THE DEVELOPMENT OF CYBERSECURITY CURRICULM IN ADVANCED TELECOMMUNICATIONS FORENSICS

By

Daniel Kalil

Richard Gloo

A Capstone Project Submitted to the Faculty of

Utica College

December 2012

In Partial Fulfillment of the Requirements for the Degree

Masters of Science CyberSecurity-Intelligence and Forensics

Abstract

A course in Telecommunications Forensics was created to fill an existing void within the Utica College Cybersecurity curriculum. The course existed as a concept, but had yet to be developed until this work was accomplished. The developed course focuses on the unique investigative techniques required to examine network communications and synthesize context as it pertains to traditional host and device digital forensics. By giving the student the insight, techniques, and tools required to solely focus on a network communications, many common questions can be answered throughout a digital forensics investigation. To achieve the development of Advanced Telecommunication Forensics, industry trends and needs were examined, cases involving network communications were reviewed, and similar educational programs were considered. The work accomplished in this capstone has resulted in the production of course materials, including a course outline, syllabus, weekly assignments, and hands-on-labs. All of this work was consequently loaded into the web based Angel course management interface, allowing the course to be offered as soon as desired by the Utica College Cybersecurity graduate program director and faculty.

Acknowledgement

The authors of this paper would first like to thank their family and friends for their patience, accommodations and understanding during the pursuit of the Utica College Cybersecurity Graduate Program. Secondly, the authors would like to thank the Utica College Cybersecurity faculty for mentorship and guidance in shaping the development of the course curriculum outlined in this capstone. Their experience, expertise and mentorship provided throughout the development of this course curriculum are all apparent in the quality of the resulting product. Specifically, we would like to thank Professor Joseph Giordano for his forward-looking vision in cybersecurity trends and educational requirements. Additionally, we would also like to thank Professor Christopher Riddell for his contribution in the fundamentals of developing effective curriculum, course content, and overall pedagogical insight. Finally, we must thank Professor Jeffrey Bardin, who taught us so much, while forcing us to look beyond the obvious. We could not have succeeded without all of your leadership.

Table of Contents

Table of Figures

The Development of Cybersecurity Curriculum in Advanced Telecommunications Forensics

Definition of Topic

Utica College offers both undergraduate and graduate degrees in Cybersecurity. Students pursuing an undergraduate degree in this discipline have the option of attending classes both online and in the classroom, while graduate classes are held online. In addition, graduate students must complete a Capstone project and must attend two residency weekends: one at the beginning of a student's first semester and one just past the halfway point of a student's graduate studies. The undergraduate program offers concentrations in two disciplines: 1) Computer Investigations and Forensics and 2) Information Assurance. The graduate program has concentrations in two similar disciplines: 1) Intelligence and 2) Computer Forensics. Public awareness and respect for this program is apparent, as enrollment for both the undergraduate and graduate programs is steadily increasing and many students are able to leverage their education toward fulltime employment or career advancement. Part of both programs' successes may be attributed to the unique course offerings and corresponding curriculum that provides students with many hands-on opportunities.

Utica College has a long history of involvement, leadership and education as it pertains to Information Assurance and Cybersecurity. The undergraduate program in Economic Crime Investigation and graduate program in Economic Crime Management were among the first of their kind, serving as a benchmark for other academic institutions to follow. These programs, like the Cybersecurity programs, provided students with education relevant to the ever-changing fields of Information Security and Cybersecurity.

Understanding that the cybersecurity field is continually changing and coursework must reflect such changes, this project is focused on preparing and delivering course curriculum and

supporting materials for a new and unique course that will be added to the Cybersecurity graduate program. Specifically, this course will be known as CYB 653, "Advanced Telecommunication Forensics" and will introduce concepts that will expand the course offerings, and provide the graduate program with an all-encompassing view of computer and network security and infrastructures. The proposed course requires that students be exposed to critical elements of network security, telecommunications and forensics. While portions of these disciplines are offered in other coursework within the same program, merging these together with a common emphasis results in unique course curriculum that leverages a diverse cross-section of the topic area. All materials will be populated into the online Angel course management shell. Upon completion of this effort, Utica College will be able to offer this course within their Master's of Science Cybersecurity program. This course could also be easily adapted and customized to meet the needs Utica College's undergraduate program in Cybersecurity.

Literature Review

Utica College had previously approved the offering of CYB653 "Advanced Telecommunication Forensics" but had yet to generate associated course content. As such, a review of relevant literature in support of necessity of this effort was conducted as a multi-prong effort. First, similar courses from other educational institutes and training organizations were reviewed. Classes offered in the area of network security and network forensics commonly provided a strong overview of networking technologies and then took an attack/defense approach to the class progression. Cybersecurity and related graduate programs within academia have steadily increased over the last 10 years. Such graduate programs appear to address similar aspects of Cybersecurity, with the distinction typically seen in course descriptions and execution of courses. This distinction may in part be due to an offering university's focus or emphasis, such

as engineering, vocational or research. To highlight the similarities and differences, three universities offering Cybersecurity and related graduate programs were reviewed. Polytechnic Institute of New York's (NYU-Poly) graduate Cybersecurity program was examined because of university's emphasis on engineering (John Hopkins University Webpage, n.d.). The University of Maryland University College's (UMUC) graduate Cybersecurity program was chosen because of its diverse vocational offerings (University of Maryland University College Master's Program, n.d.). John Hopkins's University's (John Hopkins University Webpage, n.d.) graduate Information Assurance program was examined for its long standing association with academic research (John Hopkins University Webpage, n.d.).

Polytechnic Institute of New York

NYU-Poly's Master's program in Cybersecurity offers various courses that address foundations of computer network environments, security and forensics. Specifically, "CS6963, Digital Forensics" provides graduate students with a fundamental overview of computer forensics, while other courses within the program address computer and network security (NYU Polytechnic Digital Forensics, n.d.).

University of Maryland University College

The UMUC program also provides coursework that addresses computer forensics, computer and network security. Courses such as CSEC 640 (Monitoring, Auditing, Intrusion Detection, Intrusion Prevention, and Penetration Testing) and (CSEC 650 (Cyber Crime Investigation and Digital Forensics) appear to be more vocational in nature, whereas NYU-Poly's coursework is structured around the engineering focus of the institution (University of Maryland University College Master's Program, n.d).

John Hopkins's University

JHU's Information Assurance graduate program has a strong focus on cybersecurity that is apparent when reviewing the associated course offerings. Specifically, within the program's Systems concentration, graduate courses such as "695. 742 - Digital Forensics Technologies and Techniques" provide students with a diverse overview of computer forensics, including identification, attribution and analysis on computer systems and networks (John Hopkins University 742/423, n.d.).

Within JHU's "Network" concentration, courses such as "695. 423 - Intrusion Detection" provides students with exposure to Intrusion Detection Systems (IDS) and associated challenges (John Hopkins University 742/423, n.d.). This approach shows how a network can be used to attack computer systems or steal data and allows the student to become adept at the core concepts required to investigate cases where network communications play a significant role.

Selected Readings

Numerous articles and publications were reviewed and compiled to directly support the course content generation and the weekly reading assignments, as shown within the course syllabus, located within Appendix A. The proposed course requires that students are exposed to critical elements of network security, telecommunications and forensics. While portions of these disciplines are offered in other coursework within the same program, merging these together with a common emphasis results in unique course curriculum that leverages a diverse set of readings.

The chapters selected for reading within the course book titled, "The Tao of Network Security Monitoring: Beyond Intrusion Detection" provide students with both fundamental network and related security knowledge and practical implementation of various network defense techniques (Bejtlich, R, 2005). In addition, these chapters also expose students to

network operations and associated security threats and risks. Other selected readings such as "UDP vs. TCP" provide a baseline comparison and contrast of two distinct networking protocols (User Datagram Protocol and Transmission Control protocol) and understanding the differences is critical when setting up, maintaining, protecting and forensically examining network communications (Fiedler, G, 2008).

Similar to elements found within the selected course book, the reading titled "A Summary of Network Traffic Monitoring and Analysis Techniques" provides both reasoning and practical implementation to better protect computer networks (Cecil, A, n.d.). This information can be critical to first responders and/or forensic examiners who are often tasked with examining networks and network data and must know where to look for information. Utilizing this information in conjunction with even more specific analysis techniques, such as those found within the documents titled "Quick and dirty packet capture data extraction" and "Open Source VoIP Traffic Monitoring," as well as the video titled "Extract PDF File from HTTP steam using Wireshark," prepare students of this course to not only know what information to look for but where to look and analysis techniques (Stretch, J, 2009) & (Deri, L, n.d.) & (Jlgaddis, 2009). Other selected readings, such as "Forensic investigation of peer-to-peer file sharing networks" and "Chapter 12, E-mail Investigations. IT IS 4250 Computer Forensics" provide additional granularity, offering techniques and methods to extract and analyze data from commonly used network communication applications (Erdely, R., Kerle, T., Levine, B., Liberatore, M., Shields, C, 2010) & (Long, B, n.d.).

Learning Theory and Instructional Design

Once the topic area literature review and background investigation was completed it was necessary to examine methods to systematically develop the course curriculum. Instructional

design methods provide a framework and approach to systematically progress through the analysis, design, and development of a curriculum or course. Instructional design methods are based on, and often emphasize, a specific learning theory to optimize the learning objectives. Learning theories provide specific considerations to achieve a particular learner outcome and are often grounded in psychology. Or as more simply stated by Smith (1998), a learning theory is how people learn, whereas the instructional design is the best method to create course content to ensure learning occurs. An example of a more primitive learning theory is the behaviorism learning theory, which seeks to alter the behavior of the student (Mergel, 1998).

As is outlined by Mergel (1998), the outcome sought through the behaviorism learning theory is to change a learner's behavior such that a response to stimuli becomes automatic. Mergel (1998) discusses two examples of behaviorism-based outcomes. The first is the classical psychological experiment known as Pavlov's Dog. In the Pavlov's Dog experiment, the instructor was seeking to change the behavior of the student (the dog) by ringing a bell. The dog was taught that when the bell rang it would soon be fed, and as such the dog became conditioned to salivate as it expected to be fed. Once the behavior was changed based on the stimuli, the dog would salivate when the bell was rung, regardless of whether or not it was eventually fed.

Another example outlined by Mergel (1998) was the training of World War II (WWII) pilots. The WWII pilots were taught to respond and shoot at silhouettes of enemy aircraft. The intent of the pilot training was to change the behavior of the pilot to automatically shoot at enemy aircraft when they were observed. Behaviorism is at the lowest end of cognitive scale and the major weakness outlined by Mergel (1998) is that the learner cannot be conditioned to respond to new scenarios and is limited to only those in which they have been trained.

Cognitivism is a learning theory that bridges the gap between the learning process and the functionality of the mind (Jorda & Campbell, n.d.). The cognitivism learning theory followed the behaviorism learning theory and suggested that as the student learned, the internal structure, or schemata of the mind was changed (Learning Theories Knowledgebase, 2012). To teach a new topic the mental processes are targeted and include memory, problem solving and processing of new events (Learning Theories Knowledgebase, 2012). Examples of considerations regarding the cognitivism learning theory include visual, sequential, audio, and experience based learning (Oracle Thinkquest, n.d.).

Instructional design models provide a method to develop content to ensure that learning occurs. There are many different instructional design models that can be considered. Each instructional design model typically seeks to fulfill a specific objective such as teaching a specific skill, imparting knowledge, or goal based problem solving. As outlined by Gustafson and Branch (2002), the key components of a instructional design model are that they are learner centered, goal oriented, focused on real world performance, focused on outcomes that can be measured, are empirical, and are often a team effort. In this section the ADDIE, Pebble-in-the-Pond, and Reiser and Dick instructional design models will be briefly discussed.

The ADDIE model is considered one of the early instructional design models, but the exact origin of the ADDIE is unknown to those who study instructional design (Molenda, 2003). ADDIE is an acronym where each step of the process is represented by the phases Analyze, Design, Develop, Implement, and Evaluate (Gustafson & Branch, 2002). Many other instructional design models, to include Reiser and Dick (1996), are largely extensions of the ADDIE design model and will generally contain all of the core elements of ADDIE (Gustafson & Branch, 2002). The Reiser and Dick model extends the ADDIE model to eight phases and

includes identification of the audience, instructional goals and enabling objectives, instructional activities and instructional media, development of assessment tools, as well as the implementation and revision phases.

The Pebble-in-the-Pond model diverges from the approach taken by the ADDIE based models in that the Pebble-in-the-Pond model is design oriented and prescriptive (Merrill, 2002). The concept behind the Pebble-in-the-Pond model is that the instructions stems from a problem and then tasks become increasingly more challenging to build up to the solution or approach to solve the original problem. The general flow of the Pebble-in-the-Pond model is to progress from the problem into knowledge component analysis, instructional strategy, design, and production phases (Merrill, 2002). The core idea behind the Pebble-in-the-Pond model is that the students are given a problem and told that they will be required to solve that problem. The knowledge components required to solve that component are then identified and presented to the student. Throughout a Pebble-in-the-Pond designed course, this sequence is repeated and the guidance for solving the problems reduces, because in theory, the student will build a foundation and the necessary knowledge to solve domain specific problems through this repetition (Merrill, 2002).

Methodology

To begin defining the course content and general progression it was necessary to follow a structured approach. To achieve the necessary structure in creating the Telecommunication Forensics curriculum, the Reiser and Dick (1996) instructional design model was used to develop the course in coordination with the Cybersecurity department. Regular meetings occurred in coordination with the Cybersecurity department to ensure the course material and overall objectives were being met. Before starting the development of the course curriculum a background review was conducted to evaluate existing cybersecurity programs as well as similar

training programs at respected organizations. Once the background review was complete, the Reiser and Dick instructional design model was used to structure the course content that included weekly readings, labs, and discussion topics. The Reiser and Dick instructional design model was chosen due to the granularity of the steps within the model and due to the inherent flexibility within the model to adapt to changing instructional environments. To define a class in Telecommunications Forensics, the following section outlines the details of each step within the Reiser and Dick (1996) instructional design model. Where necessary, the Reiser and Dick (1996) model has been augmented to provide additional information necessary to provide a comprehensive learning experience for the student and flexible design for the course instructor.

The Reiser and Dick (1996) Instructional design model outlines the following structured approach to developing course materials:

1. Target audience and prerequisites
2. Identification of instructional goals
3. Identification of enabling objectives
4. Identification of instructional activities
5. Identification of instructional media
6. Develop assessment tools
7. Implement instruction
8. Revise plan

Each of the steps within the instructional design model were defined and outlined throughout the development of the course and the results can be seen in the Description of Results section of this paper. The developed course materials were then loaded into the Angel content management system.

Description of Results

Prior to preparing course content for CYB653, a course description and learning goals needed to be established. To accomplish this, the terms "Telecommunications" and "Forensics" needed to be scoped, as they are extremely broad and when used together, created a wide range of interpretations. Reviewing current course descriptions and learning objectives within the same graduate program avoided potential conflicts. Individual course assignments within other courses were also considered, in effort to leverage existing knowledge areas, while leading into new ones. Finally, industry trends and needs in telecommunications and forensics were considered, ensuring that the course was focused on relevant material that students would need to mature in the discipline of computer network investigations. As also listed within Appendix A, the specific learner outcomes defined for this course are:

Target Audience and Prerequisites

This course is designed to educate a diverse student base in which their prior education, training and professional experiences are anticipated to be significantly different. The assignments and labs developed for this course will not require prior coursework in computer science, engineering and telecommunications principles. Selected readings will introduce new information and concepts, while leveraging prior knowledge gained in previous cybersecurity courses. For this reason, it is strongly recommended that students enrolled in this course have previously completed the majority of courses associated with Utica College's cybersecurity graduate program, as information related to forensics, networking and security will be utilized within this course. Labs will provide students with hands-on experiences that require them to utilize new cybersecurity software applications and techniques against various datasets. It is anticipated that these labs will be challenging but are manageable and consistent with graduate

level coursework. The discussion assignments will foster a collaborative learning environment, allowing students to not only address many aspects of a similar problem space but examine those aspects more in-depth.

Identification of Instructional Goals

To begin defining the Telecommunications course it was necessary to define the instructional goals. The instructional goals are the intended outcomes that students will have reached by the end of the course. Generally speaking, the goals were defined to provide students with a mindset and the necessary tools to explore network communications. The goals were kept broad to due to the fact that the UC Cybersecurity program is not an engineering program and students are expected to only have a foundational knowledge of networking technologies. Networking and telecommunications are very complex fields with entire degree programs dedicated to their study. The course will provide the students with the background and tools to begin investigating and exploring evidentiary data within the network infrastructure. Specifically, the following goals were developed for the Telecommunications course.

a. Develop an investigatory mindset geared towards network communications.
b. Identify and understand the methodologies used to address network communications data.
c. Identify concerns and issues unique to examining network communications.
d. Understand the tools, technology, and techniques that are used to identify and analyze forensically relevant communications data.
e. Identify and utilize proper analysis and filtering procedures for network communications.
f. Initiate investigations involving the transfer of data from one or more communicating devices.

The above section outlines the high-level goals that the students will be working to achieve by following the curriculum outlined in the Telecommunications Forensics class. The goals cover the investigatory mindset, to the more specialized applications of specific tools and technologies.

Identification of Enabling Objectives

The previously identified goals, when reached will provide students with fundamental knowledge in diverse technical areas related to cybersecurity, telecommunications and forensics. While each goal is distinctly different, the objectives required to achieve them are relatively similar and can be used to support multiple goals. A fundamental forensic process includes initial contact, preservation, acquisition, verification, recovery, analysis, correlation and reporting of examined electronic data. This process, regardless of technology or dataset must be considered prior to pursuit and regardless of actual implementation or inhibiting challenges. The objectives support the application of forensic collection and analysis of network datasets and are as follows:

a. Investigate the relevancy and necessity of each step within the forensic process.
b. Identify specific processes and techniques within each of the forensic processes.
c. Identify the differences within each step of the forensic process that require unique consideration for each dataset, including network data.

Identification of Instructional Activities

The instructional activities planned for this course were chosen to fit within Utica College's current Cybersecurity graduate program as it builds the existing knowledge base while expanding into new areas. Within the Utica College Cybersecurity Graduate program a large focus is placed on the investigation of host computer systems and endpoint devices. Although network communications are a factor in the labs and mock investigations in the Utica College

curriculum, no course takes an in-depth investigative approach focused primarily on network communications. By investigating the network communications, significant context can be lent to traditional host and device based digital forensics investigations. Additionally, the course addresses critical topics and unique technologies encountered by industry today, such as voice over IP (VoIP), peer-to-peer communications, and data exfiltration techniques. Finally, the course is laid out in a clear, concise, and consistent manner, allowing instructors to easily teach, organize and update content as needed while facilitating students in learning a rather complex topic. The three high-level instructional activities include week reading assignments, class discussion topics, and course labs. The weekly reading assignments provide the students with the foundation and background knowledge to support the secondary activities such as a discussion or lab. The discussion topics allow the students to work through the new knowledge gained in the readings to compare and contrast viewpoints as well as explore new facets of the topic that may not have been fully addressed by the reading. Ultimately the reading and discussion topics are reinforced by applying the new knowledge by putting into practice through the hands-on labs.

Weekly Reading Assignments

The course reading topics include webpages, journal articles, blogs, and the course text to provide background to the weekly lessons. The readings may include foundational information on a specific topic or take an in-depth look at a particular technology related to the weekly topic.

Class Discussion Topics

Two discussion topics were outlined for this course. The first topic provides the students with a discussion forum to scope the concept of telecommunications forensics. They will cover both how vast the technical domain is, but also start to understand how focused it can become depending on the incident being investigated.

Topic 1 – Introduction to Telecommunications Forensics. The term "telecommunication" can be summarized as the communication of information through the use of some medium. Because the medium is not defined and can range from smoke signals to cellular transmissions, we must first scope the term for the purposes of this class. To properly scope the term, we will only consider those mediums that are commonly used or emerging within the 21st century. For this discussion, we will focus on the term forensics and it's applicability to specific telecommunication mediums. Students are expected to identify a specific 21st century telecommunication medium and identify storage abilities and locations within that medium that may store digital data of interest. Additionally, please identify any tools, techniques or methodologies that currently exist to extract and analyze such data.

Topic 2 – Telecommunications and Cybercrime. Society utilizes many forms of telecommunications as a means to accomplish various tasks. As we know, this utilization is a dependency and without it, progress would be difficult to achieve. The commission of many crimes (not just cyber) is often dependent on the utilization of telecommunications. For this weeks' discussion, students are expected to identify cybercrimes that made news in recent years and encompassed a specific telecommunication medium(s). Students are expected to summarize the identified cybercrime, the purpose and methods/exploits utilized by the criminal and/or attackers, the telecommunication medium(s) utilized and/or targeted and a summary of the investigative techniques utilized.

The above discussion topics provide the students with the opportunity to explore the more subjective topics within the field to telecommunications forensics. The students will be able to participate in a collaborative discussion while exchanging and forming opinions on the general concepts required to investigative incidents on communication networks.

Course Labs

The course labs are hands-on objective based learning activities that allow the students to apply the knowledge gained in the reading and discussions assignments. The hands-on course labs also allow the students to build a competency in foundational tools that can be applied to new scenarios encountered once they graduate and move into the professional field.

Within the labs the students develop an understanding of the fundamental tools that are available to investigate and manipulate network communications. The tools also serve to reinforce the basics of network communications and functionality. Within this lab the students experiment with transferring a file over the network using the Netcat tool. Netcat is a tool used to make arbitrary raw TCP connections. Netcat is an extremely flexible tool and is the self-proclaimed and undisputed TCP/IP Swiss army knife. From an investigative standpoint, Netcat can be utilized to discover services on a remote host or to instantiate a local service to examine incoming connections. Although the lab is designed to function on a single computer system, in practice it would more commonly be deployed amongst multiple hosts on an intranet or Internet. The TCP ports used within the lab would need to be changed to traverse network firewalls and to connect to the correct ports. The Netcat tool allows the student to arbitrarily pass data over an unencrypted network connection, and is used to support later components of the Network Utility lab. To selectively identify network packets that contain specific data it is necessary to employ a network search component within the lab. The traffic search experiment employs the Ngrep tool to monitor network traffic for a specific term. Ngrep is able to monitor live network traffic and output packets to a packet capture file when a specific search term or pattern is matched. The Ngrep tools will allow the investigator to easily extract a specific term from an unencrypted network communications stream. The Ngrep utility can be configured to identify specific packets

streams for specific search terms, such as “confidential data”, or to identify a pattern such as a social security number or credit card. Ngrep is easily deployed as a real-time monitoring utility, but could also be used as an offline analysis tool for a post-mortem investigation. While the Ngrep search component shows the student how a specific keyword or pattern can be identified in plaintext network traffic, the Cryptcat tool can be used to encrypt arbitrary network connections and evade tools like Ngrep. The students use the Cryptcat tool to transfer data and see how the Ngrep tool is no longer useful when examining encrypted network communications. By using and examining encrypted network communications the students gain the insight into common techniques used by malware and attackers to exfiltrate data or control bots.

Wireshark, Argus, and EtherApe are tools that can be used to gain a statistical viewpoint of network traffic. By examining the statistical characteristics of network activity the student can easily gain a preliminary understanding of the network communications being examined. Information that can be identified includes the number of communicating nodes, the number of connections, the amount of data transferred per connection, etc. The information obtained through the statistical analysis provides the student with the initial context of the traffic being examined. The statistical characteristics allow the student to see potential anomalies or outliers that may prove to be of evidentiary value when examining network traffic and investigating an incident involving network communications.

Another important technique to master is the extraction of files from a network stream. The file extract techniques are largely covered in the data extraction utilities lab. In this lab the students gains an understanding for packet fragmentation the knowledge that when a file is transferred over the network it may get spread over multiple packets that are potentially out of order. These fragmented packets then need to be reordered and reassembled to extract the

transferred file. Multiple techniques exist for extracting a file from a communication stream. The tools covered in the lab include the Wireshark "Follow Stream" functionality, as well as the Driftnet tool and Filesnarf. Once these techniques are understood it is easy for the student to reapply the approach for any transferred file format whether it is an image, malware, document, etc. The major challenges in file extract will be discussed in the context of the lab and cover the application of encryption and new protocols. The file extraction techniques will allow the student to apply these techniques in the professional world to extract and analyze files in near real-time when investigating a case or exploring network activity.

Within the labs, techniques that are more commonly used within a malicious context are covered to provide the student with an understanding of how the network can be used against an organization. The TCPKill tool is used to show how network protocol semantics can be exploited to kill a network connection. The objective of the network attack experiment is to utilize the TCPKill command to monitor and terminate any active TCP connection. The network TCPKill experiment also reinforces how the TCP three-way handshake functions and forces the students to take a hands-on look at the functionality of how a connection is established. This will show how the TCP three-way handshake can be exploited to kill an existing connection. Often adversaries will use the TCPKill technique as a first step in session hijacking or to force an authentication process to occur. By forcing the authentication process to occur, the attacker is able to capture authentication credentials or important parameters. Network defenders could use the TCPKill command with equal success to kill an unauthorized network connection. Within the lab, the students use the Netcat tool to create a raw TCP connection that will then be terminated by the TCPKill tool. The TCPKill attack works equally well on any other TCP connection to include web connections or email. The students will gain an understanding and appreciation for

how a network protocol can be easily exploited while identifying methods to determine if such an attack has occurred. The second malicious traffic activity includes the data exfiltration lab. The data exfiltration lab allows the students to experiment with a live Domain Name Service (DNS) network tunnel. The DNS tunnel application is used as a carrier for other traffic to communicate through a network firewall or filter that only allows DNS traffic. Adversaries will commonly use tunneling techniques and the network investigators must be able to identify and understand how cover communications and tunneling techniques work. In this lab the students first run and use the tunnel, and then theorize on methods to restrict, block, or identify the tunneling activity. The DNS tunnel traffic is also compared to normal DNS traffic to determine methods identify the traffic as anomalous. Often incident response personnel will need to identify covert communications and then find all the hosts within the network that are using this communication mechanism. The DNS tunnel instructional activity provides the students with the context and tools to begin examining network communications for covert communications.

Identification of Instructional Media

The instructional media for this course will be consistent with the requirements for other online courses within the Utica College program. The course content will be delivered in online learning environment and all instructional media will be chosen as such. The instructional media will facilitate the completion of the hands-on labs, weekly readings, and discussion forum. The hands-on lab assignments will significantly rely upon a virtual machine environment. The virtual machine environment will allow students to install operating systems and tools within a virtual computing environment. The virtual machine software allows the labs and assignments to be run in isolation so as to not impact the student's personal computer. By using virtual machines there will be an inherent requirement on the student's computing system to have enough resources to

run the additional software. The performance requirements will be defined based on the installed virtual machines and should be evaluated each semester to ensure students have enough computing power to run the necessary software. The operating systems used within the virtual machine environment will be downloaded either from a website link or from a link provided on the Angel content management system. Due to the general size of operating systems, 750 megabytes to 1.5 gigabytes, it is recommended that students obtain the operating system directly from the developer's site rather than from Angel. The operating system files are most commonly distributed in a ISO 9660 archive file format. An ISO file is loaded into a virtual machine environment as if it was a physical CD-ROM. For the labs within this course a choice of two Linux live-CD's are available. Either Security Onion or Backtrack. The Security Onion Live-CD is the recommended operating system to use as it comes equipped with a significant number of network security monitoring applications as well as the applications required for the labs. The Security Onion is also a very useful tool that students can readily deploy as a network-monitoring sensor when they enter the professional world. Backtrack is an alternate to the Security Onion and more instruction may need to be provided for students to successfully install any tools that are missing to complete the labs.

Development of Assessment Tools

Assessment of course assignments will largely be focused on the course labs. At the graduate level the students are expected to have a high degree of rigor within the preparation of the lab submissions. Consistent with other classes in the Cybersecurity program, well-formatted, written, and organized documents are expected for course lab reports. The students are expected to provide a high degree of detail and analysis in their submissions to ensure the appropriate depth is achieved. Students will also be assessed based on participation within discussion

forums. The discussion forum posts will also be expected to be well written and provide a concise and compelling viewpoint on the topics being addressed. The instructor may also wish to develop a short quiz to deploy early in the semester to ensure that basic networking terminology and fundamentals are covered. This quiz and corresponding terminology will ensure that students have the basic understanding to read the necessary documentation required to operate the lab tools.

Instruction Implementation

The materials produced for this course has been populated into an Angel course shell in a straightforward and easy to follow manner. As displayed in Figure 1, the course is broken up into 8 weeks within the Lessons tab, each containing a different technical emphasis.

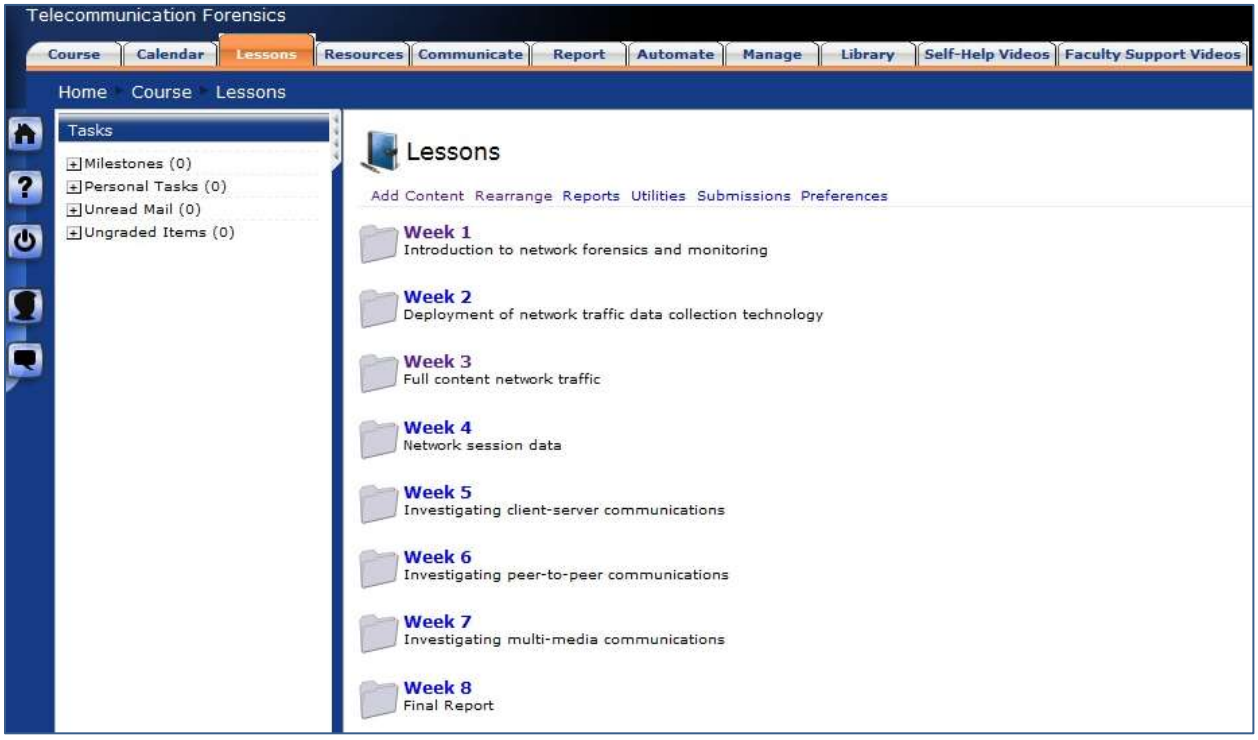

Figure 1: Angel Weekly Layout within Lessons Tab

As identified within Figure 2, each specific week is then further broken down, to include selected readings, discussions, lab practical assignments and a corresponding drop box.

Figure 2: Sample Weekly Layout

Revision plan

The course content should be reviewed and revised every semester to ensure that it is continually being improved to keep pace with common threats and market trends. Student feedback must be considered and improvements can be continually made to the labs. The class content will need to adapt as new technologies are available on the market and being deployed within networks. Given that the graduate program classes typically run 8-week semesters, the refinement of the class content should easily be able to maintain pace with market trends.

Conclusion and Recommendations

The pursued topic was relatively straightforward; develop course materials for a new course to be offered within Utica College's Cybersecurity Master's program. Successfully completing this task was not as straightforward and required overcoming multiple challenges. The proposed course title and description was vague and if followed closely, would have significantly limited the materials and learning objectives produced for this course. While the general purpose was understood, professional experiences and expertise were often relied on to produce a course with relevant and up-to-date content.

Determining where this course fit best into the Cybersecurity program was also a challenge for a couple of reasons. First, the course needed to leverage concepts in prior coursework but also needed to introduce new concepts of its own. As such, it was recommended that the course was offered after the completion of most other courses within this same program. Second, the curriculum produced for this course could have easily leveraged a significant amount of computer science concepts; however student's anticipated lack of prior knowledge in this discipline meant alternate, more practical concepts had to be introduced and developed into assignments.

To accomplish this, multiple sources of information were leveraged, including comparing similar programs offered by other universities, professional experiences, personal experiences with Utica College's Cybersecurity graduate program, as well as the utilization of many valuable informational resources, including selected readings and videos. This information was then pulled together and used to develop the course assignments, discussions and exams. Finally, the Reiser and Dick instructional design model was used in the course development, as it provided the flexibility needed to address a diverse student base and ever-changing cybersecurity field, allowing for the development of realistic goals and objectives. These efforts produced a full course being laid out and available within the Angel content management system. The result is the availability of a novel course that expands on the existing graduate program curriculum and introduces new and modern concepts not available within other courses.

Given the flexibility of the course, it is believed that multiple instructors will be able to instruct this course. It is strongly recommended that the course description and objectives remain constant, with course content being regularly evaluated and updated if necessary to reflect

industry trends and needs. To meet the current trends and to remain on the forefront of Cybersecurity education, it is recommended that the name of the class be changed.

The term Telecommunications has become antiquated is no longer used to represent current network communications. Telecommunications was traditionally used to refer the public switched telephone network and voice communications. For Utica College to remain on the forefront of Cybersecurity education a course title that accurately reflects current and future network communications technologies is most deserving. The following is a short list of potential course titles.

- Network Forensics
- Network Security Monitoring
- Investigating Network Communications
- Network Communications Forensics

It is important that the chosen name ultimately reflects the nature of the course, remains relevant for the coming years, and allows for instructional flexibility. It is important to note that although the title Telecommunications Forensics is used throughout the development of this paper and within the course, there would be no significant impact on the course by changing the name. In the event of a name change it would simply be necessary to change all occurrences of Telecommunications Forensics to the newly chosen name. The course material would not require any modification.

References

Bejtlich, R. (2005). The Tao of Network Security Monitoring: Beyond Intrusion Detection. Pearson Education, Inc. ISBN 0-321-24677-2 (pbk.)

Cecil, A. (n.d.). A Summary of Network Traffic Monitoring and Analysis Techniques. Retrieved October 29, 2012 from http://www.cse.wustl.edu/~jain/cse567-06/net_monitoring.htm

Deri, L. (n.d.) Open Source VoIP Traffic Monitoring. Retrieved October 29, 2012 from http://luca.ntop.org/VoIP.pdf

Erdely, R., Kerle, T., Levine, B., Liberatore, M., Shields, C. (2010). Forensic investigation of peer-to-peer file sharing networks. Retrieved on October 29, 2012 from http://www.dfrws.org/2010/proceedings/2010-311.pdf

Fiedler, G. (2008). UDP vs. TCP. Retrieved October 29, 2012 from http://gafferongames.com/networking-for-game-programmers/udp-vs-tcp/

Gustafson, K. L., & Branch, R. M. (2002). What is instructional design? In Reiser, R, A. and Dempsey, J. V. (ed's) Trends and Issues in Instructional Design and Technology. Columbus: OH, Merrill Prentice Hall.

Jlgaddis. (2009). Extract PDF File from HTTP steam using Wireshark. Retrieved October 29, 2012 from http://www.youtube.com/watch?v=GwAxzXSssz8 [Video]

John Hopkins University 742/423, (n.d.), Master of Science in Information Assurance, Retrieved October 30, 2012 from http://catalog.ep.jhu.edu/preview_program.php?catoid=20&poid=432&returnto=640.

John Hopkins University M.S. Program Webpage, (n.d.), Master of Science in Information Assurance, Retrieved October 30, 2012 from http://cyber.jhu.edu/.

Jorda, M. & Campbell, S., (n.d.), Cognitivism and Constructivism, Retrieved October 29th, 2012 from http://www.coe.fau.edu/faculty/cafolla/courses/eme6051/cognitivism.htm

Learning Theories Knowledgebase (2012, October). Cognitivism at Learning-Theories.com. Retrieved October 29th, 2012 from http://www.learning-theories.com/cognitivism.html

Long, B. (n.d.). Chapter 12, E-mail Investigations. IT IS 4250 Computer Forensics. Retrieved October 29, 2012 from http://coitweb.uncc.edu/~nblong/ITIS%204250/Lectures/Ver_3/Ch12-V3.ppt

Mergel, B., (1998), Instructional Design & Learning Theory, Educational Communications and Technology, University of Saskatchewan. Retrieved October 29th, 2012 from http://www.usask.ca/education/coursework/802papers/mergel/brenda.htm

Merrill, M. D. (2002). A pebble-in-the-pond model for instructional design. Perform. Improv., 41(7), 39–44.

Molenda, M. (2003). In Search of the Elusive ADDIE Model. Performance Improvement, 42(5), 34-36.

NYU Polytechnic Cybersecurity Program Overview Webpage, (n.d.), Master of Science in Cybersecurity. Retrieved October 30, 2012 from http://www.poly.edu/academics/online/masters/cybersecurity.

NYU Polytechnic Digital Forensics, (n.d.), CSC Digital Forensics, Retrieved October 30, 2012 from http://www.poly.edu/academics/course/CS6963.

Oracle Thinkquest, (n.d.), Cognitive Processes – Storage of Information, Memory and Language…, Retrieved October 29, 2012 from http://library.thinkquest.org/26618/en-5.5.3=cognitive%20learning.htm

Reiser, R. A. & Dick, W., (1996), Instructional Planning, Allyn and Bacon, Boston.

Stretch, J. (2009). Quick and dirty packet capture data extraction. Retrieved October 29, 2012 from http://packetlife.net/blog/2009/jul/13/quick-packet-capture-data-extraction/

Smith, K. J. (1998). Instructional design theory, Retrieved June 23, 2009, from http://www.ic.arizona.edu/ic/edp511/isd1.html.

University of Maryland University College Masters Program, (n.d), Master of Science in Cybersecurity, Retrieved October 30, 2012 from http://www.umuc.edu/grad/gradprograms/csec.cfm.

Appendix A - Course Syllabus

SYLLABUS

CYB 653 Advanced Telecommunications Forensics

Utica College

MS in Cybersecurity

3 credits

Instructor: TBD

Utica email: TBD

Phone: TBD

Course Description:

This course expands on previously learned forensic theories, technologies, and procedures by expanding into the area of network communications. This course will provide the necessary tools to lend context to a forensics investigation by examining the data being exchanged over various communication mediums. Students will receive hands-on practical application of specific tools, techniques and forensic investigation methodologies and workflows.

Required Textbooks:

Bejtlich, Richard (2004), The Tao of Network Security Monitoring: Beyond Intrusion Detection. ISBN: 978-0321246776

General Requirements

Since this as a distance learning course, there are a few assumptions about your access to technology. They are: You have regular access to a computer and high speed broadband Internet connection. The interaction with the course in Angel can be accomplished via a slower

connection but multiple downloads, research projects and activities will require a broadband throughput. If you cannot meet any of the above criteria, please contact the instructor in advance so alternative options may be considered.

Learner Outcomes:

At the completion of this course, students will be able to:

- Develop an investigatory mindset focused on network communications.
- Identify and utilize proper analysis and filtering procedures for network communications.
- Understand the tools, technology, and techniques that are used to identify and analyze forensically relevant communications data.
- Identify and understand the methodologies used to address network communications data.
- Initiate investigations involving the transfer of data from one or more communicating devices.
- Identify concerns and issues unique to examining network communications.

Evaluation:

Grading

Grading will be on the following point system:

93%-100% = A

90 %– 92.9% = A-

87%-89.9% = B+

83%-86.9% = B

80%-82.9% = B-

77% – 79.9% = C+

70%-76.9% = C

Below 70 = F

Points are given to the following course components:

Participation in threaded discussions	20 points
Final Report Abstract	10 points
Forensic labs and exercises	40 points
Final Report	30 points
TOTAL	100 points

Academic Expectations:

This is a 600 level Masters course, and all submitted work is expected to be commensurate with that level. To that end the grading of your projects and related work will be affected by: Spelling, Grammar, Punctuality, Demonstration of effort, Participation, and Academic honesty (See institutional policies link for more on this)

Unless otherwise noted, all written papers are required to conform to the APA style guidelines.

Grade of Incomplete

A grade of **Incomplete** may be granted only if it can be demonstrated that it would be unfair to hold a student to the normal time limits for the course. A Request for Grade of Incomplete Contract must be completed by both the student and the instructor and requires the approval of the appropriate division dean. The amount of time granted to

complete the Incomplete will be set by the instructor at the time the contract is submitted. Even though an instructor may require a student to repeat certain elements of a course to finish an **Incomplete**, students should not register for the course a second time.

A grade of **"I"** will remain on the record until a change of grade is submitted by the instructor. Completing requirements for a course does not remove the Incomplete from the record. The **"I"** remains a permanent part of the academic record and transcript so that the change from **Incomplete** to a grade can be clearly identified. An **Incomplete** may affect a student's financial aid. Please contact the Office of Financial Aid for more information.

Make-up Examinations

If a student is unable to take any scheduled examination, a make-up examination may be given at the discretion of the instructor. Such examinations must be taken during the same semester in which the examination was missed, unless a grade of Incomplete is given for sufficient reason.

Withdrawal

Students who withdraw from the college must notify the Office of the Registrar and the Office of Financial Aid. Withdrawal notification must be made in writing. Unless this is done, a student's grade for all current courses will automatically be an **"F"**, and he or she will not be eligible to receive a refund.

Students who withdraw from the college up to two weeks after the official midterm date of the term will receive grades of **"WD"** (withdrawn). Students who withdraw after that

date will receive grades of **"WF"**. Students may be placed on probation by the committee when they return, depending on the conditions surrounding their withdrawals.

Class Policies:

This is an accelerated eight week course of online learning. Students are expected to post assignments in a timely manner. For discussion threads students are expected to post substantive reactions to others at least three times each week during the discussion. Regular and timely posting is critical to both your learning and that of your fellow students. Specific instructions will be given for each discussion.

The three required posts must include at least 1 original post and 2 replies to other classmate's posts. In all cases, threaded discussion posts must be substantive, but not excessive. Simple "I agree with X" posts will not receive credit. You are expected to include details, opinions and thought provoking analysis of the topic. As a general rule, each post should be at least 2 sentences, but not more than 2 paragraphs.

Academic Honesty. Utica College expects students to adhere to the principles and policies of academic honesty articulated in its Policy on Academic Honesty published in the Graduate Catalog. While collaboration and discussion, both in class and online is encouraged, work submitted as an individual must be only the work of that student. Written or spoken assignments which have been previously prepared or presented for any reason must have instructor permission to be used in this class. Use of sources of information or the ideas of others must be properly cited and credited. Questions about the application of this expectation and policy should be directed to the instructor for

clarification in advance of submission of work. Violation of this policy is grounds for awarding an 'F' for the assignment and/or referral to the College for academic misconduct disciplinary review.

Intellectual honesty is necessary for the free exchange of ideas. Plagiarism, a serious form of intellectual dishonesty, is defined as the use of ideas and phrases in the writings of others as one's own without crediting the source. Sources can include books, papers written by anyone else, editorials, opinions, reference articles, or other media, including the Internet. Paraphrasing must be cited and credited as well. Credit must be given either internally in the text or in formal notes.

Cheating refers to both the giving and the receiving of unauthorized assistance in the taking of examinations. Students who assist other students in acts of plagiarism and/or cheating, or who otherwise contribute to acts of intellectual dishonesty, such as providing a term paper, lab report, or other assignment paper for unauthorized use, are subject to the appropriate penalties. Utica College faculty are authorized to assign the grade "F" for Cheating as a penalty for dishonesty in examinations or in the writing of themes, term papers, laboratory reports, or other assignments. Students who receive an "F" for cheating forfeit their right to withdraw without penalty. (The phrase "for Cheating" will be removed upon graduation at the student's request.) The vice president for academic affairs and dean of the faculty shall inform the student in writing of the professor's decision and of his or her right to a hearing before the Judicial Committee. Requests for a hearing should be made to the vice president for academic affairs and dean of the faculty. The vice president for academic affairs and dean of the faculty will refer any repeat offense to the

Academic Standards Committee, which may recommend a more severe penalty.

Software and Intellectual Rights

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is so volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments.

VIOLATIONS OF AUTHORIAL INTEGRITY, INCLUDING PLAGIARISM, INVASION OF PRIVACY, UNAUTHORIZED ACCESS, AND TRADE SECRET AND COPYRIGHT VIOLATIONS MAY BE GROUNDS FOR SANCTIONS AGAINST ANY MEMBER OF THE ACADEMIC COMMUNITY.

Non-Discrimination Policy

Utica College is an equal opportunity, affirmative action institution and accepts students and employs individuals without regard to race, creed, color, sex, ethnic or national origin, religion, marital status, age, sexual orientation, veteran status, or disability. This nondiscrimination policy covers admissions, employment, and access to and treatment in College programs, services, and activities.

Utica College welcomes the physically challenged, and in compliance with Section 504 of the Rehabilitation Act of 1973 (as amended) and the Americans with Disability Act of

1990 (ADA) does not discriminate on the basis of handicap. The coordinator of learning services coordinates the College's efforts to comply with the applicable law and regulations. The director of student development coordinates the College's academic support services to provide reasonable accommodations for students with disabilities.

Utica College also welcomes qualified disabled veterans and veterans of the Vietnam Era and, in compliance with section 402 of the Vietnam Era Veterans' Readjustment Assistance Act of 1974, does not discriminate against such individuals. The director of physical education and athletics coordinates the College's efforts to comply with the applicable law and regulations.

Utica College supports equal opportunity for both sexes and, in compliance with Title IX of the Education Amendments of 1972, does not discriminate on the basis of sex.

In accordance with federal law and regulations, this policy is subject to exceptions with regard to military programs. The College remains strongly opposed to legally discriminatory policies that are contrary to our core values, philosophy of inclusion, and Non-Discrimination Policy.

Questions about any of the College's affirmative action policies may be directed to the affirmative action officer in the Office of Human Resources, Utica College, 1600 Burrstone Road, Utica, New York 13502-4892, (315) 792-3276.

Weekly Schedule

	Topics	**Assignments**
Week 1	Introduction to network forensics and monitoring	Readings: • Chapter 1 and 2 -Tao of NSM • Networking refresher – UDP/TCP Discussion Topic: • Introduction to Telecommunications Hands-On Labs: • Fundamental Network Utilities
Week 2	Deployment of network traffic data collection technology	Readings: • Chapter 3 and 4 -Tao of NSM • A Summary of Network Traffic Monitoring and Analysis Techniques Hands-On Lab(s): • Network Stream Statistics
Week 3	Full content network traffic	Readings: • Chapter 5 and 6 - Tao of NSM • Quick and dirty packet capture data extraction Video: • Extract a file from HTTP stream using Wireshark Hands-on Lab(s): • Stream File Extraction
Week 4	Network session data	Readings: • Chapter 7 - Tao of NSM

		• Chapter 15 – Tao of NSM • Suggested: overview-session-hijacking-network-application-levels_1565 300 word abstracts for final report are due.
Week 5	Investigating client-server communications	Readings: • Presentation, IT IS, CH12 – V3 Discussion Topic: • Telecommunications and Cybercrime Hands-on Lab(s): • Data Exfiltration Lab
Week 6	Investigating peer-to-peer communications	Readings: • *Forensic Investigation of Peer-to-Peer File Sharing Networks.* DFRWS 2012. Hands-on Lab(s): • Peer-to-peer communications Lab
Week 7	Investigating Voice over IP (VoIP) communications	Readings: Deri, L., Open Source VoIP Traffic Monitoring Hands-on Lab(s): • VoIP Lab
Week 8	Final Report	A scoped and defined 1,500 word final report. Identify at least one IPV6 vulnerability, associated cybercrime and sources of evidence that could be forensically examined.

Appendix B - Course Labs

Fundamental Network Utilities

Objective: The objective of this lab is to develop an understanding of the fundamental tools that one has available to investigate and manipulate network communications. The tools also serve to reinforce the basics of network communications and functionality.

Setup

- Security Onion must be installed within an virtual environment
- Helpful Shortcuts
    - Within Linux terminal CTRL+SHIFT+T, will open a new terminal window
    - sudo is the command to obtain administrative privileges
    - CTRL-C kills a running command
- Once a command has been typed into the terminal, and is running in the foreground, you can no longer type commands into the terminal. It is necessary to open a new tab or kill the running process.

Procedure

1. **<u>Use Netcat to create a raw TCP connection – Similar to Chat</u>**

    1.1. Start a Netcat listening server

    ```
    1.1.1.    nc -l 45000
    ```

    1.2. Connect to the listening server with a Netcat client

    ```
    1.2.1.    nc localhost 45000
    ```

    1.3. Type text into each window similar to a chat session.

    1.4. Use CTRL-C to terminate one side of the Netcat, the other side should terminate as well.

2. Use Netcat to transfer a file

2.1. Objective: The objective of this lab is to experiment with transferring a file over the network using the Netcat tool. Netcat is a tool often used to make arbitrary TCP connections and allows for a lot of flexibility in its usage. Although we are doing this lab on a single computer system, these techniques would work amongst any two hosts with a network connection. The ports would most likely need to be changed to traverse firewalls, etc.

2.2. Create an file with your name in it, replace the *yourname* below with your actual name**:**

2.2.1. `echo yourname > my_file.txt`

2.3. Start a listening Netcat server and redirect input from the file

2.3.1. `nc –l 45000 < my_file.txt`

2.4. Connect to the Netcat server with a Netcat client connect and direct output to a new file

2.4.1. `nc localhost 45000 > my_xfer_file.txt`

2.5. Verify the MD5 sum of the transferred file.

2.5.1. `openssl md5 my_file.txt my_xfer_file.txt`

3. Network Grep

3.1. **Objective:** The objective of this experiment is to utilize the ngrep tool to monitor network traffic for a specific term. The ngrep tools will allow the investigator to easily extract a specific term from a unencrypted network communications stream.

3.2. **Run the command (replace yourname with yourname from sections 2.3 and 2.4):**

3.2.1. `sudo ngrep -d lo yourname -O yourname.pcap`

3.3. Repeat the sequence of steps in in 2.3 and 2.4 of this lab.

3.4. In the ngrep window type CTRL-C

3.5. Examine the yourname.pcap file with the command:

3.5.1. `wireshark yourname.pcap`

4. Use TCPKill to terminate at TCP connection

4.1. Objective: The objective of this experiment is to utilize the TCPKill command to terminate an active TCP connection. This will show how the TCP three-way hand shake can be exploited to kill an existing connection. Often attackers will use this type of technique to conduct session hijacking or force a reauthentication. For our TCP connection we will utilize the Netcat tool to create a raw TCP connection. This technique would work equally as well on any other TCP connection such as a web connection or email. Please follow the steps below:

4.2. From the Terminal start Wireshark

4.2.1. `sudo wireshark`

4.3. In Wireshark sniff the loopback interface (lo).

4.4. In Wireshark, in the Filter Box type the filter:

4.4.1. `ip.version == 4 && tcp.port == 45000`

4.5. Start a listening Netcat server

4.5.1. `nc -l 45000`

4.6. Connect to the Netcat server with a Netcat client connect

4.6.1. `nc localhost 45000`

4.7. On the Netcat client type some text and observe that it is sent over the TCP connection. The message sent should be viewable on both sides of the Netcat connection similar to a chat session. The message should also be viewable within the filtered packets in Wireshark. The packets observed should include the TCP Handshake and data packets.

4.8. Start the TCPKill Program

4.8.1. `sudo tcpkill -i lo port 45000`

4.9. Type text into either one of the Netcat Windows

4.9.1. What happens to the connection?

4.9.2. What new packet is observed when the tcpkill program is being run?

4.10. TCPKill Brute Force Flag:

4.10.1. Experiment with other variations of the "degree of brute force field" (read the man page via command `'man tcpkill'`) to determine how it effects the volume of packets sent to kill the connection.

4.10.2. Try to do a large file (MBs, etc.) transfer and experiment with the "degree of brute force" field. Does a large number of transfer packets impact the TCPKill capability? Try the run TCPKill on a TCP based video streaming connection.

5. Cryptcat

5.1. **Utilize the Cryptcat command to communicate and transfer a file.** Read the manual pages to determine how to use the command. Examine the communication in Wireshark and determine if you are able to view any cleartext traffic – why or why not? When a large volume of data is sent does Cryptcat appear to transmit uniformly sized packets? How might an attacker utilize a technique like Cryptcat to evade network security monitoring applications?

Wireshark Statistics Lab

Objective: The objective of this lab is to utilize the extended analysis techniques of Wireshark to obtain a statistical understanding of a network communications capture.

Questions:

- How many hosts are represented in the network packet capture?
- Identify ‘conversations’ between hosts. Examine protocols such as Ethernet, IP, UDP, and TCP communications.
- How much data was transferred between all communicating hosts?
- Provide a list of conversations sorted by the number of bytes transferred.
- Identify the relative time of major ‘burts’ of network traffic were transmitted. (ie- at 20 seconds the first burst of traffic occurred).

Procedure

1. Open the provided network capture in Wireshark
2. Utilize the Wireshark features under Statistics menu to answer the questions:
    a. Summary
    b. Protocol Hierarchy
    c. Conversations
    d. IO Graph

Data Extraction Utilities Lab

Objective: The objective of this lab is to identify and extract all of the files transferred within TCP and UDP streams of the provided packet capture.

Procedure

1. **Manually extract the Image from the Packet Capture file**

   1.1. Download the packet capture (pcap) file from Angel

   1.2. Using Wireshark, find the packet with an HTTP payload

   1.3. Once you identify the HTTP JPEG File Interchange Format payload, export that JPG data as a JPG image. Remember that a JPG has the characters JFIF early in the file format. You should be able to observe this pattern in the hex view once the packet is identified.

      1.3.1. When the bytes are selected – go to File->Export->Selected Bytes. This will allow you to save the packet bytes as a file.

      1.3.2. Once exported it should be possible to view the JPEG image.

   1.4. Calculate the MD5 for the extracted image using the OpenSSL command:

      1.4.1. `sudo openssl md5 <filename>`

   1.5. Report the MD5 and the picture contents within the Angel Assessment.

2. **Extract a file from a Network File System (NFS) stream**

   2.1. **Download the NFS packet capture file**

   http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=nfsv2.pcap.gz

   2.2. Use the filesnarf command to process the downloaded PCAP file and extract the transferred file. What does the file say?

3. **Automatically capture images traversing the network in real-time**

3.1. From the command line, run:

```
3.1.1.      sudo driftnet
```

3.2. A small window will pop-up with a black background. See Figure 3.

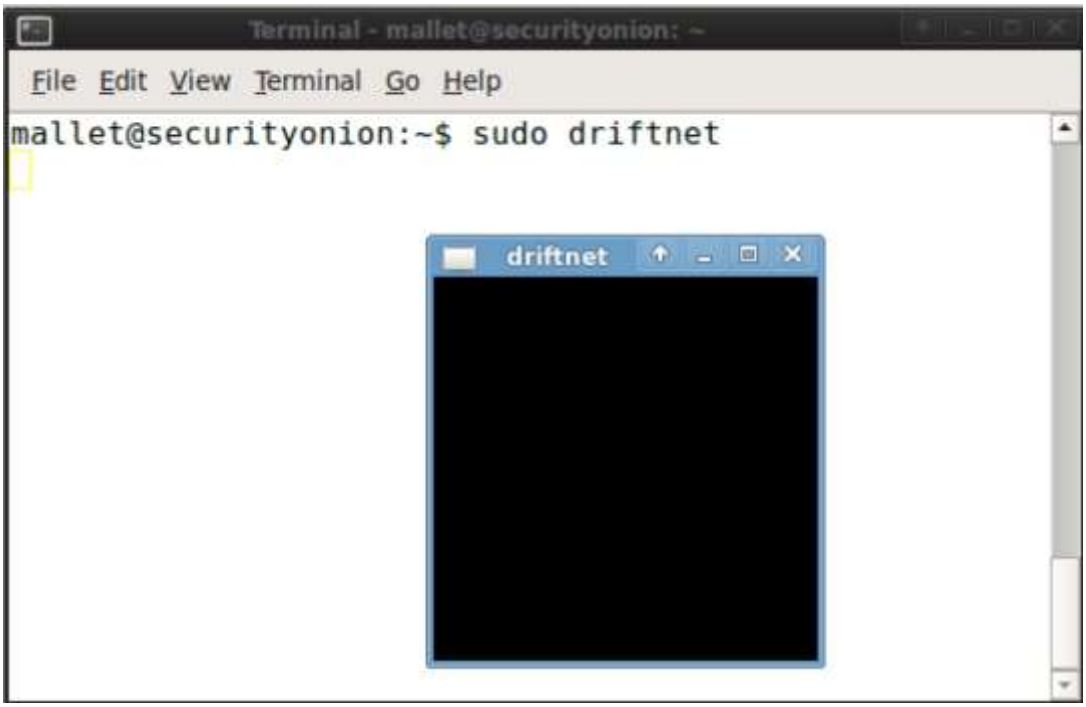

Figure 3 - Driftnet initialization

3.3. Open a web browser and in Google search for the term ‘beagles’

3.4. Report what is observed within the Driftnet window. Discuss how this could be used as a monitoring device. Discuss privacy issues. Discuss how an attacker would evade such a monitoring system.

3.5. Experiment accessing other pages such as cnn.com or Google news. Notice that the images on the page appear within Driftnet.

4. Manually examine traffic flows from a offline packet capture file

4.1. Convert the http.pcap file to an argus file

```
4.1.1.      argus –r http.pcap –w http.argus
```

4.2. Analyze the argus file to show traffc traffic flows

4.2.1. `ra –r http.argus - tcp`

4.3. Note that the output from the ra command is line delimited and that singles lines may span multiple terminal lines depending on your Security Onion display resolution.

4.4. Report the connection line where the most data was transferred.

5. <u>Examine network traffic characteristics in real-time using EtherApe</u>

5.1. From the command line, run:

5.1.1. `sudo etherape`

5.1.2. A user interface will pop-up with a blank black screen. Network traffic will be displayed as lines between nodes. The width of the line loosely represents the amount of traffic flowing between nodes.

5.1.3. Conduct the following experiments and report how the display changes. It will be necessary to stop and restart the EtherApe display between each test to ensure only the traffic within the display is represented by the test being run. Because EtherApe displays network activity in real-time it will be necessary to position windows within the Security Onion display so that EtherApe can be viewed while the test is being conducted. When observing EtherApe Consider the number of nodes within the display, general line width, etc.

5.1.3.1. ping an Internet host IP address such as 8.8.8.8

5.1.3.2. ping an Internet web domain such as www.utica.edu

5.1.3.3. traceroute to IP address such as 8.8.8.8

5.1.3.4. Browse to youtube.com. Security Onion does not have the necessary plugins to view a video, but it will still be possible to observe network activity within EtherApe.

Data Exfiltration Lab

Objective: The objective of this lab is to run a network exfiltration tunnel over the DNS protocol and then explore methods to detect and prevent tunneling.

Procedure

1. **Install the Iodine DNS tunnel application**

   1.1. Note: the Security Onion virtual machine must have Internet access to install software

   1.2. `sudo apt-get install iodine`

2. **Check the IP address of the Security Onion virtual machine**

   2.1. `ifconfig`

   2.2. Make note of the IP address for the eth0 interface

   2.3. This is the IP address of the actual host on the network and the address is not related to the DNS tunnel. This address should not be used for communicating over the DNS tunnel.

3. **Start the Iodine DNS Server Tunnel application**

   3.1. `sudo iodined –fP password 10.10.10.85 mydomain.asdf`

   3.2. In the above example, the 10.10.10.85 IP address is an address that is unique to the DNS tunnel. This should be a “fake” or non-existent IP address that will be utilized only for the purposes of addressing hosts on within the tunnel. All communications using this IP address space will be transferred by the DNS tunnel.

   3.3. You should observe the following output:

```
Opened dns0
Setting IP of dns0 to 10.10.10.85
Setting MTU of dns0 to 1200
Opened UDP socket Listening to dns for domain test.asdf
```

4. **Start the Iodine DNS Client Tunnel application**

4.1. `sudo iodine -fP password <ip_address> mydomain.asdf`

4.2. **Note:** in the above command, the field `<ip_address>`, must be replaced with the IP address you identified in step 2.1.

4.3. You should observe the following output after running the Iodine client:

```
Opened dns1
Opened UDP socket Version ok, both using protocol v 0x00000500.
You are user #0
Setting IP of dns1 to 10.10.10.65
Setting MTU of dns1 to 1200
Switching to Base64 codec
Server switched to codec Base64
Autoprobing max downstream fragment size... (skip with -m
fragsize) 768 ok.. 1152 ok.. 1344 ok.. 1440 ok.. 1488 ok.. 1512
ok.. 1524 ok.. will use 1524
Setting downstream fragment size to max 1524...
Sending queries for mydomain.asdf to 192.168.1.112
```

5. **Examine network interfaces**

5.1. Run: `ifconfig –s`

5.2. If the tunnel is running properly, you should see a `dns0` and `dns1` interface as well as the default `eth0` and `lo`

5.3. Upload your output to the Angel shell. Be sure that both the `dns0` and `dns1` interfaces exist. If they do not exist the tunnel may not be running properly.

6. **Start Wireshark**

6.1. In a dedicated Terminal window type:

6.1.1. `sudo wireshark`

6.1.2. Type your password when prompted

6.1.3. **Note:** if you kill this terminal window you will kill the Wireshark process

6.2. Begin sniffing on the 'lo' interface

6.3. Add a filter of 'dns' and click 'Apply'. The DNS filter will show all DNS packets and ultimately all traffic that is serving to create the DNS tunnel. It will not be possible to make much sense out of the DNS traffic in Wireshark.

7. Use the DNS tunnel - Ping to test communication

7.1. Ping the DNS tunnel server by typing:

7.1.1. `ping 10.10.10.85`

7.1.2. **Note:** the server that you ping should match the IP address used to setup the tunnel in step 3.1.

8. **Stop Wireshark**

8.1. Examine the DNS packets collected while the DNS tunnel is running.

8.2. Save only the DNS tunnel packets. Be sure that the DNS filter is still applied and that only DNS tunnel packets are displayed in the Wireshark interface. In the save dialog box, be sure to click Displayed.

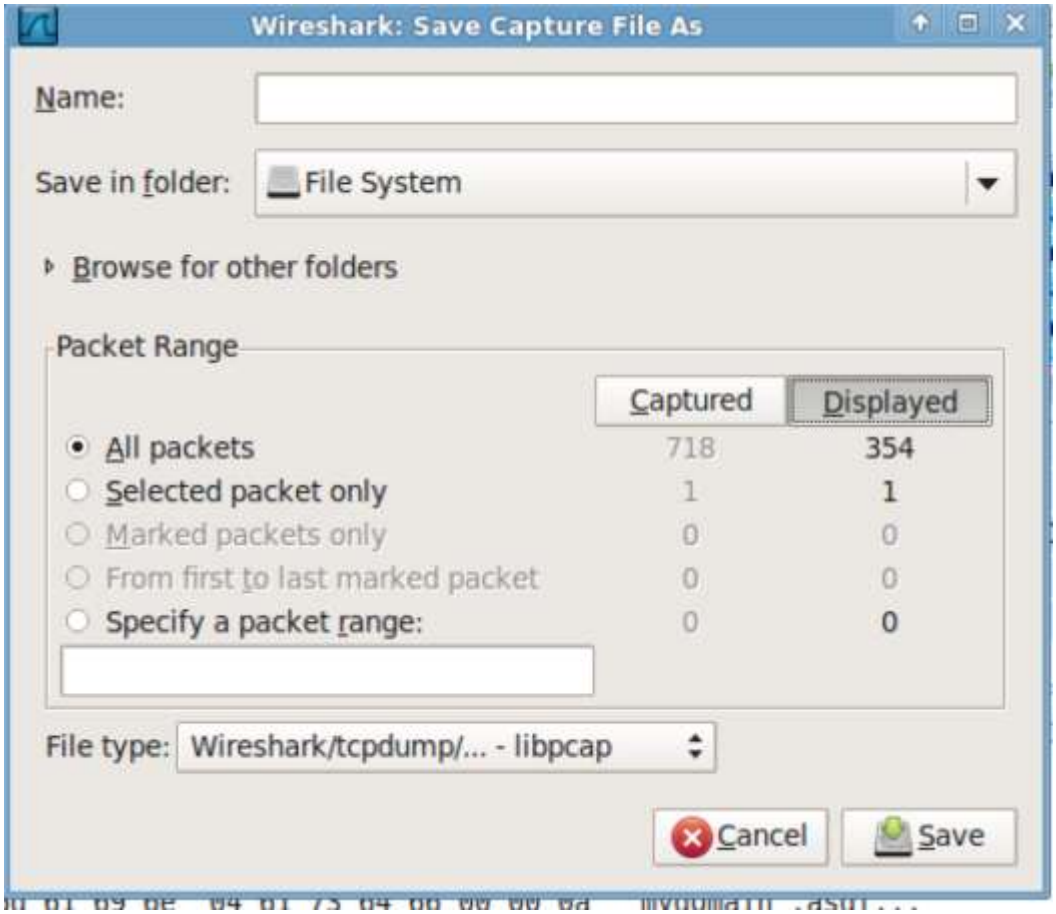

Figure 4 - Wireshark - save only displayed packets

1.1. Upload the filtered DNS tunnel packets to the Assignment dropbox.

1.2. After saving the packets collected while the DNS tunnel was running, restart Wireshark on the eth0 interface and connect to Google with a web browser. Examine the initial DNS packets to lookup Google.com. How do the DNS packets for Google look different than the DNS packets in the DNS tunnel? Report your answer in the Angel assessment.

2. <u>Use the DNS tunnel – Netcat</u>

2.1. Use netcat to communicate over the tunnel. You will need both a netcat listener and client. Be sure that you are communicating over the tunnel and not on the regular network. The IP addresses used with netcat should be the addresses

Peer-to-peer Lab

Objective: The objective of this lab is to provide hands on experience examining the traffic of peer-to-peer communications traffic.

VoIP Lab

Objective: The objective of this lab is to identify and gain hands-on experience with the technologies and techniques used to analyze VoIP communications.

Appendix C - Weekly Reading Assignments

Long, B., (n.d.). Chapter 12, E-mail Investigations. IT IS 4250 Computer Forensics. Retrieved October 29, 2012 from http://coitweb.uncc.edu/~nblong/ITIS%204250/Lectures/Ver_3/Ch12-V3.ppt

Bejtlich, R. (2005). The Tao of Network Security Monitoring: Beyond Intrusion Detection. Pearson Education, Inc. ISBN 0-321-24677-2 (pbk.)

Cecil, A. (n.d.). A Summary of Network Traffic Monitoring and Analysis Techniques. Retrieved October 29, 2012 from http://www.cse.wustl.edu/~jain/cse567-06/net_monitoring.htm

Deri, L. (n.d.) Open Source VoIP Traffic Monitoring. Retrieved October 29, 2012 from http://luca.ntop.org/VoIP.pdf

Erdely, R., Kerle, T., Levine, B., Liberatore, M., Shields, C. (2010). Forensic investigation of peer-to-peer file sharing networks. Retrieved on October 29, 2012 from http://www.dfrws.org/2010/proceedings/2010-311.pdf

Fiedler, G. (2008). UDP vs. TCP. Retrieved October 29, 2012 from http://gafferongames.com/networking-for-game-programmers/udp-vs-tcp/

Jlgaddis. (2009). Extract PDF File from HTTP steam using Wireshark. Retrieved October 29, 2012 from http://www.youtube.com/watch?v=GwAxzXSssz8 [Video]

Lin, M. (2005). An Overview of Session Hijacking at the Network and Application Levels. SANS Institute InfoSec Reading Room. Retrieved October 29, 2012 from http://www.sans.org/reading_room/whitepapers/ecommerce/overview-session-hijacking-network-application-levels_1565

Stretch, J. (2009). Quick and dirty packet capture data extraction. Retrieved October 29, 2012 from http://packetlife.net/blog/2009/jul/13/quick-packet-capture-data-extraction/

Appendix D - Discussion Assignments

Topic 1 – Introduction to Telecommunications Forensics

The term "telecommunication" can be summarized as the communication of information through the use of some medium. Because the medium is not defined and can range from smoke signals to cellular transmissions, we must first scope the term for the purposes of this class. To properly scope the term, we will only consider those mediums that are commonly used or emerging within the 21st century.

For this discussion, we will focus on the term forensics and it's applicability to specific telecommunication mediums. Students are expected to identify a specific 21st century telecommunication medium and identify storage abilities and locations within that medium that may store digital data of interest. Additionally, please identify any tools, techniques or methodologies that currently exist to extract and analyze such data.

Topic 2 – Telecommunications and Cybercrime

Society utilizes many forms of telecommunications as a means to accomplish various tasks. As we know, this utilization is a dependency and without it, progress would be difficult to achieve. The commission of many crimes (not just cyber) is often dependent on the utilization of telecommunications.

For this weeks' discussion, students are expected to identify cybercrimes that made news in recent years and encompassed a specific telecommunication medium(s). Students are expected to summarize the identified cybercrime, the purpose and methods/exploits utilized by the criminal

and/or attackers, the telecommunication medium(s) utilized and/or targeted and a summary of the investigative techniques utilized.