Suite 350 Lindon, UT 84042 Phone: 801.377.5410, Fax: 801.377.5426, Email: sales@accessdata.com

Amounts are in US dollars

TRAINING CANCELLATION AND POLICIES

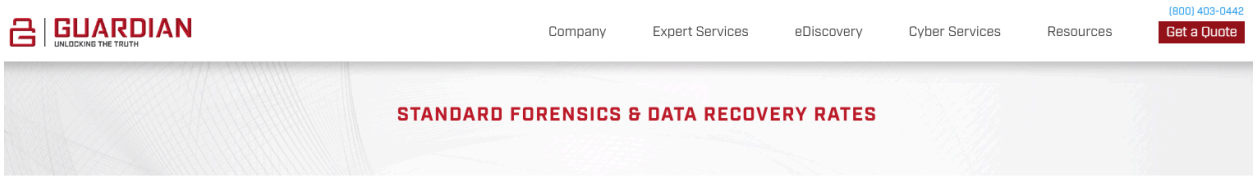
Training Credits are valid for one year from purchase date.

Cancellations made ten (10) or more business days PRIOR to a scheduled class can be rescheduled at no additional charge. Cancellations made less than ten (10) business days PRIOR to a scheduled class can be rescheduled for a 20% processing fee. Refund requests can be made less a 20% processing fee. If a student fails to attend a class as registered, they forfeit their purchase price in full. Students that do not attend at least eighty percent (80%) of course instruction time will not receive a Certificate of Completion.

Training Pass Holders failing to attend two (2) training events without proper cancellation notice will forfeit their Training Pass.

AccessData Group Inc., a Delaware Corp.

APPENDIX B – Guardian: Standard Forensics & Data Recovery Rates



STANDARD FORENSICS & DATA RECOVERY RATES

Forensics Hourly Rates

Civil / Corporate Forensics	$200.00 per hour
Criminal Forensics	$250.00 per hour
Minimum Initial Retainer, if required:	
Computers Examinations	$2,500.00
Cell / Mobile Devices	$1,500.00
Cloud / Email Forensics	$2,000.00

Forensic Imaging / Collection

Mobile Device – Delivered to Guardian	$350.00
Single Hard Drive – Delivered to Guardian	$499.00
On-Scene Imaging / Forensics	$250.00 per hour
Cloud & Email Forensics **(One-Time Technology Fee)**	$750.00

Expert Witness Services

Expert Testimony (Minimum 3 hour charge)	$250.00
Client Consultation / Research	$175.00

Data Recovery Rates

*** Evaluation Fee	$45.00
All Digital Devices (Smartphones, Computers, Tablets, USB, GPS Devices)	$95.00 per hour

Forensics Examination Triage Packages

Includes administration, forensic imaging, analysis, ongoing storage of a single evidence media delivered to Guardian.

Level 1 Triage Up to 1 hour of forensic examination, 1 month of ongoing evidence storage	$499.00 per device
Level 2 Triage Up to 8 hours of forensic examination, 3 months of ongoing evidence storage	$1,695.00 per device
Level 3 Triage Up to 16 hours of forensic examination, 6 months of ongoing evidence storage	$2,995.00 per device

Other Forensics Services

Computer Processing Time	$25.00 per hour
Travel Rate	$89.00 per hour
Ongoing Evidence Storage *(Up to 1TB for 12 Months)*	$300.00

APPENDIX C – SOP 001: Data Preservation for Investigations

DATA PRESERVATION FOR INVESTIGATION

Standard Operating Procedure #001

Defines the information necessary for data preservation during an investigation requiring data forensics. An investigation can be initiated from a request by an Approving Authority concerning issues such as but not limited to: legal hold, federal investigation, internal security investigation, internal audit investigation, Title IX investigation, HR investigation, or UPD investigation.

I. General Information

This procedure defines the necessary steps to properly preserve evidentiary data. Creating a forensic image will ensure that the data is unaltered once an investigation is initiated. Capturing the data in a forensic image will also maintain data integrity and allow for nonrepudiation.

II. Scope

This procedure is used to preserve specific evidentiary data and information on campus when an investigation is in process. This procedure cannot be used unless requested by an appropriate Approving Authority. Once request has been made by Approving Authority, OIS personnel can begin data preservation process.

III. Applicable Definitions

A. Data Preservation
   1. Capturing the data to ensure it is not altered to retain data integrity and protect against destruction of potential evidence.

B. OIS
   1. Office of Information Security

C. Approving Authority
   1. An internal office, or authoritative Federal or State agency, with appropriate jurisdiction requesting inquiry of data for an investigation.

D. Tableau TXI Forensic Imager
   1. Mobile imaging device that can be used out in the field or in a stationary location to securely capture data.

E. FTK Imager
   1. Disk imaging software that can be used to securely capture data.

F. Data forensics
   1. Encompasses identifying, preserving, recovering, analyzing, and presenting attributes of digital information.

IV. Procedure

A. Prerequisites
   1. Received a written or auditable request, preferably through email, from Approving Authority to preserve specific evidentiary data. An auditable request

will provide appropriate evidence as to why the data preservation procedure should be initiated.

B. Process

1. A witness or escort should be available for chain of custody as deemed appropriate to the sensitivity of the investigation.
2. Secure equipment where data may be stored
    a) Desktops, laptops, tablets, external storage devices, etc.
3. Document Chain of Custody using the form linked below in **Applicable Regulations and Guidelines**. A record of custody must be entered each time equipment or data is handled. Equipment/data is considered in custody if in one of the following states:
    a) In actual, physical possession
    b) In view after being in physical possession
    c) In physical possession and in locked safe or locked drawer to avoid tampering
    d) In a secured area, such as locked safe or locked office, restricted to only authorized personnel
4. Preserve data
    a) Create forensic image of drive(s) containing data
        (1) Use Tableau TXI Forensic Imager, if applicable
            (a) Retain hashes of drive(s) for data integrity purposes

        -OR-

        (2) Use FTK Imager software that is installed on the data forensic workstation
            (a) Retain hashes of drive(s) for data integrity purposes
    b) Create a duplicate of the forensic image to reserve for data integrity and nonrepudiation purposes
    c) Store forensic image, duplicate forensic image and hashes in separate locations. Options include:
        (1) Locked safe
        (2) Locked drawer
        (3) Locked office
    d) Retain forensic images until end of legal hold

V. Applicable Regulations and Guidelines

A. Chain of Custody Tracking Form
B. Incident Response Policy

VI. References to Other Applicable SOPs

A. SOP_002 DATA EXTRACTION FOR INVESTIGATION

VII. Responsibilities

Title	Responsibility
Office of Information Security	Process/Facilitation

VIII. Revisions

Date	Description
02/21/19	Applied new format
02/26/19	Revisions to procedure
03/04/19	Revisions to procedure
03/15/19	Revisions to procedure

APPENDIX D – SOP 002: Data Extraction for Investigations

DATA EXTRACTION FOR INVESTIGATION

Standard Operating Procedure #002

Defines the information necessary for data extraction during an investigation requiring data forensics. An investigation can be initiated from a request by an Approving Authority such as but not limited to: legal hold, federal investigation, internal security investigation, internal audit investigation, Title IX investigation, HR investigation, or UPD investigation.

VIII. General Information

This procedure defines the necessary steps to properly extract evidentiary data. Using a forensic image to extract evidentiary data will ensure that the original data continues to remain unaltered, which is necessary to maintain data integrity and allow for nonrepudiation during an investigation.

IX. Scope

This procedure is used to extract specific evidentiary data and information on campus when an investigation is in process. This procedure cannot be used unless requested by an appropriate Approving Authority. Once request has been made by Approving Authority, OIS personnel can begin data extraction process.

X. Applicable Definitions

A. Data extraction
   1. From a forensic image, gathering the appropriate and relevant data for an investigation.

B. OIS
   1. Office of Information Security

C. Approving Authority
   1. An internal office, or authoritative Federal or State agency, with appropriate jurisdiction requesting inquiry of data for an investigation.

D. Autopsy
   1. Data forensic software used to analyze data.

E. Examiner
   1. Name of Office of Information Security (OIS) Staff creating Autopsy case for data extraction.

F. Ingest Modules
   1. Various components that can be used to analyze the data.

XI. Procedure

A. Prerequisites
   1. Received a written or auditable request, preferably through email, from Approving Authority to extract specific evidentiary data. An auditable request

will provide appropriate evidence as to why the data extraction procedure should be initiated.

2. Completed SOP_001 DATA PRESERVATION FOR INVESTIGATION

B. Process

1. A witness or escort should be available for chain of custody as deemed appropriate to the sensitivity of the investigation.

2. Document Chain of Custody using the form linked below in **Applicable Regulations and Guidelines**. A record of custody must be entered each time equipment or data is handled. Equipment/data is considered in custody if in one of the following states:

    a) In actual, physical possession

    b) In view after being in physical possession

    c) In physical possession and in locked safe or locked drawer to avoid tampering

    d) In a secured area, such as locked safe or locked office, restricted to only authorized personnel

3. Extract data

    a) Create Autopsy case using forensic copy of preserved data

        (1) Give Case Name

        (2) Choose Base Directory for the location to save the case

        (3) Assign Case Number

        (4) Assign Examiner

        (5) Select **Disk Image** as Data Source Type

        (6) Browse to forensic image file

        (7) Select the appropriate Ingest Modules

    b) Search for and extract specified evidentiary data requested by Approving Authority.

4. Provide forensic copy of extracted data to Approval Authority.

5. Store Autopsy case file and forensic copy of extracted data in separate locations. Options include:

    a) Locked computer

    b) Locked safe

    c) Locked drawer

    d) Locked office

    e) Retain Autopsy case and forensic copy until end of legal hold.

XII. Applicable Regulations and Guidelines

A. Chain of Custody Tracking Form

B. Incident Response Policy

XIII. References to Other Applicable SOPs

A. SOP_001 DATA PRESERVATION FOR INVESTIGATION

XIV. Responsibilities

Title	Responsibility
Office of Information Security	Process/Facilitation

IX. Revisions

Date	Description
02/21/19	Applied new format
02/26/19	Revisions to procedure
03/04/19	Revisions to procedure
03/15/19	Revisions to procedure

APPENDIX E – Chain of Custody Tracking Form

Office of Information Security

CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Date/Time: _____

Approving Authority (Name/Office) _____

Name of Employee: _____

Location of Evidence: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody			
Item #	**Date/ Time**	**Released by** (Signature & Office)	**Comments/ Location**
		Received by (Signature & Office)	
Item #	**Date/ Time**	**Released by** (Signature & Office)	**Comments/ Location**
		Received by (Signature & Office)	

Item #	Date/ Time	Released by (Signature & Office)	Comments/ Location
		Received by (Signature & Office)	
Item #	**Date/ Time**	**Released by** (Signature & Office)	**Comments/ Location**
		Received by (Signature & Office)	
Item #	**Date/ Time**	**Released by** (Signature & Office)	**Comments/ Location**
		Received by (Signature & Office)	
Item #	**Date/ Time**	**Released by** (Signature & Office)	**Comments/ Location**
		Received by (Signature & Office)	
Item #	**Date/ Time**	**Released by** (Signature & Office)	**Comments/ Location**
		Received by (Signature & Office)	

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to case number: _____ is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Employee ☐ Destroy

Name & Office of Authorization:

_____

Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian (Name & Office _____ in my presence on (Date) _____ at (Time)_____.

Name & Office of Witness to destruction: _____

Signature: _____Date: _____

Release to Employee

Item(s) #: _____ on this document was/were released by Evidence Custodian (Name & Office _____ to (Name)_____

Location: _____

I certify that I am the lawful owner of the above item(s).

Signature: _____Date: _____

This Chain of Custody Tracking Form is to be retained as a permanent record by the Office of Information Security.

APPENDIX F – Data Forensic Workstation Configuration Outline

Setup:

- Windows 10
    - Full disk encryption

- Off domain

- No Internet connection

- Accounts
    - Standard Account for general use
    - Administrator Account for elevated use

- Forensic Software
    - The Sleuth Kit Autopsy
    - FTK Imager

- Change in settings
    - Disable Autorun/Autoplay
    - Disable search indexing
    - Disable anti-virus
        - This is to ensure anti-virus does not quarantine or delete any data

APPENDIX G – Data Forensic Scoring Guidelines and Template

The purpose of this scorecard is to help identify the optimal data forensic hardware and software solution for your organization.

The hardware, software, and third-party options in the navy column are currently identified with generic placeholders. You should fill out these placeholders with the specific options your organization is considering. Example: Licensed Software → AccessData FTK

Hardware Criteria

- Cost effective: This will be dependent on the budget of your organization as to what will be cost effective for your department.
- Uphold data integrity: The hardware should be evaluated on its ability to keep data consistent and unchanged. Any alteration to the data will obstruct the validity of the data.
- Multiple storage devices: The hardware should be evaluated on its compatibility with multiple types of storage devices.
- Secure configuration: The hardware should be evaluated on its system configuration to ensure that there are specific security settings in-place to prevent any changes that could alter the data under investigation.
- Secure network integration: The hardware should be evaluated on its network integration ability that will keep the data from being vulnerable to alteration if accessed over the network.

Software Criteria

- Cost effective: This will be dependent on the budget of your organization as to what will be cost effective for your department.
- Uphold data integrity: The software should be evaluated on its ability to keep data consistent and unchanged. Any alteration to the data will obstruct the validity of the data.
- Multiple OS: The software should be evaluated on its compatibility with multiple operating systems.
- Multiple cases: The software should be evaluated on its ability to support multiple investigation cases.
- Easy to use: The documentation of the software should be evaluated to determine the sufficiency of provided instruction on how to use the software. This will help assess how easy the software will be for your staff.

How to Weight Criteria

There are two options your organization can choose from to weight the hardware and software criteria based on preference.

1. Each criterion can be given a weight ranging from 1 to 3 based on how important a specific criterion is to your organization.
    a. 1 = Low
    b. 2 = Medium
    c. 3 = High

2. The criterion can be ranked from 1 to 5 with 1 being the least important and 5 the most important.

How to Score Options

For each hardware and software option, you will score the corresponding criteria on a 5-point scale.

- 1 Point = Not Applicable
- 2 Points = Least Appropriate
- 3 Points = Slightly Appropriate
- 4 Points = Moderately Appropriate
- 5 Points = Most Appropriate

To tally the hardware or software score for each option, multiply each given score by its criteria weight then add them all together.

Example: S = Score, CW = Criteria Weight
(S*CW) + (S*CW) + (S*CW) + (S*CW) + (S*CW) = Hardware/Software Score

Finding Optimal Solution

Once the hardware and software option scores have been tallied, apply the scores in the appropriate combinations in the second table to get a total score for each configuration. The configuration with the highest total score is the optimal data forensic solution for your organization.

Hardware	Cost-effective	Uphold data integrity	Multiple storage devices	Secure configuration	Secure network integration	Hardware Score
	Weight					
	-	-	-	-	-	
Preconfigured Workstation & Mobile Imager						
Repurposed Workstation & Mobile Imager						
Third-party Company & Mobile Imager						

Software	Cost-effective	Uphold data integrity	Multiple OS	Multiple cases	Easy to use	Software Score
	Weight					
	-	-	-	-	-	
Licensed Software						
Open-source & Freeware						
Third-party Company						

Configuration Total Scores

Software \ Hardware	Preconfigured Forensic Workstation & Mobile Imager	Repurposed Standard Workstation & Mobile Imager	Third-party & Mobile Imager
Licensed Software			
Open-source & Freeware			
Third-party			