Computer Crimes Case Simulation and Design Model

“Kitty” Exploitation and Illicit Drug Activities

Submitted by Maritza Stephanie Jeremias

University of Central Oklahoma

W. Roger Webb Forensic Science Institute

Dr. Joe C. Jackson College of Graduate Studies

University of Central Oklahoma

Edmond, Oklahoma

11/30/2018

This thesis is submitted to

The Jackson College of Graduate Studies

University of Central Oklahoma

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Forensic Science

Computer Crimes Case Simulation and Design Model

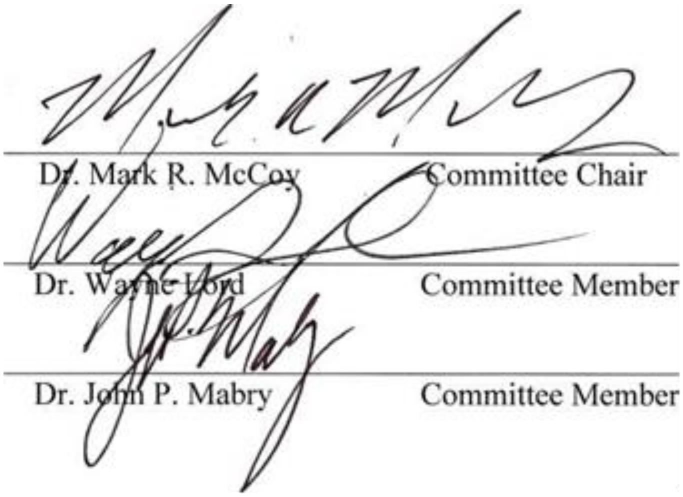
“Kitty” Exploitation and Illicit Drug Activities

Submitted by Maritza Stephanie Jeremias

University of Central Oklahoma

Graduate Thesis Approved by the W. Roger Webb Forensic Science Institute

11/30/2018



Dr. Mark R. McCoy	Committee Chair
Dr. Wayne Lord	Committee Member
Dr. John P. Mabry	Committee Member

Acknowledgments

I would like to thank my graduate thesis advisor and committee chair, Dr. Mark R. McCoy, of the University of Central Oklahoma, Forensic Science Institute. Dr. McCoy provided me with the support and resources necessary to complete this project. I must also thank my thesis committee members, Dr. Wayne Lord and Dr. John P. Mabry, for their insight and dedication. I greatly appreciate the time and dedication put forth by the entire Forensic Science Institute faculty and staff members at the University of Central Oklahoma.

I am grateful to my employers for not only encouraging me to pursue and complete my Master of Science in Forensic Science, but also for allowing me to continue to work full-time through a flexible schedule around my classes and coursework.

Additionally, I am appreciative of my friends and classmates for taking the time out of their busy lives to review the multiple revisions of my thesis paper.

Lastly, I wish to express my gratitude to my family. To my mom, Maria, thank you for always having faith in me and doing everything within your power to ensure my brothers and I achieve our goals in life. To my younger brothers, Adam and Eddie, I am very proud of how much the both of you have accomplished this far and I cannot wait to see all that you achieve in the future.

Abstract

The overall purpose of this graduate project is to provide digital forensics instructors at the University of Central Oklahoma (UCO) with a manually generated computer crimes case simulation that offers students a replicated real-world experience of what it is like being a practicing digital forensic examiner. This simulation offers digital forensic students an opportunity to apply their forensic knowledge and skills in a realistic environment. Secondarily, this project sought to develop a rudimentary computer crimes simulation design model. The case simulation provides scenario/simulation-based learning to future digital forensic students at UCO. The computer crimes simulation design model presents general steps and considerations that should be taken when generating similar digital forensic simulations. The generated simulation portrays typical "kitty" exploitation and illicit drug activities and consists of two computer crimes case scenarios, two sets of investigative notes, two search warrant affidavits, eight crime scene processing forms, a solution report with associated PowerPoint presentation for the instructors, the digital evidence, a bootable clone of the evidence, and a disk image of the evidence.

Keywords: computer crime, digital crime, cyber crime, computer forensics, digital forensics, forensic triage, crime scene processing, digital evidence, disk image, disk clone, forensic analysis, anti-computer, counter-computer, anti-forensics, counter-forensics, forensic training, forensic simulations, forensic scenario, forensic case study

Table of Contents

Introduction

The complexity of safety and privacy laws combined with high employer expectations of graduating students necessitate the use of hands-on learning tools. Various departments of higher education across the nation are adapting their curricula to accommodate these needs. There are two primary reasons for pursuing higher education: the pursuit of education for its own sake, and preparation for a career. On the most fundamental level, education is the process of facilitating the acquisition of knowledge, skills, values, beliefs, and habits. One of the methods for demonstrating and evaluating the actual comprehension of knowledge is through the practical application of the knowledge towards a task.

As society has advanced technologically, the formal educational process has become more reliant upon intangible, abstract concepts and less on practical, real-world, hands-on training and application. Much of this is due historically higher rates of illiteracy. With higher rates of literacy, teaching abstract concepts is more feasible. Furthermore, in some environments active, real-world training is even prohibited due to privacy, safety, or legal concerns. Despite this hands-on training offers a plethora of advantages including faster learning, instant productivity from the student, and instant feedback which allows immediate correction of erroneous action.

Hands-on training typically comes in two different forms: on-the-job training or through simulation-based learning. On-the-job training consumes trainer time and organization assets for the span of the training period, so it can often be rushed or carelessly taught. On the other hand, simulation-based learning can have expensive up-front costs in terms of time and money spent while planning and creating the simulation. In academic environments, on-the-job training may not be a viable training option, and thus simulation-based training may be the only hands-on learning method available to students.

Simulation-based training, like most learning styles, is not a standalone tool, but rather is used in conjunction with in-class instruction, guides, quizzes, etc. Simulations can be used when data is difficult to obtain or limited, and for experimentation in a low-risk setting. Regardless of whether it is a case study or a complex flight or medical simulator, all the student's mistakes in a simulation are valuable learning experiences. The students can make mistakes, learn from them, and apply the lessons learned before ever working in a real-world environment. The outcome is not damaging to the organization, its equipment, or its personnel, and the process itself acts as a mechanism to reduce the student's anxiety. Simulations create a safe, enjoyable, and engaging learning environment where failures and experimentation are possible. Simulations are also effective for improving knowledge retention because the student can practice responses and actions rather than just thinking in theoretical terms.

Simulation-based Training in the Forensic Science Education

Simulation-based training is not new to the field of forensic science, and is regularly used in a variety of ways across the forensic disciplines. Some examples of forensic simulations include students role-playing in scenarios involving crime scene processing, chain of custody, witness interviews, evidence analysis, and subject matter expert testimonies. In the case of digital forensics, students are often asked to seize and image digital evidence, forensically analyze the evidence, and present the findings in a simulated courtroom. While many simulations can be crafted with a simple and straightforward approach, several types of simulations have their own set of challenges that must be overcome during their creation. As previously stated, real-world training can be limited in some settings due to privacy, safety, or legal concerns, but the same can be said about stored real-world, user-generated data. Unfortunately, simulations involving digital forensic evidence analysis present their own challenges, in particular, with regards to obtaining, analyzing, and sharing real-life data.

Obtaining Digital Forensic Data for Research, Education, and Training Purposes

The planning and execution of a simulation is just as important as the simulation itself. The simulation must be thoughtfully and deliberately developed and presented in a way that minimizes any potential confusion and clearly demonstrates how the forensic knowledge is applicable to the real-world. The usefulness of many simulations, including digital forensic simulations, is dependent on how closely the simulations replicate the real-world experiences and events that actual practitioners observe in the field. Acceptable digital forensic analysis simulations can be difficult to manufacture due to numerous barriers that presently limit the usability of real-world, user-generated data.

In terms of digital forensics, user-generated datasets offer a wealth of research and educational knowledge about user activities on digital devices. The drawback with user-generated data is that because it is not created in a controlled or supervised environment, it almost certainly will contain personally identifiable information (PII), copyrighted material and software, and possibly even incriminating evidence of illegal activities. Those who handle PII must abide by information privacy laws or data protection laws that prohibit the disclosure or misuse of PII of individuals unless specifically authorized by law or by consent of the individual. In instances where a dataset only contains the PII of a handful of people, obtaining their consent may not be too much of a challenge, but when hundreds or thousands of individuals are involved, it may not be practical to use the dataset if consent is needed. Additionally, when using user-generated or real-world datasets, copyright infringement concerns arise when distributing and obtaining entire disk images containing an operating system, other software, or media. Finally, a large user-generated dataset may contain evidence of a crime, such as child pornography, and the consequences of further distributing the dataset could be disastrous for all the parties involved as well as for any future court proceedings involving the evidence.

Problem Statement

According to the University of Central Oklahoma's Forensic Science Institute (FSI) mission statement, the institute "seeks to provide educational, research, and professional training opportunities for both undergraduate and graduate students." One of the many goals of the institute is to foster students' application of foundational forensic knowledge and skills to the continuum that consists of crime scenes through courtrooms. The FSI is a comprehensive training organization in all aspects of evidence collection, preservation, analysis, reporting, and testimony. However, while many of the major forensic areas taught at the FSI currently include simulation-based training, the digital forensics program is currently without a single, long-term computer crimes simulation that cohesively links all aspects of digital forensic collection and analysis together. Many digital forensic students rely heavily on practical exercises and scenarios in order to retain, comprehend, and apply the knowledge being taught by the instructors. Although the FSI's digital forensic program has been extremely successful in developing competent, highly sought-after forensic practitioners, the program has not taken full advantage of the many benefits of hands-on, scenario-based learning.

Project Statement and Objectives

In response to the stated problem, this graduate project seeks to provide digital forensics instructors at the University of Central Oklahoma (UCO) with a manually generated computer crimes case simulation that offers students a replicated real-world experience of what it is like being a practicing digital forensic examiner. This simulation will offer digital forensic students an opportunity to apply their forensic knowledge and skills in a realistic environment. Secondarily, this project seeks to develop a rudimentary computer crimes simulation design model. The case simulation will provide scenario/simulation-based learning to future digital forensic students at UCO. A single, well-developed, long-term case simulation will connect disjointed topics more effectively and will provide a low-cost, low-risk learning environment. In this environment, students can acquire practical skills, reduce mistake driven anxiety, foster learning from those mistakes, and apply their forensic knowledge in a way that does not cause damage to the organization, equipment, or personnel. The computer crimes simulation design model will present general steps and considerations that should be taken when generating simulations which mimic current real-world experiences of practicing digital forensic examiners.

Background

The University of Central Oklahoma's Forensic Science Institute (FSI) is a world-class Institute dedicated to quality forensic science education, training, and research for professionals and students. The FSI is a comprehensive training and research organization in all aspects of evidence collection, preservation, analysis, reporting, and testimony. The Institute promotes leadership, character, and public service throughout all training events. The FSI is devoted to academic excellence, through a unique multidisciplinary program, that provides outstanding research, educational, and professional training opportunities for practicing professionals and both undergraduate and graduate students.

The University of Central Oklahoma offers a FEPAC accredited B.S. Forensic Science – Digital Forensics degree in which students must satisfy all requirements in either the

Management of Information Systems or Computer Science undergraduate programs at UCO and, concurrently complete requirements for a degree in Forensic Science. UCO is currently only one of two schools in the country that have an FEPAC accredited digital forensic program. The university also offers an M.S. Forensic Science degree in which students must complete 36 hours of graduate level work including required core courses, electives, and 6 hours of research in their major area. Although many of the major forensic areas taught at the FSI currently include simulation-based training, the digital forensics program does not have a case simulation to tie all aspects of digital forensic collection and analysis together.

In order to construct a simulation that mimics the current real-world experiences of practicing digital forensic examiners, there must be at least a minimal understanding of the digital artifacts that are typically present and identified in computer crimes evidence. Outlined below are the non-exclusive, general categories of common computer user activities and software that generate and leave traces of artifacts on computer forensic evidence.

Commonly Performed Computer User Activities

The general purpose of digital devices is to store, process, and retrieve data to simplify and improve people's lives. Digital devices and computers are used in a wide variety of ways by their users. The most common computer user activities include:

- Emailing via webmail service or email client
- Internet surfing via web browsers and search engines
- Communicating via text messaging or instant messaging applications
- Viewing and posting to online social media
- Streaming videos (movies, shows, etc.)

- Streaming audio (music, radio, podcasts, etc.)
- Creating, designing, or editing media content
- Playing video games
- Shopping (ordering goods/services, booking reservations, online consumer services, etc.)
- Using financial services (banking, paying bills, investing, cryptocurrency, etc.)
- Uploading and downloading software and media content
- Using spreadsheet or word processing software
- Organizing, cleaning, and customizing PC
- Interacting with household equipment via internet

Commonly Utilized Software

In order to function, digital devices and computers need software, or code, to provide them instructions. Software can be divided into two categories: system software and application software. The most common software types include:

System software.

System software is software that is necessary to operate and maintain the basic functions of a computer system and provides a platform for running application software. The most common types of system software include:

- Operating System
- Utility Software
    - Anti-virus software
    - Data backup and recovery software

  - Disk cleaners
  - Disk defragmenters
  - Disk formatters
  - Disk/data compressors
  - Registry cleaners
- Device Drivers
  - Keyboard drivers
  - Mouse drivers
  - Printer drivers
- Firmware

Application software (End-user software).

Application software or end-user software is software that is designed to perform a group of specific, coordinated functions, tasks, or activities for the benefit of the user. The most common types of application software include:

- Business and education productivity software
  - Accounting software
  - Calendar and scheduling software
  - Office software suites
  - Presentation software
  - Spreadsheet software
  - Word processing software
- Graphics and multimedia software

  - Image design and editing software
  - Video and audio recording and editing software
- Home/personal software
  - Multimedia viewing software
  - Video gaming software
- Communications software
  - Emailing software
  - FTP/P2P file sharing software
  - Instant messaging software
  - Search engines
  - Social media platforms
  - Videoconferencing software
  - Web browsers

Basic Anti-Computer Forensics Techniques & Tools

Anti-computer forensics tools and techniques are used as countermeasures to the forensic analysis of digital evidence. Whether intentional or not, computer users routinely employ some of these anti-computer forensic techniques and tools. The average computer user utilizes fairly basic anti-computer forensic techniques and tools developed by advanced users. Anti-computer forensic techniques and tools typically fall under one of three categories: data hiding, artifact wiping, and trail obfuscation.

Data hiding.

Data hiding tools and techniques involve the process of making data difficult to find while also retrievable for future use. The most common types of data hiding methods include:

- Encryption
- Hiding columns and spreadsheets in Excel workbooks
- Hiding files and folders by changing their attributes
- Hiding files and folders in less visibly accessible areas of the disk
- Hiding text in Word documents
- Steganography
- Traditional ciphers

Artifact wiping.

Artifact wiping tools and techniques involve the process of eliminating particular files or entire file systems. Depending on the method, data can be permanently deleted if it is overwritten by new data. The most common types of artifact wiping methods include:

- Deleting cache and browser history
- Deleting chat logs and databases produced by instant messengers
- Deleting documents and transitory files
- Deleting SQLite records
- Formatting the disk (quick or full format)
- Securely deleting data by overwriting
- Using disk cleaning tools
- Using registry cleaning tools

Trail obfuscation.

Trail obfuscation tools and techniques serve the purpose of confusing and diverting the forensic examination process. The most common types of trail obfuscation methods include:

- Altering file extensions
- Altering file signatures
- Altering/overwriting metadata/timestamps
- Disabling logging (preventing data creation)
- Email spoofing
- Using a proxy server
- Using a VPN (Virtual Private Network)
- Using misleading folder and file names
- Using multiple email addresses
- Using TOR (The Onion Router)
- Using Virtual Machines (VM)

Definition of Terms

- Anti-computer forensics – tools or techniques used as countermeasures to the forensic analysis of digital evidence.
- Anti-forensics/counter-forensics – tools or techniques used as countermeasures to the forensic analysis of evidence.
- Data corpora – a collection of digital data, often used for research, scholarship, and teaching.
- Device drivers – software designed to instruct operating systems and other software on how to communicate with a piece of hardware or a device.

- Digital forensics – a branch of forensic science encompassing the recovery and investigation of information found in all devices capable of storing digital data.
- Disk clone – a bootable, uncompressed, bit for bit copy of a disk volume or disk drive.
- Disk image – a compressed, bit for bit copy of a disk volume or disk drive.
- Disk or data cleaning, deleting, erasing, scrubbing, or wiping tools – software for deleting data from digital storage devices. The software can either mark the space the data occupies as usable or it can completely destroy the data by overwriting it with new data.
- Email client – desktop software application specifically designed to enable configuring one or more email addresses to compose, store, manage, send, and receive emails from that email address(es) through the desktop interface.
- Emailing – a method of exchanging digital messages via a network.
- FEPAC - Forensic Science Education Programs Accreditation Commission
- Firmware – software permanently etched into the read-only memory of device hardware that provides instruction on how that device should operate.
- Freeware – software that is offered for use at no monetary cost. While freeware is free to use, it may be copyrighted and include a license agreement prohibiting the modification and re-distribution of the software without the author’s permission.
- Instant messaging – a method of exchanging near real-time digital messages.
- Internet/web browser – software application for accessing the World Wide Web.
- Operating System (OS) – software that manages the computer's resources, such as the central processing unit, memory, disk drives, and printers, establishes a user interface, and executes and provides services for application software.

- Problem-Based Scenario – a type of scenario in which the learner is expected to integrate theoretical and practical knowledge to investigate a problem. Decision-making, logical reasoning, and critical analyses are applied to identify a problem, identify the cause of a problem, and develop recommendations.
- Programming software (software development tool) – software used by programmers to create, debug, modify, or translate high-level programming language source code to machine language code to create other software. Programming software is often regarded as a sub-category of system software, but sometimes it is listed as its own category.
- Search engine – software for searching information on the World Wide Web.
- Skill-Based Scenario – a type of scenario in which the learner is expected to demonstrate previously acquired skills and knowledge. The knowledge is applied within clearly-defined steps or procedures.
- Social media – websites and applications that serve as forms of electronic communication through which users join online communities to create and share content.
- Utility software – software designed to support computer infrastructure through maintenance, monitoring, analysis, configuration, and optimization.

Related Work

Lang et al. (Lang, Bashir, Campbell, & DeStefano, 2014) describe their efforts to develop an undergraduate digital forensics certificate program at the University of Illinois at Urbana-Champaign. At the time of writing their paper, they had developed the curriculum for their introductory course and taught a pilot class. Lang et al. outline the lessons learned from the pilot class, their evaluation methodology, a summary of student feedback, as well as the curriculum revisions following the pilot course. Student feedback included that the topics did not flow well and suggested using a single case study to connect the lectures from the beginning to the end of the semester. In an effort to improve the flow of the course material and to demonstrate the inter-connectivity of the topics with one another, Lang et al. planned to incorporate a fictitious case study that would run for the entire semester. Additionally, Lang et al. planned to change the topic order by leading the course with the legal justice system and law section lectures before all technical material. This provides students with an understanding of the legal motivation and processes of digital forensics before they learn how it is practiced.

Woods et al. (Woods, et al., 2011) presented their work on the design, implementation, use, and distribution of their "M57-Patents" scenario and corpora. The four objectives that guided the development of their corpora was that it includes answer keys, realistic wear and depth, realistic background data, and that it can be freely shared and redistributed. Woods et al. had to ensure that their corpora did not include copyright material, personally identifiable information, or illegal material to make it publicly available.

Grajeda et al. (Grajeda, Breitinger, & Baggili, 2017) compiled an extensive list of publicly available corpora and datasets by analyzing 715 peer-reviewed digital forensic research articles spanning from 2010 to 2015. As part of their research, Grajeda et al. also documented whether the corpora were real-world or synthetic, the types of corpora that exist, and whether the corpora was publicly released. Their findings indicated that 56.4% of the corpora they reviewed was experimentally generated, 36.7% was real-world generated, and only 29% (102/351) was made publicly available to other researchers.

Scalon et al. (Scanlon, Du, & Lillis, 2017) introduce EviPlant as an alternative to the time-consuming manual creation, manipulation, storage, and distribution of digital forensic images to classes of students. EviPlant works by allowing a user to boot a baseline disk image in a virtual machine, emulating criminal behavior, and then using the EviPlant diffing tool to compare the baseline image to the modified image. An evidence package that includes all the newly created and modified files and other digital artifacts, along with their associate metadata, is produced and distributed to students, who then use the EviPlant injection tool to “plant” this evidence on their clones of the baseline images. In order to demonstrate the viability of the proposed system, Scalon et al. conducted preliminary testing of the diffing and injection tools and were able to identify and recover the planted evidence in the resultant generated image.

Methodology

Experimental Design and Materials

In order to minimize potential confusion and to clearly demonstrate the applicability of forensic knowledge taught, the simulation must be thoughtfully and deliberately developed and presented. The usefulness of this particular simulation is dependent on how accurately it portrays the current real-world experiences of practicing digital forensic examiners. Before even beginning the creation of the digital evidence, foundational questions about the simulation’s design should be addressed. After those questions have been answered, the next step is to design the computer crimes case scenario and any supporting documents that are needed to put the scenario into context. Finally, the hardware, software, and the computer user activities should be methodologically selected to achieve the desired outcome. Once all these steps are completed, the actual evidence creation can begin. This portion of the paper will outline the steps taken for each of the stated processes.

Simulation design framework.

During the initial planning of the simulation, several design questions should be asked and answered. Presented here is a sample of some general questions that should be addressed prior to the creation of the simulation:

- What is the purpose of the simulation?
- What are the objectives of the simulation?
- Who are the intended participants that will work through the simulation?
- What is the intended level of difficulty of the simulation?
- Will the simulation be freely distributed?
- Have considerations been made about the inclusion of copyrighted material and software?
- Are there any presently recognized challenges or issues that will need to be addressed prior to or during the simulation?
- How will the participants document their role in the simulation?
- How will the participants document and present their key findings?
- What is the most efficient way to provide the solutions at the end of the simulation?
- Does any of the simulation material need to be returned or protected for the simulation to maintain its usefulness for future classes?

Regarding the generated simulation discussed in this paper, the included scenarios and supporting documents can be distributed freely. However, because the generated evidence most likely contains incidentally captured copyrighted material and licensed software, the case evidence is not intended for distribution outside of the University of Central Oklahoma. Since one of the simulated crimes is child exploitation, precautions were taken to ensure that illegal contraband was not actually observed or included in the simulation. Furthermore, obscene photos were represented by innocuous photos of everyday items or animals and the child exploitation crime type was renamed “kitty exploitation.” The case simulation includes the following items:

- Scenario 1a - Execution of Search Warrant
- Scenario 1b - Forensic Analysis of Seized Evidence
- Investigation Case Notes Summary #1
- Investigation Case Notes Summary #2
- Search Warrant Affidavit - Kitty Exploitation
- Search Warrant Affidavit - Drug Possession & Distribution
- Crime Scene Entry & Exit Log
- Crime Scene Processing Logistical Preparation Checklist
- Crime Scene Preliminary Survey and Narrative Description
- Crime Scene Photography Log
- Crime Scene Sketch - Landscape Orientation
- Crime Scene Sketch - Portrait Orientation
- Crime Scene Evidence Log
- Original Digital Evidence Hard Drive
- Bootable Clone of Digital Evidence Hard Drive
- Disk image of Digital Evidence Hard Drive
- Solution Report with associated PowerPoint

Simulation participants should document their crime scene processing actions in the provided forms and their key forensic analysis findings in a forensic report. In addition, students can provide their final conclusions as investigative leads via a word document. An instructor should be available throughout the simulation to provide guidance and to clear up any confusion for the students. Instructors should always ensure that while the original evidence is being copied, it remain in a read-only mode. Optionally, the included bootable hard drive clone can be used in combination with the solution report as a means to illustrate the evidence location and the anti-forensic techniques that were implemented in the simulation. The method by which the simulation solutions are provided will beat the instructor’s discretion. Finally, to maintain the long-term integrity of the simulation, copies of the case solution report and PowerPoint presentation should not be provided to students.

Scenario design.

Once the simulation design framework has been addressed, the next step is to design the scenario. The scenario in this project is both skill-based and problem-based. The scenario must consist of a framework and an environment where the students can apply their previously acquired forensic skills and knowledge, as well as integrate theoretical and practical knowledge towards the investigation of a problem. The students should apply decision-making, logical reasoning, and critical analysis to identify a problem, its cause, and develop recommendations. A list of design considerations is provided below:

- Craft an engaging and interactive story with good characters and valuable lessons.
- Choose how the scenario will begin and think about when and how it will end.
- Determine what aspects of the investigation must be abbreviated for the purposes of the simulation (e.g. time compression or time extension).
- Decide what information will be provided to the participants.
- Plan the scenario progression by anticipating the participant’s potential conclusions, decisions, and actions.

- Decide if there will be a single scenario or multiple branching scenarios.
- Decide which props, equipment, media, videos, photos, and help will be available to the participants.

The simulation in this project takes place in two different settings over the course of multiple days. The first scenario begins in a digital forensic lab and moves into the crime scene. The second scene takes place exclusively in the digital forensic lab. The students will be provided with a service request at the beginning of each scenario. The service request outlines the general tasks that they must perform during the simulation. The presence of two scenarios allows the simulation to be spread over the course of multiple days. The first scenario involves a request for assistance with the execution of a search warrant and the second scenario begins with an assistance request for the forensic analysis of seized digital evidence. Props may be used during the simulation, but that decision will be left to the instructor.

Hardware selection.

During the hardware selection process, a list should be compiled of all the resources and materials that will be needed to generate the simulation. The list can be modified later, but a well thought-out list can greatly assist with the planning and funding request. Once the list is compiled, the noted resources can be separated into two categories based on whether they are currently available or if they will need to be obtained. For this simulation, all the basic, necessary resources were already present and available at the Forensic Science Institute. The graduate project was assigned a dedicated Forensic Recovery of Evidence Device (FRED) upon which the digital evidence could be both created and later analyzed. The FRED had the typical peripherals that would be found with a computer, including a mouse and keyboard. The FRED was not associated with a printer. A small-storage flash drive was used to transfer files to the FRED. The digital evidence, evidence clone, and the disk image were each stored on 160 GB Serial ATA Samsung HD161HJ hard disk drives. Lastly, a network dongle with the Forensic Toolkit (FTK) licensing was used to gain access to the software that was used to perform the analysis of the digital evidence. UCO digital forensic students are trained to use FTK, and for that reason it was selected as the analysis tool.

Software selection.

During the software selection process, open source research should be leveraged to identify the most suitable software for the simulation. When designing a forensic simulation, it is important to select software appropriate for the time period in question. For this simulation, the selected time period is present day, October 2018. Reasonable attempts should be made to avoid software expected to become obsolete in the near future. Wherever possible, freeware software should be used. The remainder of this section describes some of the general strategies utilized to select this simulation's operating system, web browsers, email service providers, instant messengers, search engines, social media platforms, and additional software.

Operating system selection.

Microsoft's Windows operating system was selected for this simulation because of its continual worldwide popularity. According to the web analytics services, Net Applications and StatCounter, in August 2018, the Windows OS held between 83-88% of the worldwide desktop operating system market shares. The next highest OS was the Mac OS at around 9-13% of the market shares (Net Applications, 2018) (StatCounter, 2018). The large drop-off between the first and second place standings cemented the Windows OS as the best operating system choice for this particular project simulation. The operating system Windows 10, the latest version of Windows OS, was selected as the best fit for this computer crimes simulation.

Microsoft Windows 10 operating system.

Windows 10 is a personal computer operating system developed and released by Microsoft. The first version of the Windows 10 operating system was issued for public beta testing in October 2014, prior to its consumer release on July 29, 2015 (Myerson, Windows 10 Free Upgrade Available in 190 Countries Today, 2015). During the first year of its release, upgrade licenses for Windows 10 could be obtained for free for devices with a genuine license for an eligible edition of Windows 7 or 8.1. Windows 10 introduced a new default web browser, Microsoft Edge, and also incorporated Microsoft's intelligent personal assistant, Cortana.

Windows 10 is serviced differently from previous releases of Windows, because once a Windows device is upgraded to Windows 10, Microsoft will continue to keep it current for the supported lifetime of the device (Myerson, The next generation of Windows: Windows 10, 2015). The Windows lifecycle fact sheet states that Windows 10 will be supported for five years in "mainstream" support until October 13, 2020, and then another five years in "extended" support until October 14, 2025. Although traditionally Microsoft has offered both security and bug fixes in mainstream but only security updates in extended, Windows 10 updates can include new features, fixes (security and/or non-security), or a combination of both (Microsoft). But unlike previous versions of Windows, Windows Update does not allow the selective installation of updates, and instead downloads and installs updates automatically.

Windows 10 is available in four main editions for personal computer devices: Home, Pro, Enterprise, and Education. Windows 10 Home and Pro editions are sold at retail and as pre-loaded software on new computers, while Windows 10 Enterprise and Education are only available through volume licensing. Each edition of Windows 10 includes all the capabilities and features of the edition below it, and adds additional features oriented towards their market segments. The Windows 10 Home edition is targeted at home users, while the Windows 10 Pro edition is aimed at small businesses. The Windows 10 Pro edition adds additional networking and security features and the ability to join a domain. The Windows 10 Enterprise and Windows 10 Education editions contain additional features aimed towards business environments (Prophet, 2015). The University of Central Oklahoma presently has volume licensing of the Windows 10 Enterprise edition, and thus this particular edition was used for the simulation.

Web browser selection.

Google Chrome, Mozilla Firefox, Microsoft Internet Explorer 11, and Microsoft Edge were selected for the case simulation due to their continual popularity and long-term success. According to Net Applications and StatCounter, in August 2018, the worldwide desktop browser market shares were approximately 65-68% for Chrome, 10-11% for Firefox, 7-11% for Internet Explorer and 4% for Edge (Net Applications, 2018)(StatCounter, 2018). In an effort to include a web browser with anti-computer forensic properties, the TOR browser was also added to the simulated environment. Multiple web browsers were chosen in order to expose the students to the various artifacts associated with each browser.

Search engine selection.

Google, Bing, and Yahoo were selected as the search engines for the case simulation due to their standing as the three top English-language search engine websites used worldwide. According to the web analytics website Alexa.com, as of August 2018, Google.com has ranked

#1 in their list of top 500 sites on the web for several years (Alexa Internet, 2018). In August 2018, Net Applications and StatCounter showed that Google had between 71-91% of the worldwide search engine market share, Bing had approximately 3%, and Yahoo had roughly 2% of the market shares (Net Applications, 2018)(StatCounter, 2018). In an effort to include a search engine with anti-computer forensic properties, DuckDuckGo was also added to the simulated environment. Multiple search engines were chosen in order to acquaint the students to different artifacts.

Email selection.

Due to the vast and ever-growing number of email service providers, several providers may need to be selected for inclusion into the scenario. Several email accounts were created with various providers including Outlook, Gmail, GMX, Hushmail, Mail.com, Protonmail, Tutanota, Rambler, and Elude. There were also plans to create Yahoo, AOL, and QQ email accounts, but the account creation and verification for those services proved to be a challenging process without a mobile device to verify the account.

Instant messenger selection.

As the popularity of smartphones increases, the use of desktop instant messaging applications decreases. In this simulation, Facebook messenger, Skype, and Google hangouts were selected as the instant messengers due to their ongoing popularity and cross platform capabilities.

Online social media platform selection.

The social media platforms that were used in this simulation were narrowed down from a much larger list of the most popular platforms in the United States and across the world.

Alexa.com provided a good starting point for identifying the most commonly used social media platforms (Alexa Internet, 2018). Social media accounts were created on ASKfm, Blogger (BlogSpot), Facebook, Flickr, Instagram, Last.fm, LinkedIn, LiveJournal, Mix (StumbleUpon), Pinterest, Steam, Tagged, Tumblr, Twitch.tv, Twitter, and YouTube.

Selection of additional software.

Since software plays such a large and important part of online and offline computer activities, creating a narrow list of just a handful of software can feel like a daunting task. For this project, Download.cnet.com was used to develop a list of some of the most frequently downloaded software. Download.cnet.com is an internet download directory website that provides more than 150,000 free-to-try legal software downloads. This site allows software filtering by categories and platforms and also permits software sorting by total downloads and most popular software (CNET, 2018). Additional software directory websites including BrotherSoft, FileHippo, MajorGeeks, Soft32, Softpedia, Tucows, were also reviewed to ensure that the compiled list included the essential software (BrotherSoft, 2018) (FileHippo, 2018) (MajorGeeks, 2018) (Soft32, 2018) (Softpedia, 2018) (Tucows, 2018) (ZDNet, 2018). The system software chosen for the simulation included Avast Antivirus, CCleaner, iObit Advanced Systemcare, iObit Drive Booster, iObit Malware Fighter, iObit Smart Defrag, iObit Uninstaller, and Malwarebytes. Additional installed application software included 7zip, Adblockerplus, Adobe Reader, FrostWire, iCloud, iTunes, PhotoScape, Spotify, TeamSpeak, and the Microsoft Office suite of products which include Word, Excel, PowerPoint, Access, and Outlook.

Selection of computer user activities.

During the selection process of the most suitable computer user activities, the simulation design framework and the designed case scenario should be reviewed to ensure that the computer user activities are in line with both. For this particular simulation, the generated digital evidence needed to reinforce fundamental digital forensic knowledge and provide students the opportunity to roleplay as a practicing digital forensic examiner. The evidence should assist with discussions of various topics including the types of digital crimes, the scope of legal processes, digital forensic tools, digital forensic analysis, and anti-forensic techniques.

The user activities incorporated into this simulation were selected due to their ease of execution and reproducibility. Some operational challenges that arose midway through the project were beyond the scope of this thesis project, including the acquisition of mobile devices to assist in the creation of email and social media accounts. The simulation was modified so that these operational challenges were not a factor. The major computer user activities that were incorporated into the simulation environment are as follows:

Data creation by:

- bookmarking favorite webpages
- communicating via instant messaging applications
- downloading and uploading software and media content
- emailing via webmail service and email clients
- internet surfing via web browsers and search engines
- organizing, cleaning, and customizing file system
- streaming audio and video
- using spreadsheet and word processing software
- viewing and posting to online social media platforms

Data hiding by:

- encrypting files
- encrypting emails
- hiding columns and spreadsheets in Excel workbooks
- hiding files and folders by changing their attributes
- hiding text in Word documents
- 7z steganography

Artifact wiping by:

- deleting documents and transitory files
- securely deleting data
- using disk cleaning tools

Trail obfuscation by:

- altering file extensions
- altering file signatures
- using misleading folder and file names
- using multiple email addresses
- using TOR (The Onion Router)

Browsing activities.

To replicate internet browsing, the simulation requires a list of terms, phrases, or websites that will be looked up via search engines. Rather than creating a list from scratch, a simple search was conducted for “popular google search terms”. Numerous websites were returned with already compiled lists. Mondovo.com has a keyword research tool that generates lists of the top Google searches. Mondovo had several different keyword lists posted online, but for the purpose of this project the “Most Searched Words on Google” and “Most Asked Questions on Google” lists were the most appropriate (Mondovo, 2018). Each of the lists was composed of 1000 keywords or phrases covering all types of topics. The 2000 phrases were combined into a single spreadsheet, categorized into groups (e.g. finances, food, grammar, health, math, science, technology, etc.), and then filtered down to around 600 phrases. All the obscene, sexual, or questionable search terms were removed along with any names of individuals. During the creation of the digital evidence, this list was used to conduct extraneous web searches in between the fabricated criminal activity.

Experiment Implementation

Creating the evidence.

Once the experimental design is formulated, the hard drives should be forensically sterilized, so they do not contain any data. FTK Imager was used to confirm that the hard drive did not have any data. After formatting the drive and installing the operating system, a password protected windows account was created under the name of the criminal suspect of the simulation. Microsoft Office was installed and additional windows user accounts were created. A password protected user account was created for the suspect’s spouse and another account was created under the name of “Other guest.” Over the course of three weeks, data was written to the hard drive. The next three sections in this paper briefly summarize the computer activities conducted by the suspect, the suspect’s spouse, and the suspect’s best friend on the computer of interest.

These summaries should not be divulged to the students until after the simulation has concluded, given that as forensic examiners they would not be privy to this personal information.

Computer activities conducted by the suspect.

As part of the simulation, Sylvester Cheshire, the suspect, has recently lost his job and is showing signs of stress and frustration. In an effort to occupy his time, Sylvester purchases a new computer. He receives the computer and creates three windows user accounts, one account for his wife Alice, one for his best friend Tom, and one for himself. Sylvester installs various programs, links several of his email addresses to his outlook desktop client, and transfers a folder from his old computer to his new one via a flash drive. Each time he logs into his windows account, he streams music, checks his emails, does casual internet browsing via search engines, posts and browses social media, and bookmarks webpages of interest to him.

As time passes, Sylvester eventually accesses the folders and files he transferred from his old computer. Stored within this folder is his collection of (legal) pornography as well as evidence of his involvement in illicit drug crime activities. Sylvester adds (legal) pornography viewing to his daily routine and begins reaching out to his old drug dealing contacts. As Sylvester reintroduces himself to the drug life, he also starts to view and download “kitty” porn. Eventually, viewing isn’t enough for him and he reaches out to a kitten via Facebook. Sylvester befriends the kitten and plans a meeting with her, but his plans are derailed when her parents find out and stop the meeting. Although annoyed, Sylvester conducts online searches for ways to fine tune his approaches and reaches out to another kitten via social media. They begin communicating via instant messaging. Sylvester befriends the kitten and is able to convince her to swap nude photos with him. Eventually, he arranges a meeting with the kitten, but no additional information is available to determine whether he successfully met with her.

In order to simulate the suspect’s activities, several things had to occur. The suspect’s email addresses and social media accounts had to be created prior to him accessing them on his new computer. The folder and files from his old computer also had to be created before he received his new computer. A routine had to be established and important elements of that routine had to be logged. The suspect’s criminal activity also had to be intermingled among his typical everyday activities. All the activities listed in the “Selection of computer user activities” section of this paper were performed on the suspect’s computer, but will not be outlined further in this paper as that would reveal the simulation solutions.

Computer activities conducted by the suspect’s wife

As part of the simulation, Alice Cheshire, Sylvester’s wife, occasionally uses Sylvester’s computer. Sylvester bought a new computer and created a windows user account for his wife. Alice is not technologically savvy and only logs into the computer to check her emails and to use Facebook. She logs into the computer so sparingly that she struggles to remember her password and as a result has numerous failed login attempts. Eventually, Alice completely forgets her password and her husband allows her to quickly check her emails and Facebook on his account. On her user account, Alice has googled, “How to know if husband is cheating?” and “How to divorce husband?” In order to simulate the wife’s activities, only her email and Facebook were accessed and multiple failed login attempts were always performed on her account prior to the successful login.

Computer activities conducted by the suspect’s friend.

As part of the simulation, Tom Garfield, Sylvester’s best friend, has previously used Sylvester’s computer. Tom is a gamer and has only accessed the computer on two occasions to look at gaming websites. On October 17, Tom logged into a windows user account called, “Other guest” and visited epicgames.com and gamestop.com. On October 29, Sylvester left his windows account unlocked and unattended, and without asking, Tom visited battle.net, blizzard.com, epicgames.com, minecraft.net, and unrealengine.com. Sylvester caught his friend on his computer and made him log out and log back in under the “Other guest” account. In order to simulate the friend’s activities, his search history was almost exclusively of gaming websites.

Analyzing the evidence.

Once the digital evidence is written to the hard drive, a bootable clone of the evidence can be created to allow the instructor to boot up the operating system and see the desktop just as the suspect saw it. After the creation of a cloned disk, FTK Imager was used to generate a disk image of the evidence hard drive and to confirm the integrity of the data by comparing the hash values. The disk image was added to the Forensic Toolkit (FTK) where the NTFS filesystem was parsed, processed, and indexed for subsequent analysis.

The image was searched and any identified incriminating or derogatory files were bookmarked in FTK. The bookmarked evidence was divided up into the four primary categories: drug evidence, kitty exploitation evidence, internet/chat history evidence, and other evidence. A report of the bookmarked evidence was generated and included with the solution report. In addition, the SAM.dat (Security Account Manager), SECURITY.dat, SOFTWARE.dat, SYSTEM.dat, and each of the NTUSER.dat registry databases were reviewed for more evidence. Registry reports were generated and included with the solution report.

Results

The computer crimes simulation design model proposed in this paper led to the creation of a computer crimes case simulation consisting of two computer crimes case scenarios, two sets of investigative notes, two search warrant affidavits, eight crime scene processing forms, and a solution report with associated PowerPoint presentation for the instructors. Simulated digital evidence was also produced, including a bootable clone of the evidence, and a disk image of the evidence.

Computer Crimes Case Scenarios

The generated simulation contains two computer crimes case scenarios. The first scenario begins with a request for assistance with the execution of a search warrant. The second scenario begins with a request for assistance with the forensic analysis of seized digital evidence.

In the first scenario, a law enforcement investigator with an Oklahoma state agency requests the assistance of UCO Digital Forensic Examiners (students) with the execution of a search warrant. The examiners are provided with a copy of the search warrant affidavit, investigation case notes summary #1, and necessary administrative forms. The examiners are also reminded that it is university policy that UCO Digital Forensic Examiners must utilize the FBI’s “12 Steps in Crime Scene Investigations” methodology. This methodology is to be followed while preparing for searches, documenting crime scenes, documenting and maintaining the chain of custody of the evidence, and throughout the execution of the search and seizure of evidence. The examiners are told that the storage device may be previewed on-site to assist with interviews or to identify additional evidence and leads, at the discretion of the lead investigator. Following the execution of the search warrant, the investigator decides that on-site forensic analysis of the evidence would take far too long. The investigator will maintain custody of the storage device until it is time to identify the data that falls within the scope of the warrant. The examiners are told that the evidence will remain in the agency's evidence vault until it is ready for imaging and analysis. The examiners are also informed that during the course of the search, they were able to locate the digital evidence, associated peripherals, and an attached sticky note with what appears to be passwords (see Appendix A).

In the second scenario, the same investigator has returned to request the assistance of UCO Digital Forensic Examiners with the subsequent search and forensic analysis of the seized digital evidence. Additionally, the examiners are now provided with the original digital evidence as well as investigation case notes summary #2. The examiners are now expected to take custody of the evidence, image the storage device, analyze the image for data that is within the scope of the warrant affidavit, create a forensic report documenting their findings, provide any newly generated leads to the detective, and finally to release the digital evidence back to the detective. The examiners are instructed that if they come across evidence of a crime that is not identified by the warrant, they should cease the examination of that particular file and obtain a second warrant (see Appendix B).

Scenario Supporting Documentation

Investigative Notes.

The generated simulation contains two sets of investigation case notes. The first case notes describe the detective's investigative work as well as his knowledge of the case prior to the search. The notes serve to establish probable cause for the search warrant and to provide the students with additional content that can be searched for during the evidence analysis. The second set of investigation case notes includes a transcript of the suspect interview that was conducted by the detective. During this interview the suspect acknowledges using the digital device, but also states that others have used it as well.

Search Warrant Affidavits.

The simulation also contains two search warrants affidavits. The first affidavit establishes probable cause for a warrant to search the suspect's premise and seize any evidence of "kitty" exploitation. The second affidavit establishes probable cause for a warrant to search the suspect's computer and seize any evidence of drug possession and distribution.

Crime Scene Processing Forms.

The simulation includes eight different crime scene processing forms. It includes the Crime Scene Entry/Exit Log that should be maintained by the instructor, as well as seven additional forms to be provided to the students to document their crime scene processing activities. The eight crime scene processing forms are:

1. Crime Scene Entry/Exit Log (see Appendix C)
2. Crime Scene Processing Preparation Checklist (see Appendix D)
3. Crime Scene Preliminary Survey and Narrative Description (see Appendix E)
4. Crime Scene Photography Log (see Appendix F)
5. Crime Scene Sketch (Portrait Orientation) Form (see Appendix G)
6. Crime Scene Sketch (Landscape Orientation) Form (see Appendix H)
7. Crime Scene Evidence Log (see Appendix I)
8. Crime Scene Chain of Custody Log (see Appendix J)

Solution Report with associated PowerPoint presentation.

The simulation's solution report outlines the minimal digital evidence that students should find while conducting the evidence analysis. The solution packet also includes additional information about the suspect, his wife, his friend, his associates, and his computer activities. This additional information will be useful to the instructor if the students locate evidence that is not listed in the solution report. The PowerPoint presentation provides click-by-click instructions on locating the digital evidence on the subject's computer.

Digital Evidence

Lastly, the simulation comes with the original digital evidence, a bootable clone of the evidence, and a disk image of the evidence.

Conclusion

This project sought to generate a computer crimes case simulation that offers students a replicated real-world experience of what it is like being a practicing digital forensic examiner. The proposed computer crimes simulation design model led to the creation of a computer crimes case simulation and associated digital evidence. A pilot of the simulation will be needed to truly test the efficacy of the simulation design model. Nevertheless, the generated simulation/scenarios, associated paperwork, and digital evidence provide an additional mechanism to aid in the discussion of digital forensic topics. These topics include the different types of digital crimes, the types of digital evidence, the scope of legal processes, the FBI's 12 Steps in Crime Scene Investigations, the chain of custody of evidence, digital forensic tools, digital forensic analysis, anti-forensic techniques, digital forensic reports, and subject matter expert testimonies in court.

Graduate Project Limitations

This project, like any project, is limited in design and scope. The first and most observable limitation was chronological data span. In the real-world, a hard drive may contain several years' worth of data created by various computer activities. This project had to generate many different types of activity data within a period of around a month. Additionally, some operational challenges that arose midway through the project were beyond the scope of this thesis project, including the acquisition of mobile devices to assist in the creation of email and social media accounts. Due to time constraints, the simulation was modified so that these operational challenges were not a factor. For example, the simulation originally intended to include Yahoo, AOL, and QQ email accounts. In order to create accounts, those services require verification via a mobile phone. In an effort to avoid delaying the simulation any further, the decision was made to continue without those accounts.

The second limitation, copyright infringement, was recognized in the early phase of the project. Due to the nature of the internet, it would be extremely difficult to closely replicate real-world digital evidence without incidentally capturing copyrighted material. In some cases, the copyrighted material is intentionally added. In the case of the generated scenario, Windows 10 and Microsoft Office are two examples of copyrighted material.

The third recognized limitations are the security measures utilized by email and social media service providers to detect and inactivate fake accounts. On at least two occasions, an account was created, used to contact the simulation's suspect, and inactivated within a few days by the service provider. To circumvent this, new accounts had to be created to replace the previous accounts that were shut down.

A fourth limitation is that the simulation does not provide across-the-board representation of all digital devices, software, crime types, or computer user activities. The presented simulation illustrates a “kitty” exploitation and drug-related case with evidence stored on a hard drive with an NTFS file system and Microsoft Windows 10 operating system. If any of those variables were changed, the procedures and results would vary.

The final major limitation is that the evidence analysis was conducted using only FTK. All tools have their weaknesses and strengths. FTK may not be financially feasible for everyone and does not include every feature necessary to conduct a thorough analysis of all digital artifacts. FTK has a wide range of features for digital artifact analysis, but there exist competing tools designed specifically for the analysis of particular artifact types. For example, there are specialized tools that are better at parsing and analyzing internet browsing activity, Skype messaging activity, and SQLite databases.

Significance of Findings

As a result of this project, future digital forensic students at the University of Central Oklahoma have a computer crimes case simulation that affords them the opportunity to roleplay as a practicing digital forensic examiner. UCO students now possess a low-cost, low-risk environment in which they can acquire practical skills, reduce mistake driven anxiety, foster learning from those mistakes, and apply their forensic knowledge in a way that does not cause damage to the organization, equipment, or personnel. Furthermore, a computer crimes simulation model has been proposed and partially tested through the creation of the simulation discussed in this paper. Even though the proposed rudimentary computer crimes simulation model has not been fully evaluated, the model can nevertheless assist others with the design and implementation of their prospective computer crimes simulation.

Suggestions for Future Research

Should a pilot of the simulation prove successful, more simulations may be developed using the design model provided in this paper. Furthermore, the generated simulation only portrayed “kitty” exploitation and illicit drug criminal activities. It may be beneficial for students to work simulations encompassing the other cybercrime types. Since time was a limiting factor for the generated simulation, additional research may be needed on how to create a simulation covering a longer period of time. Future research can also be conducted to redesign or re-purpose the design model for other devices such as mobile phones. Subsequent research and analysis of the generated simulation evidence may be possible through the use of analysis tools specializing in internet browsing activity, Skype messaging activity, or SQLite databases.

References

Alexa Internet. (2018, August). *The top 500 sites on the web*. Retrieved August 2018, from https://www.alexa.com/topsites/category/Computers/Internet/Searching/Search_Engines

Alexa Internet. (2018, August). *The top social networking sites on the web*. Retrieved August 2018, from http://www.alexa.com/topsites/category/Computers/Internet/On_the_Web/Online_Communities/Social_Networking

BrotherSoft. (2018, August). *Freeware Software*. Retrieved August 2018, from http://www.brothersoft.com/windows/

CNET. (2018, August). *Freeware Software*. Retrieved August 2018, from https://download.cnet.com/most-popular/windows/

FileHippo. (2018, August). *Freeware Software*. Retrieved August 2018, from https://filehippo.com/

Grajeda, C., Breitinger, F., & Baggili, I. (2017). Availability of datasets for digital forensics – And what is missing. *Digital Investigation. Proceedings of the 17th annual DFRWS USA* (pp. S94-S105). Austin, Texas: Elsevier. doi:https://doi.org/10.1016/j.diin.2017.06.004

Lang, A., Bashir, M., Campbell, R., & DeStefano, L. (2014, August). Developing a new digital forensics curriculum. *Digital Investigation*, S76-S84. doi:https://doi.org/10.1016/j.diin.2014.05.008

MajorGeeks. (2018, August). *Freeware Software*. Retrieved August 2018, from https://www.majorgeeks.com/

Microsoft. (n.d.). *Windows lifecycle fact sheet*. Retrieved August 2018, from https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

Mondovo. (2018, August). *Top Searched Keywords: Lists Of The Most Popular Google Search Terms Across Categories*. Retrieved August 2018, from https://www.mondovo.com/keywords/

Myerson, T. (2015, January 21). *The next generation of Windows: Windows 10*. Retrieved August 2018, from https://blogs.windows.com/windowsexperience/2015/01/21/the-next-generation-of-windows-windows-10/#5gy6lEre4lpuXg3i.97

Myerson, T. (2015, July 28). *Windows 10 Free Upgrade Available in 190 Countries Today*. Retrieved August 2018, from https://blogs.windows.com/windowsexperience/2015/07/28/windows-10-free-upgrade-available-in-190-countries-today/#RYVt4ybEVR5I6Idc.97

Net Applications. (2018, August). *NetMarketShare Report - Desktop Browser Market Share.* Retrieved August 2018, from https://www.netmarketshare.com/browser-market-share.aspx

Net Applications. (2018, August). *NetMarketShare Report - Search Engine Market Share*. Retrieved August 2018, from https://www.netmarketshare.com/search-engine-market-share.aspx

Net Applications. (2018, August). *NetMarketShare Report - Worldwide Desktop Operating System Market Share*. Retrieved August 2018, from https://www.netmarketshare.com/operating-system-market-share.aspx

Prophet, T. (2015, May 13). *Introducing Windows 10 Editions*. Retrieved August 2018, from https://blogs.windows.com/windowsexperience/2015/05/13/introducing-windows-10-editions/#LAO1lDt2txHopD17.97

Scanlon, M., Du, X., & Lillis, D. (2017). EviPlant: An efficient digital forensic challege creation, manipulation, and distribution solution. *Digital Investigation. Proceedings of the 4th annual DFRWS Europe* (pp. S29-S36). Europe: Elsevier. doi:https://doi.org/10.1016/j.diin.2017.01.010

Soft32. (2018, August). *Freeware Software*. Retrieved August 2018, from https://www.soft32.com/

Softpedia. (2018, August). *Freeware Software*. Retrieved August 2018, from https://win.softpedia.com/

StatCounter. (2018, August). *StatCounter Global Stats - Desktop Browser Market Share United States Of America.* Retrieved August 2018, from http://gs.statcounter.com/browser-market-share/desktop/worldwide/#monthly-201808-201808-bar

StatCounter. (2018, August). *StatCounter Global Stats - Search Engine Market Share United States Of America*. Retrieved August 2018, from http://gs.statcounter.com/search-engine-market-share#monthly-201808-201808-bar

StatCounter. (2018, August). *StatCounter Global Stats - Worldwide Desktop Operating System Market Share*. Retrieved August 2018, from http://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-201808-201808-bar

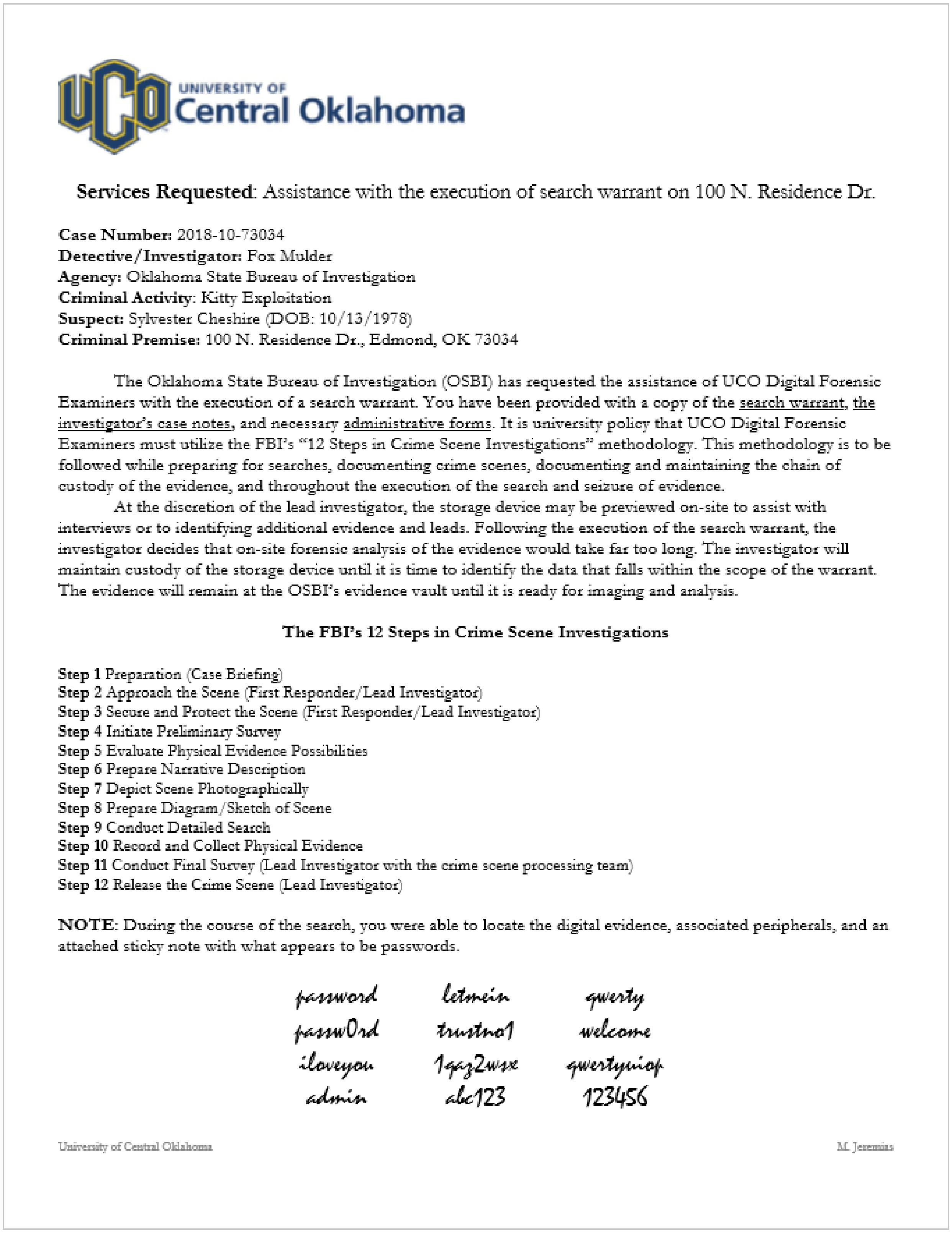
Tucows. (2018, August). *Freeware Software*. Retrieved August 2018, from http://www.tucows.com/list_detail.html?id=9

Woods, K., Lee, C., Garfinkel, S., Dittrich, D., Russel, A., & Kearton, K. (2011). Creating realistic corpora for forensic and security education. *ADFSL Conference on Digital Forensics, Security and Law* (pp. 123–134). Richmond, Virginia: Elsevier.

ZDNet. (2018, August). *Freeware Software*. Retrieved August 2018, from https://downloads.zdnet.com/

Appendices

Appendix A: Sample Scenario 1a - Execution of Search Warrant



UNIVERSITY OF Central Oklahoma

Services Requested: Assistance with the execution of search warrant on 100 N. Residence Dr.

Case Number: 2018-10-73034
Detective/Investigator: Fox Mulder
Agency: Oklahoma State Bureau of Investigation
Criminal Activity: Kitty Exploitation
Suspect: Sylvester Cheshire (DOB: 10/13/1978)
Criminal Premise: 100 N. Residence Dr., Edmond, OK 73034

The Oklahoma State Bureau of Investigation (OSBI) has requested the assistance of UCO Digital Forensic Examiners with the execution of a search warrant. You have been provided with a copy of the search warrant, the investigator's case notes, and necessary administrative forms. It is university policy that UCO Digital Forensic Examiners must utilize the FBI's "12 Steps in Crime Scene Investigations" methodology. This methodology is to be followed while preparing for searches, documenting crime scenes, documenting and maintaining the chain of custody of the evidence, and throughout the execution of the search and seizure of evidence.

At the discretion of the lead investigator, the storage device may be previewed on-site to assist with interviews or to identifying additional evidence and leads. Following the execution of the search warrant, the investigator decides that on-site forensic analysis of the evidence would take far too long. The investigator will maintain custody of the storage device until it is time to identify the data that falls within the scope of the warrant. The evidence will remain at the OSBI's evidence vault until it is ready for imaging and analysis.

The FBI's 12 Steps in Crime Scene Investigations

Step 1 Preparation (Case Briefing)
Step 2 Approach the Scene (First Responder/Lead Investigator)
Step 3 Secure and Protect the Scene (First Responder/Lead Investigator)
Step 4 Initiate Preliminary Survey
Step 5 Evaluate Physical Evidence Possibilities
Step 6 Prepare Narrative Description
Step 7 Depict Scene Photographically
Step 8 Prepare Diagram/Sketch of Scene
Step 9 Conduct Detailed Search
Step 10 Record and Collect Physical Evidence
Step 11 Conduct Final Survey (Lead Investigator with the crime scene processing team)
Step 12 Release the Crime Scene (Lead Investigator)

NOTE: During the course of the search, you were able to locate the digital evidence, associated peripherals, and an attached sticky note with what appears to be passwords.

password
passw0rd
iloveyou
admin

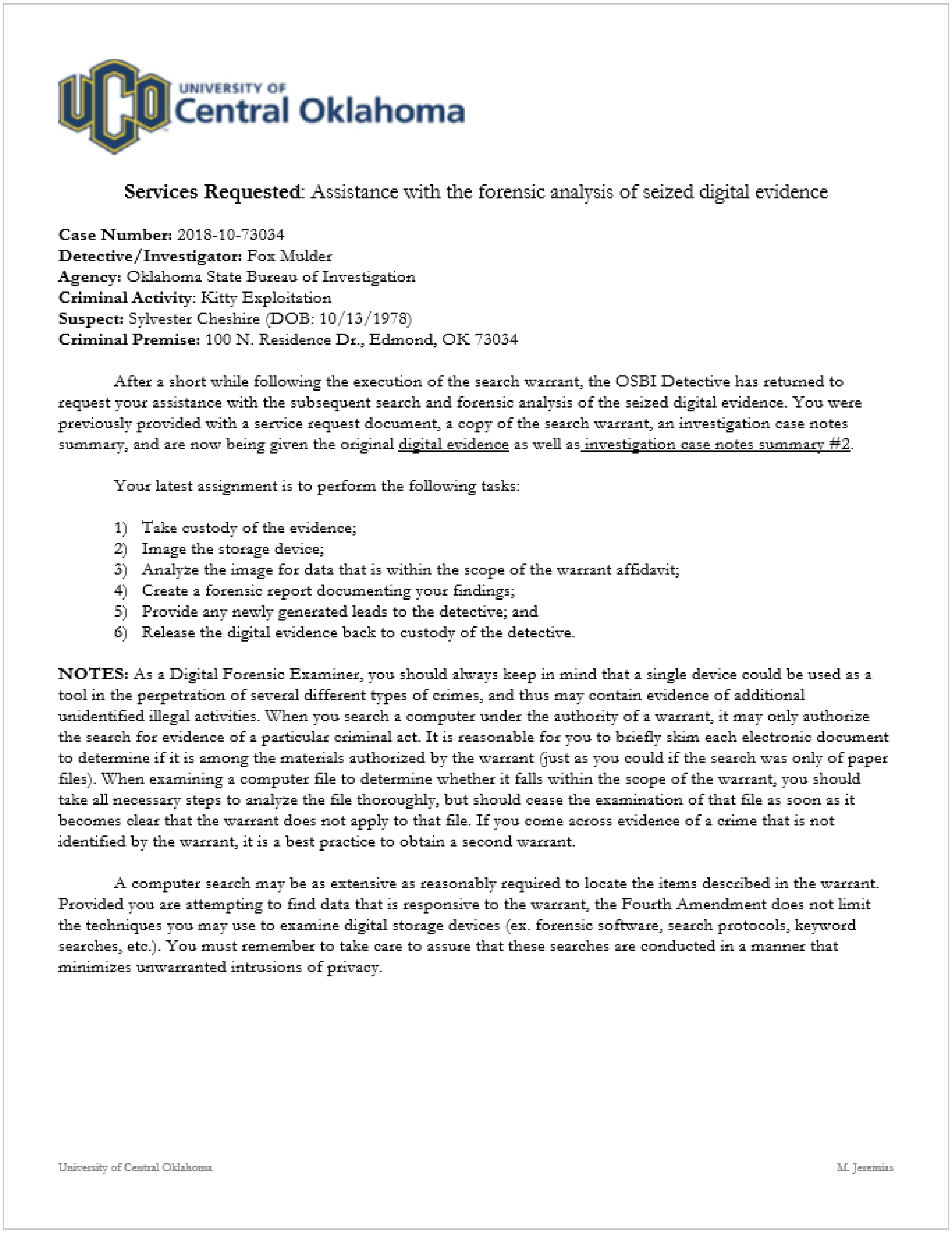
letmein
trustno1
1qaz2wsx
abc123

qwerty
welcome
qwertyuiop
123456

University of Central Oklahoma M. Jeremias

Appendices

Appendix B: Sample Scenario 1b - Forensic Analysis of Seized Evidence



UNIVERSITY OF Central Oklahoma

Services Requested: Assistance with the forensic analysis of seized digital evidence

Case Number: 2018-10-73034
Detective/Investigator: Fox Mulder
Agency: Oklahoma State Bureau of Investigation
Criminal Activity: Kitty Exploitation
Suspect: Sylvester Cheshire (DOB: 10/13/1978)
Criminal Premise: 100 N. Residence Dr., Edmond, OK 73034

After a short while following the execution of the search warrant, the OSBI Detective has returned to request your assistance with the subsequent search and forensic analysis of the seized digital evidence. You were previously provided with a service request document, a copy of the search warrant, an investigation case notes summary, and are now being given the original digital evidence as well as investigation case notes summary #2.

Your latest assignment is to perform the following tasks:

1) Take custody of the evidence;
2) Image the storage device;
3) Analyze the image for data that is within the scope of the warrant affidavit;
4) Create a forensic report documenting your findings;
5) Provide any newly generated leads to the detective; and
6) Release the digital evidence back to custody of the detective.

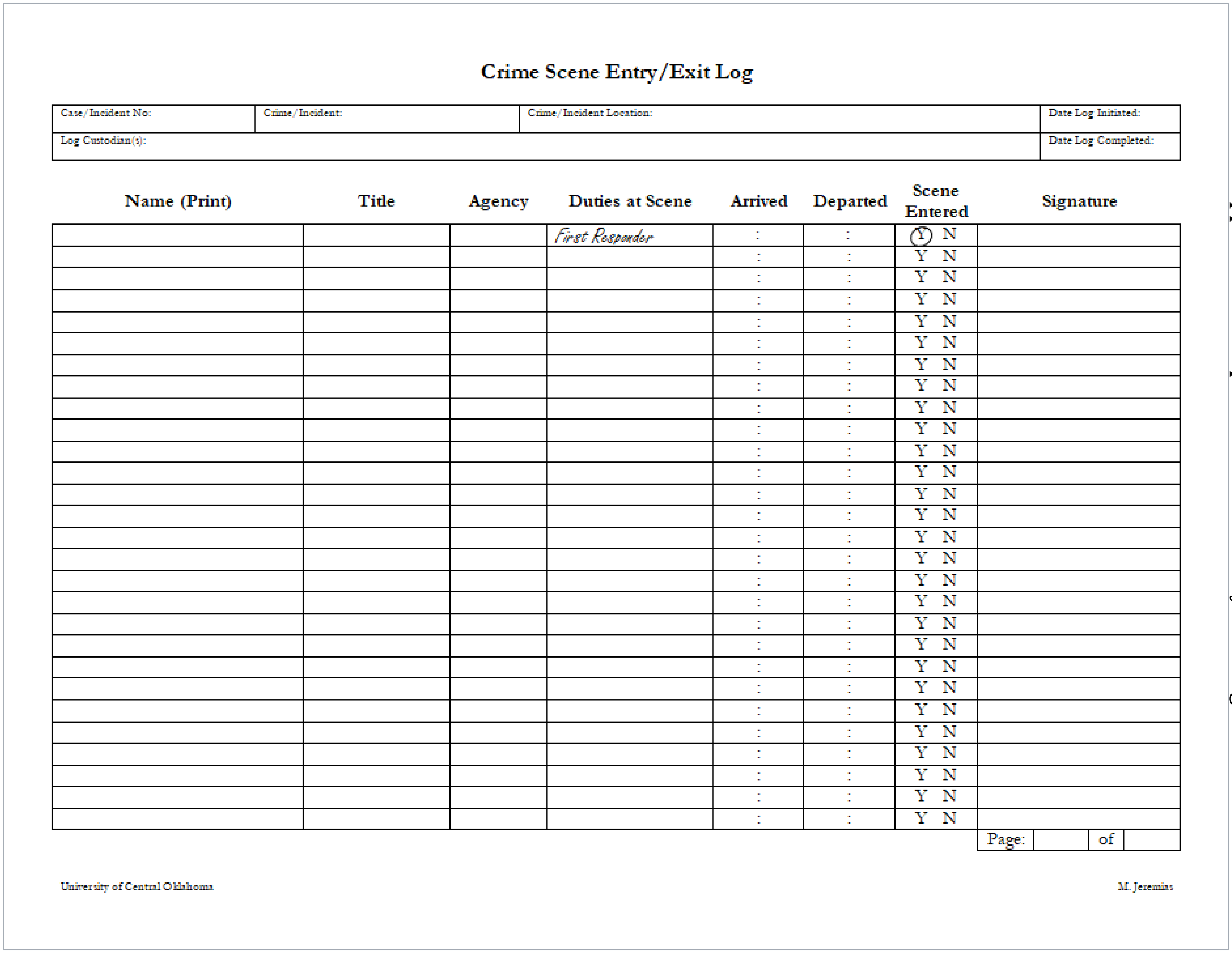
NOTES: As a Digital Forensic Examiner, you should always keep in mind that a single device could be used as a tool in the perpetration of several different types of crimes, and thus may contain evidence of additional unidentified illegal activities. When you search a computer under the authority of a warrant, it may only authorize the search for evidence of a particular criminal act. It is reasonable for you to briefly skim each electronic document to determine if it is among the materials authorized by the warrant (just as you could if the search was only of paper files). When examining a computer file to determine whether it falls within the scope of the warrant, you should take all necessary steps to analyze the file thoroughly, but should cease the examination of that file as soon as it becomes clear that the warrant does not apply to that file. If you come across evidence of a crime that is not identified by the warrant, it is a best practice to obtain a second warrant.

A computer search may be as extensive as reasonably required to locate the items described in the warrant. Provided you are attempting to find data that is responsive to the warrant, the Fourth Amendment does not limit the techniques you may use to examine digital storage devices (ex. forensic software, search protocols, keyword searches, etc.). You must remember to take care to assure that these searches are conducted in a manner that minimizes unwarranted intrusions of privacy.

University of Central Oklahoma M. Jeremias

Appendices

Appendix C: Sample Crime Scene Entry/Exit Log Form



Crime Scene Entry/Exit Log

Case/Incident No:	Crime/Incident:	Crime/Incident Location:	Date Log Initiated:
Log Custodian(s):			Date Log Completed:

Name (Print)	Title	Agency	Duties at Scene	Arrived	Departed	Scene Entered	Signature
			First Responder	:	:	[✓ Y] N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	
				:	:	Y N	

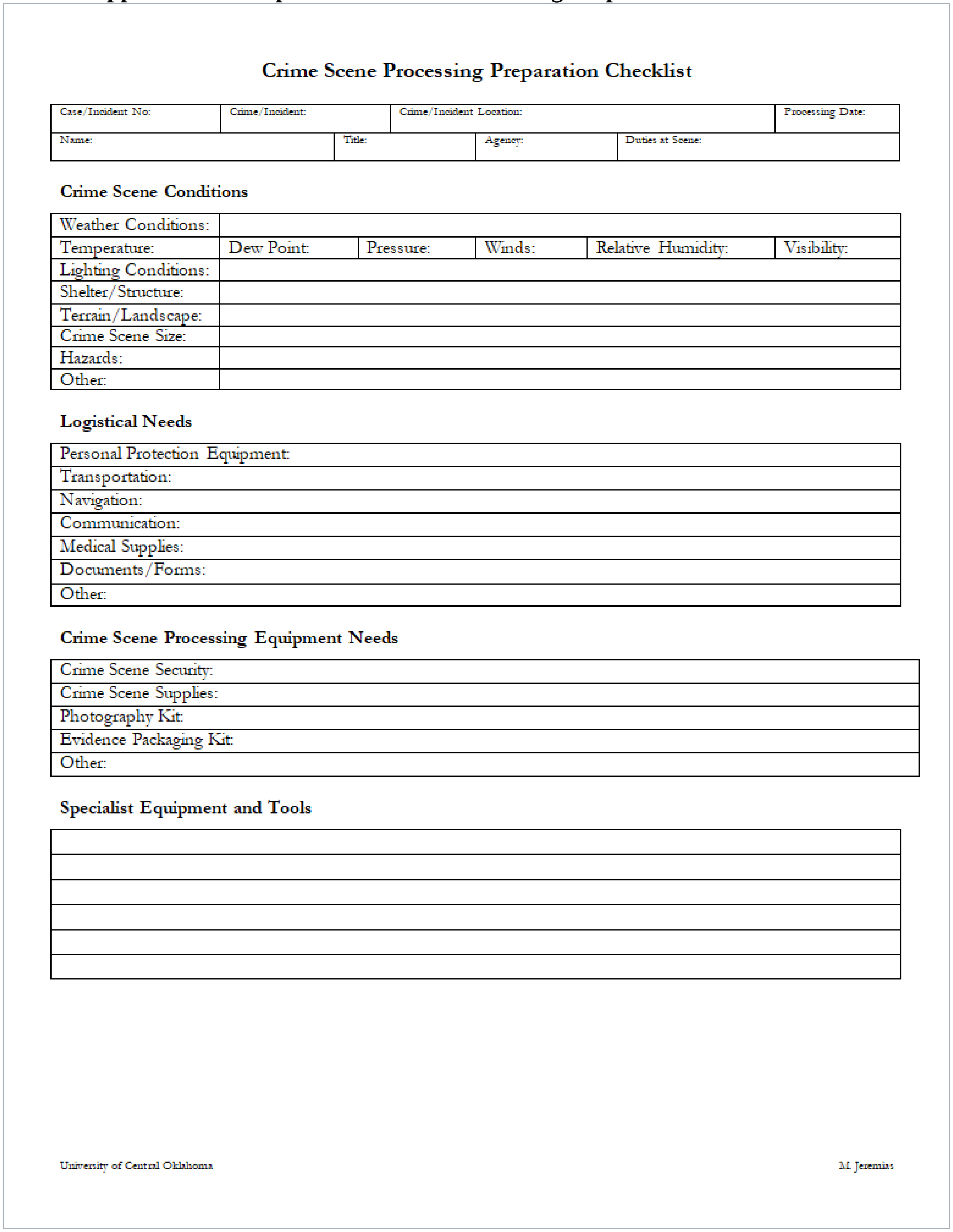
Page: ____ of ____

University of Central Oklahoma

M. Jeremias

Appendices

Appendix D: Sample Crime Scene Processing Preparation Checklist Form



Crime Scene Processing Preparation Checklist

Case/Incident No:	Crime/Incident:	Crime/Incident Location:	Processing Date:
Name:	Title:	Agency:	Duties at Scene:

Crime Scene Conditions

Weather Conditions:						
Temperature:	Dew Point:	Pressure:	Winds:	Relative Humidity:	Visibility:	
Lighting Conditions:						
Shelter/Structure:						
Terrain/Landscape:						
Crime Scene Size:						
Hazards:						
Other:						

Logistical Needs

Personal Protection Equipment:

Transportation:

Navigation:

Communication:

Medical Supplies:

Documents/Forms:

Other:

Crime Scene Processing Equipment Needs

Crime Scene Security:

Crime Scene Supplies:

Photography Kit:

Evidence Packaging Kit:

Other:

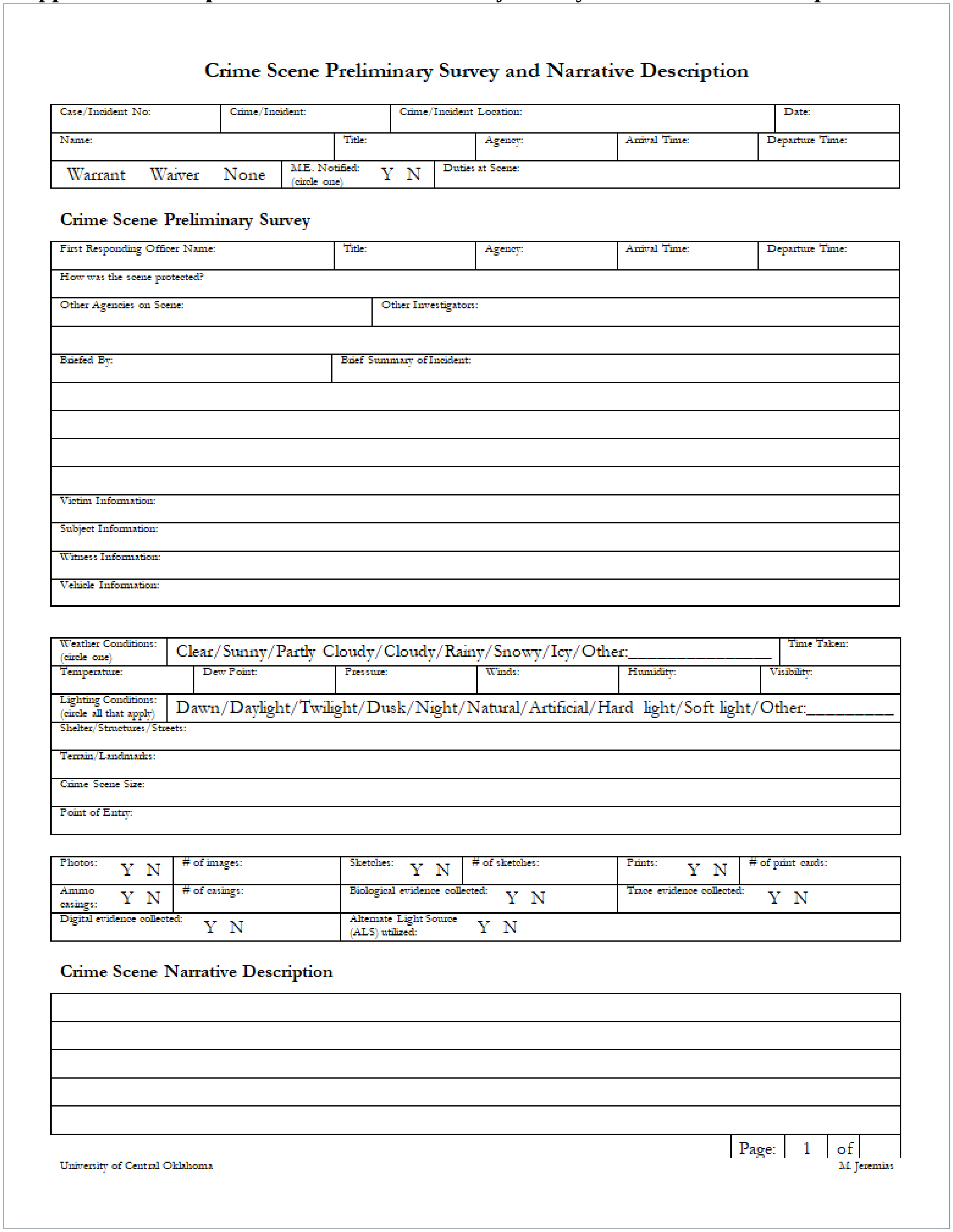
Specialist Equipment and Tools

University of Central Oklahoma

M. Jeremias

Appendices

Appendix E: Sample Crime Scene Preliminary Survey and Narrative Description Form



Crime Scene Preliminary Survey and Narrative Description

Case/Incident No:	Crime/Incident:	Crime/Incident Location:	Date:	
Name:	Title:	Agency:	Arrival Time:	Departure Time:
Warrant Waiver None	M.E. Notified: (circle one) Y N	Duties at Scene:		

Crime Scene Preliminary Survey

First Responding Officer Name:	Title:	Agency:	Arrival Time:	Departure Time:
How was the scene protected?				
Other Agencies on Scene:	Other Investigators:			
Briefed By:	Brief Summary of Incident:			
Victim Information:				
Subject Information:				
Witness Information:				
Vehicle Information:				

Weather Conditions: (circle one)	Clear/Sunny/Partly Cloudy/Cloudy/Rainy/Snowy/Icy/Other:________________	Time Taken:			
Temperature:	Dew Point:	Pressure:	Winds:	Humidity:	Visibility:
Lighting Conditions: (circle all that apply)	Dawn/Daylight/Twilight/Dusk/Night/Natural/Artificial/Hard light/Soft light/Other:__________				
Shelter/Structures/Streets:					
Terrain/Landmarks:					
Crime Scene Size:					
Point of Entry:					

Photos: Y N	# of images:	Sketches: Y N	# of sketches:	Prints: Y N	# of print cards:
Ammo casings: Y N	# of casings:	Biological evidence collected: Y N		Trace evidence collected: Y N	
Digital evidence collected: Y N		Alternate Light Source (ALS) utilized: Y N			

Crime Scene Narrative Description

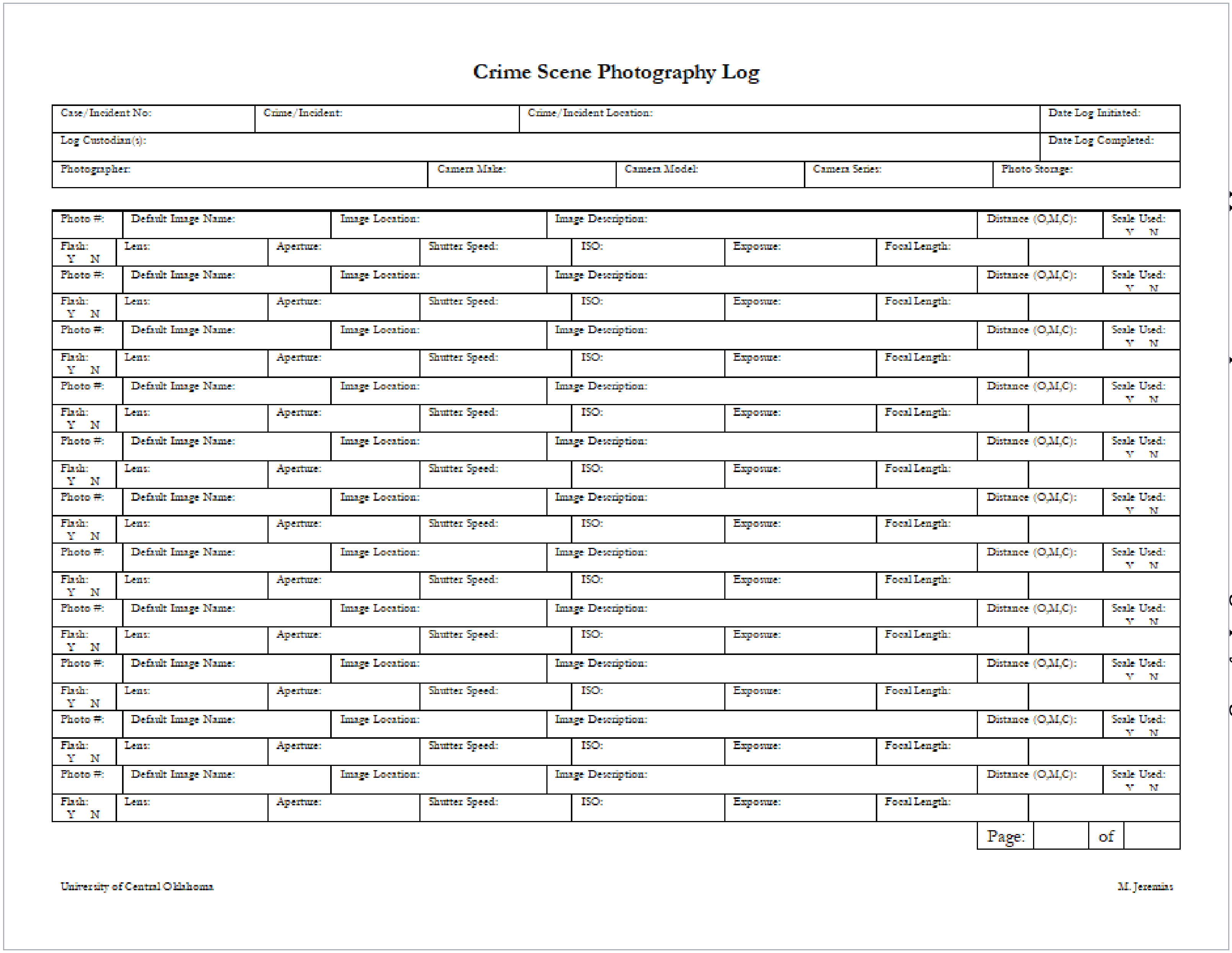
Page: 1 of

University of Central Oklahoma

M. Jeremias

Appendices

Appendix F: Sample Crime Scene Photography Log Form



Crime Scene Photography Log

Case/Incident No:	Crime/Incident:	Crime/Incident Location:		Date Log Initiated:
Log Custodian(s):				Date Log Completed:
Photographer:	Camera Make:	Camera Model:	Camera Series:	Photo Storage:

Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	
Photo #:	Default Image Name:	Image Location:	Image Description:			Distance (O,M,C):	Scale Used: Y N
Flash: Y N	Lens:	Aperture:	Shutter Speed:	ISO:	Exposure:	Focal Length:	

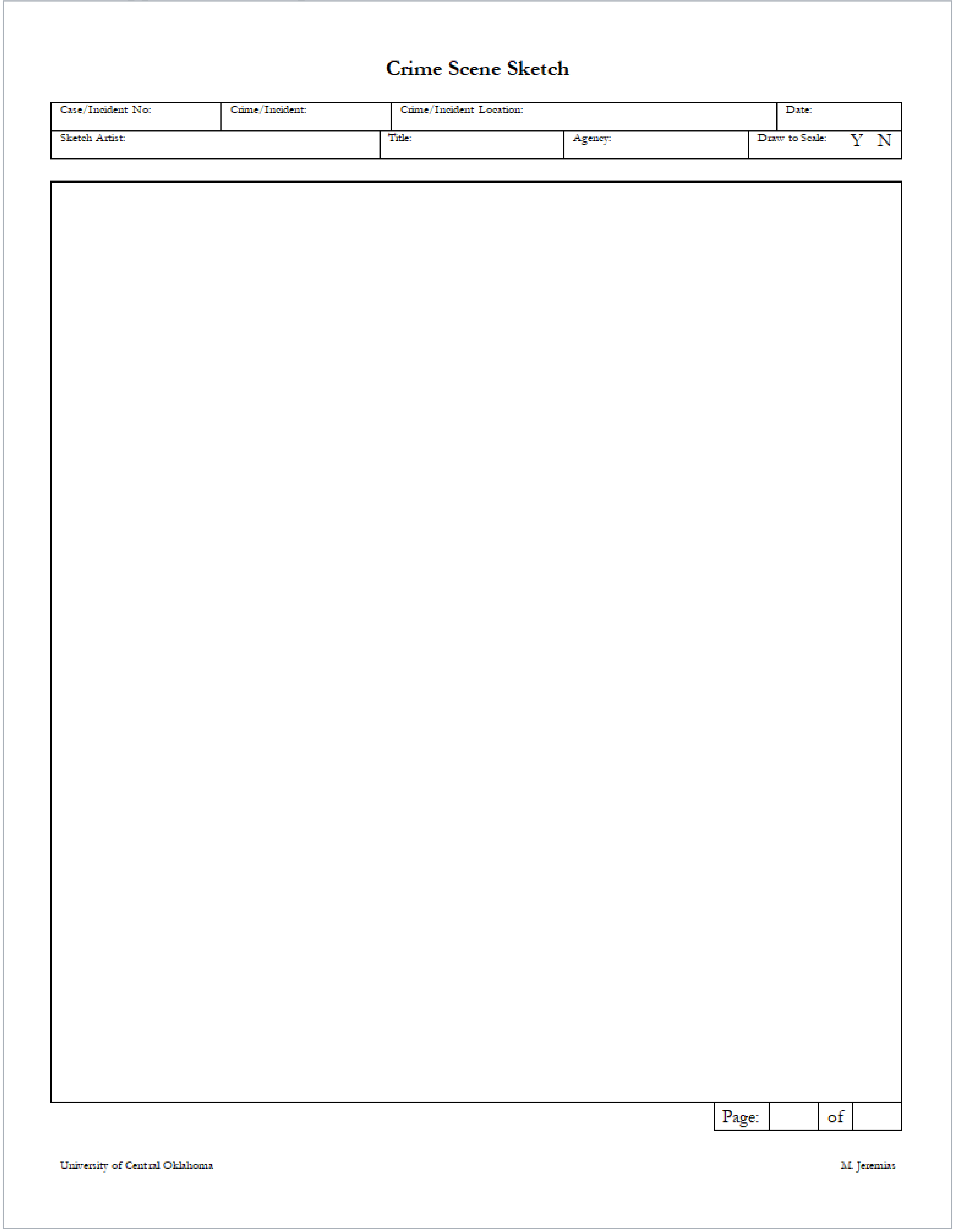
Page: ____ of ____

University of Central Oklahoma

M. Jeremias

Appendices

Appendix G: Sample Crime Scene Sketch (Portrait Orientation) Form



Crime Scene Sketch

Case/Incident No:	Crime/Incident:	Crime/Incident Location:	Date:
Sketch Artist:	Title:	Agency:	Draw to Scale: Y N

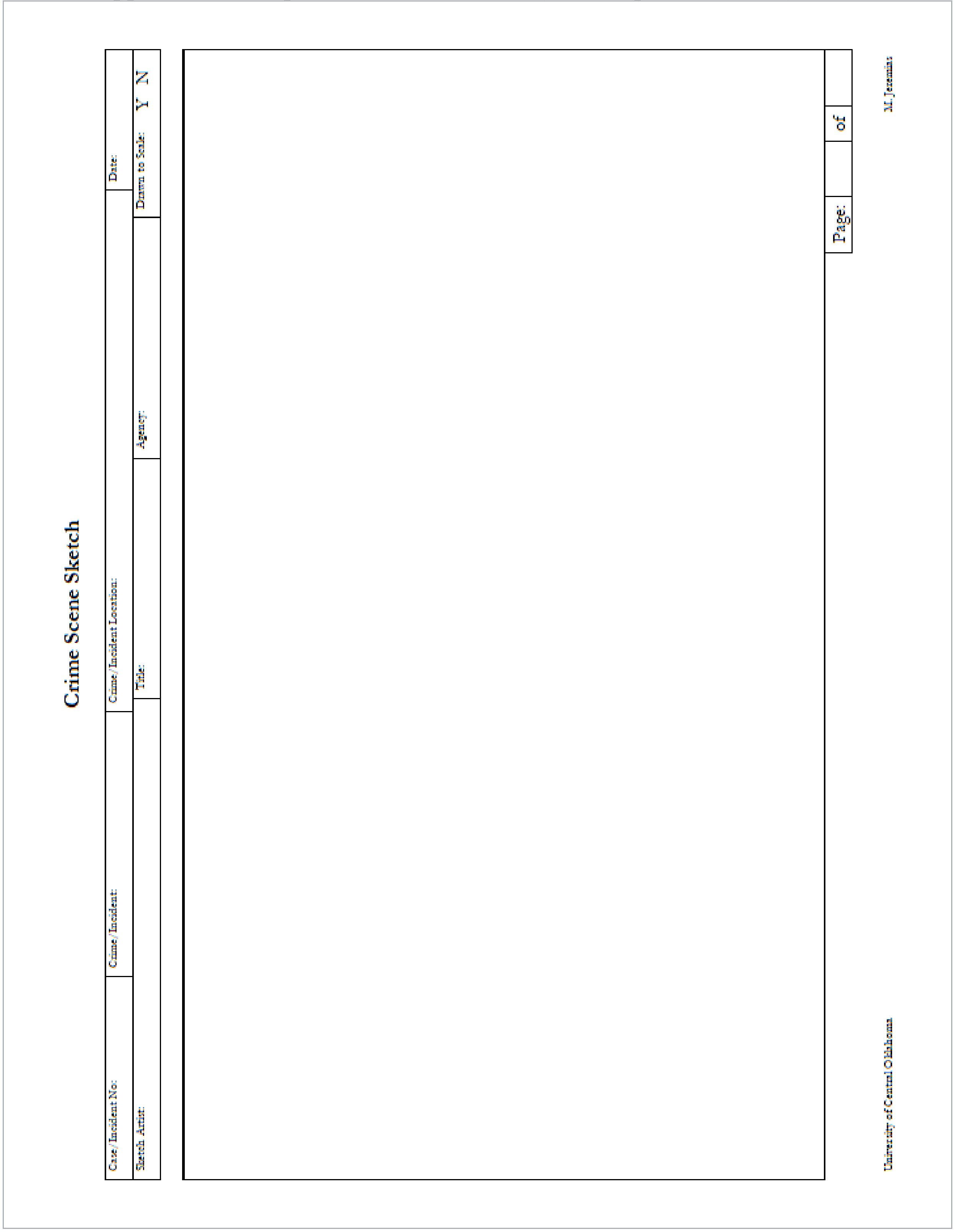
Page: of

University of Central Oklahoma

M. Jeremias

Appendices

Appendix H: Sample Crime Scene Sketch (Landscape Orientation) Form



Crime Scene Sketch

Case/Incident No:

Crime/Incident:

Crime/Incident Location:

Date:

Sketch Artist:

Title:

Agency:

Drawn to Scale: Y N

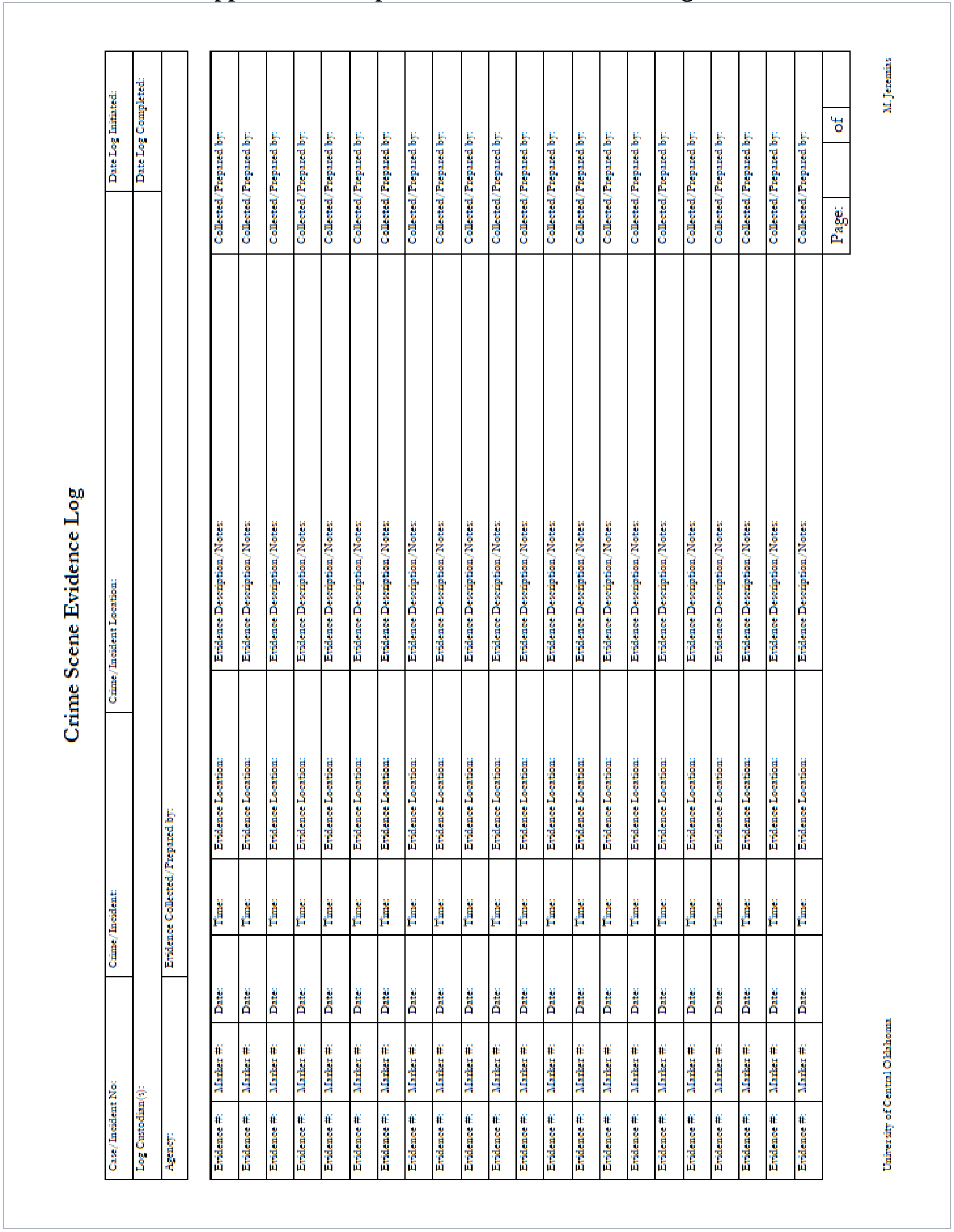
Page: of

University of Central Oklahoma

M. Jeremias

Appendices

Appendix I: Sample Crime Scene Evidence Log Form



Crime Scene Evidence Log

Case/Incident No:	Crime/Incident:	Crime/Incident Location:	Date Log Initiated:
Log Custodian(s):			Date Log Completed:
Agency:	Evidence Collected/Prepared by:		

Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:
Evidence #:	Marker #:	Date:	Time:	Evidence Location:	Evidence Description/Notes:	Collected/Prepared by:

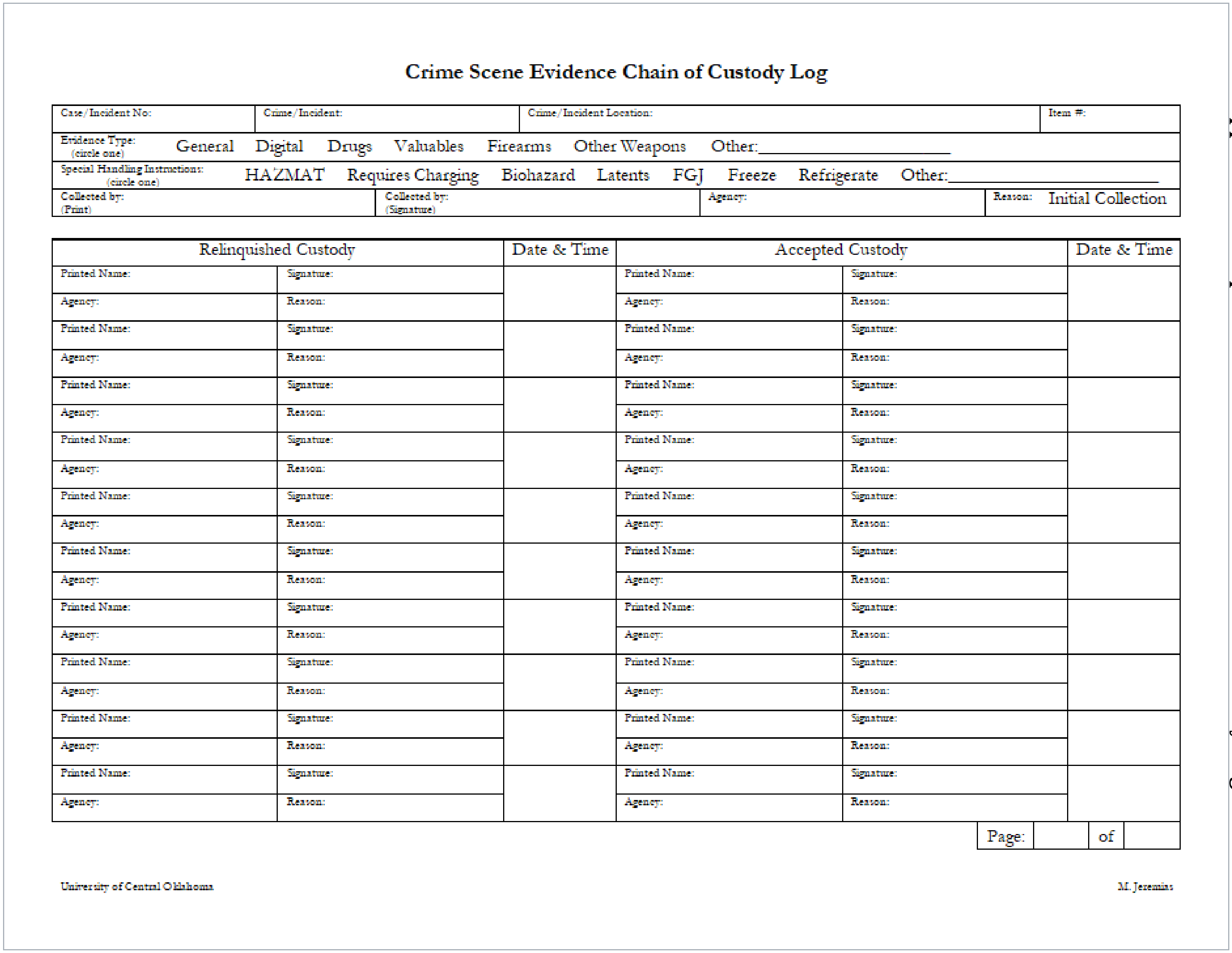
Page:		of	

University of Central Oklahoma

M. Jeremias

Appendices

Appendix J: Sample Crime Scene Evidence Chain of Custody Log Form



Crime Scene Evidence Chain of Custody Log

Case/Incident No:	Crime/Incident:	Crime/Incident Location:	Item #:
Evidence Type: (circle one)	General Digital Drugs Valuables Firearms Other Weapons Other:____________		
Special Handling Instructions: (circle one)	HAZMAT Requires Charging Biohazard Latents FGJ Freeze Refrigerate Other:____________		
Collected by: (Print)	Collected by: (Signature)	Agency:	Reason: Initial Collection

Relinquished Custody		Date & Time	Accepted Custody		Date & Time
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	
Printed Name:	Signature:		Printed Name:	Signature:	
Agency:	Reason:		Agency:	Reason:	

Page: ______ of ______

University of Central Oklahoma

M. Jeremias