2009

The Enhancement of Graduate Digital Forensics Education via the DC3 Digital Forensics Challenge

Timothy H. Lacey
Air Force Institute of Technology

Gilbert L. Peterson
Air Force Institute of Technology

Robert F. Mills
Air Force Institute of Technology

Recommended Citation

T. H. Lacey, G. L. Peterson and R. F. Mills, "The Enhancement of Graduate Digital Forensics Education via the DC3 Digital Forensics Challenge," 2009 42nd Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 2009, pp. 1-9, doi: 10.1109/HICSS.2009.433.

The Enhancement of Graduate Digital Forensics Education via the DC3 Digital Forensics Challenge

Timothy H. Lacey, Gilbert L. Peterson, Robert F. Mills
Air Force Institute of Technology, Wright-Patterson AFB OH
{Timothy.Lacey, Gilbert.Peterson, Robert.Mills}@afit.edu

Abstract

This paper describes supplementing the digital forensics course at the Air Force Institute of Technology (AFIT) with the highly-successful DoD Cyber Crime Center (DC3) Digital Forensics Challenge. The DC3 Digital Forensics Challenge consists of several difficult digital forensic tasks. The knowledge and skills required to complete these tasks often resides outside of the material presented in a graduate digital forensics course. By utilizing concepts taught in AFIT's digital forensics course, a team of four graduate students won the 2007 competition. In this paper, we explain how our team used forensically sound principles learned in class, reinforcing the class concepts, coupled with old-fashioned hard work to successfully complete the challenge.

1. Introduction

The digital forensics course at AFIT is currently in its fifth year of existence. Enrollment is strong as this is one of the most desired courses we offer. The course is part of three different Masters of Science degree programs: Cyber Operations, Computer Science, and Computer Engineering. The digital forensics course is tightly integrated with our other computer security courses. The techniques that the students learn build on experiences from the Cyber Defense Exercise (CDX), an inter-service competition, in which the students administer a network and defend it against Red Team attacks for a week. One component of defending the network is that during the CDX students must determine what fails and how to rectify the situation after an attack. In the cyber forensics course, one fourth of the course is spent on live network response. This exposes students to the tools needed when faced with these situations in the future.

The Department of Defense (DoD) Cyber Crime Center (DC3) Digital Forensic Challenge [1] is a competition that encourages technological innovation from pioneers in the digital forensics community. The contest presents several scenarios covering a variety of current digital forensic problems and trends. Like the CDX, the DC3 challenge requires hands-on work by the students. We have found that it is the hands-on reinforcement of concepts taught in class that grounds the students' learning experience [2].

The tasks in the DC3 Digital Forensics Challenge provide the students with a set of technical challenges that the DC3 feels are, or will be, important in the future of digital forensics. This is important as it provides the students ideas on where the field may be heading in the future. These technical challenges also build on the policy, technical, and engineering skills that they develop and use in the existing digital forensics course and lab curriculum.

To best understand how the DC3 Digital Forensics Challenge can be used in a digital forensics course, background on digital forensics and on our course is discussed. From this background information, the tasks in the 2007 DC3 Digital Forensics Challenge are presented with discussion on how they are grounded in the course. One of the important items to note is that although different tasks make use of different course components, the one component that extends across all of the tasks is the ability to express the policy and process to be followed to maintain the integrity of the evidence.

2. Background

Information technology and cyberspace represent a double-edged sword: on one hand, they enable us to do things that were not possible before; on the other hand, we have reached a point where many things that we take for granted (banking, telephony, air-traffic control, energy, and health care) are completely dependent on cyberspace. The U.S. Air Force recognizes the significant impact of this new domain and recently added "Cyberspace" to its mission statement [3]. Education and training will play a pivotal role in creating cyber warriors to support this

new mission. Exercises and simulations also provide opportunities for students to present innovative solutions to existing problems in forensics. Two examples include the National Security Agency (NSA) sponsored CDX and the annual DoD sponsored DC3 Digital Forensic Challenge [4, 5].

2.1. Digital Forensics

Digital media has become an integral part of our lives, from leisure and entertainment, to business. Digital media is used for numerous legitimate purposes, but unfortunately it is also used for criminal activities. Therefore, it is very important that the science of digital forensics be addressed as a profession, requiring specialized training and education to handle the myriad of scenarios an examiner will encounter. Digital forensics is "… the application of science and technology to the identification, recovery, transportation, and storage of digital evidence [6]." Digital evidence, much like definitions of cyberspace, encompass a large domain, including computers, computer networks, all types of storage devices, and all types of digital hardware, from iPods to Tivos.

It is not difficult to recognize that a broad range of skills is required by the forensic examiner. Training in basic digital forensics and incident response on Internet Protocol (IP) based systems builds the foundational skill set that can then be extended to multiple disciplines. However, this expertise must extend from IP based networks into more diverse applications such as telephony, Supervisory Control And Data Acquisition (SCADA), and Command and Control systems. The next section describes how our cyber forensics course addresses these concerns.

2.2. AFIT's Cyber Forensics Course

To gain a working insight into an approach for teaching digital forensics, an acceptable model for process breakdown needs to be identified. Several publications consider the roles of the digital forensic scientist consist of preservation, collection, examination, and analysis [7-12]. Although there are a number of different ways to teach a digital forensics course, we have adopted an approach that breaks the material into five areas: Ethics and Legal Procedures, Basic Forensic Science, Media Capture and Analysis, Network Forensics, and Digital Device Analysis. Table 1 shows the percentage of course time spent within each of the five topic areas.

Table 1. Digital Forensics Course Material Breakdown

Course Subject Area	Percentage of Course
Ethics and Legal Procedures	10
Basic Forensic Science	10
Media Capture and Analysis	40
Network Forensics	25
Digital Device Analysis	15

The *Ethics and Legal Procedures* subject area includes material on ethical behavior as it relates to computer usage. We discuss where individuals learn computer ethics (at home, school, and/or from the community) and how ethical behavior translates into a networked environment. The digital forensics side of these issues emphasizes the criminal mind and how some individuals reject ethics. The legal procedures then address the definition of cyber crime, concerns about search and seizure rights, the Fourth Amendment, and the large base of legal precedent being developed. This also extends into the question of the validity of analysis tools. That is, what are the standards, practices and/or precedence for use that must take place prior to a tool being "validated" and its results admissible in a court of law? An excellent introduction of these topics can be found in Casey's book, *Digital Evidence and Computer Crime* [13].

For use during the labs, students are issued their own hard drive for imaging, analysis, and retention of chain-of-evidence. The machines the students use all run *Windows XP* with Service Pack 2. The software is a mixture of freeware and commercial. We use *Helix*, and *Penguin Sleuth* bootable CDs, both of which include the *dcfldd* imaging tool and the *Autopsy* analysis tool suite. The commercial tools range from the forensics professional version of *Winhex*, which allows the students the lowest level view of the media, to *EnCase* and *Forensic Tool Kit* (FTK) which provide a Graphical User Interface (GUI) with advanced recovery and analysis tools.

In the first lab, *Policy Creation*, students develop a first responder's policy for search and seizure. An added twist that starts the students thinking about the different situations that could confront them is that each team must use another team's policy when conducting the second lab, First Response.

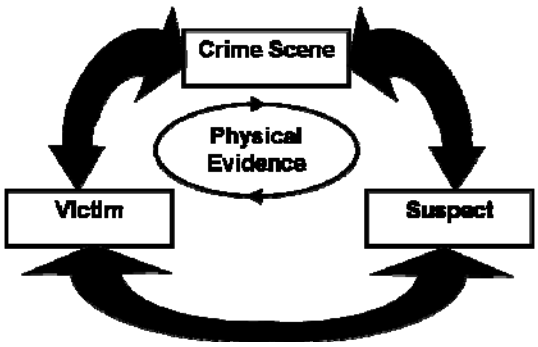

Figure 1. Locard's Principle

Basic Forensic Science is concerned with both the law enforcement view of forensics as well as general lab policies. Some of these topics include: Locard's Principle (Figure 1); Inman & Rudin Forensic Science Paradigm; what can and should be seized at a crime scene; what needs to be included in a warrant's text to ensure that the seizure is legal; once items are seized what happens with them; and how are items handled in the lab. Some of these questions are addressed via a general overview and guide by the Department of Justice (DOJ) on Search and Seizure of digital media [14]. The American Society of Crime Laboratory Directors (ASCLD) has provided a means by which forensics and digital forensics labs can be certified, and this is discussed as well [15].

As previously documented, in the *First Response* lab students follow a policy they have not written themselves. This technique offers a different view on the search and seizure procedure. Additionally, the students are responsible for other items present at the scene. We incorporate numerous characters from the game of Clue by Milton Bradley to add an element of intrigue. In this lab, students look for information on who killed Mr. Boddy. They must locate and seize all media and other physical evidence related to this fictitious case. Figure 2 is a crime scene sketch indicating a typical setup for this lab. After locating the evidence and creating a crime scene sketch, students must tag, photograph, and retain the evidence for their chain of custody documentation.

The correct and accurate handling of media is taught in *Media Capture and Analysis*. The classroom instruction includes proper techniques for acquiring and verifying an image of storage media and analyzing the media's physical and logical structure to extract evidence. Addressing some of the most difficult problems that forensics investigators encounter, the data analysis portion investigates information hiding in the logical structure of the media and in the network traffic itself. This includes such topics as steganalysis, Domain Name Service (DNS) messaging, document metadata, and encryption.

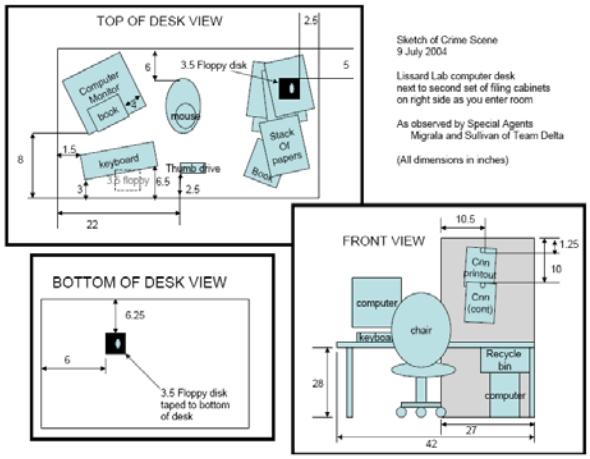

Figure 2. Lab 2 Setup and Crime Scene Sketch.

Students encounter a live network in the third lab, *Live Response*. In this lab, the networked machine must remain on and the students must determine what has gone wrong, gathering information without loss of service. Specifically, the students must open a secure command line interface and create a network connection to a machine used for analysis. The students must gather as much volatile information from the machine as possible. They also transfer non-volatile information such as logs, registry keys, and anything else they feel is relevant. This lab focuses on having the students detect issues with the computer itself rather than as a part of a network. Specifically, we have installed various Trojans, viruses, and rootkits that the students are responsible for locating.

In the fourth lab, *Password Cracking*, students are locked out of the victim machine, which has been turned off. They must then gain reentry by circumventing the computer's security, including defeating both the Basic Input Output System (BIOS) and login passwords. When circumventing the computer's security, students must inflict the least amount of evidentiary harm. During lectures, we demonstrate how the BIOS and the Power On Self Test (POST) function. We also demonstrate the mechanisms available to bypass user and administrator BIOS passwords. As for the OS on the computer, we discuss the Windows XP authentication mechanism and the different methods available to bypass it. We've found the most successful of the different methods used has been for the students to utilize *pwdump* during the live response and capture the Windows password hashes prior to this lab.

Network Forensics investigates the situation from a network standpoint. When viewed from this perspective, evidence can be contained within network log files. Questions are raised about the type of logging information available and how from these logs additional information about the network traffic can be extracted.

In the fifth lab, *Network Log Analysis*, students analyze two days of network capture logs and track individuals attacking the system as far away as their Internet Service Provider (ISP). We use the dataset that students capture during the CDX. This dataset provides a rich and realistic environment for forensics analysis, and draws from the students experience during the CDX as well. Only two day's worth of network traffic are analyzed because of the sheer amount of data. The lab requires the students to use multiple tools to prune the search space before performing a packet by packet analysis to track down the exact attack and exploit packets. The commonly used toolset consists of *Snort* [16], *WireShark* [17], and *EagleX* [18].

Digital Device Analysis looks at all of the disparate devices that may confront investigators. In our course, we look at the storage and extraction of information from Universal Serial Bus (USB) flash drives and Moving Picture Experts Group version 3 (MP3) players, and introduce the topic of mobile phone forensics, but, not to the detail level of media and data analysis.

Dr. Boddy is scrutinized in the sixth lab, *Imaging a Drive*. Here, students seize the victim's machine and image the hard drive. After completing this lab, the students' all-encompassing seventh lab, *Hard Drive Analysis*, requires them to perform the entire process. Students enter a new crime scene, perform a first response, seize all evidence in the area, and image and analyze the drive and the file system for hidden information.

Additionally, the students have a final project. The tasks of the final project, build on the information and labs conducted during the course. The students select topics of difficulty comparable to those of the DC3 competition. The advantage of the DC3 competition for our course is that it provides the students with real world problems to attempt solving.

Any introductory course in digital forensics should address all of these topics. The depth to which each is covered can vary depending on the program. The text that we use for the course is Mandia and Prosise's *Incident Response and Computer Forensics, 2nd Edition* [19], supplemented with several documents on best practices and search and seizure, and course notes. For search and seizure best practices, we make use of the National Institute of Justice's "Electronic Crime Scene Investigation: A Guide for First Responders" [20], and also the Air Force Office of Special Investigations Crime Scene Training Manual [21].

3. 2007 DC3 Challenges

As stated in the introduction, the DC3 Digital Forensic Challenge is a competition that encourages technological innovation in the digital forensics' community and recognizes new investigative tools, techniques and methodologies. Solutions are sought to assist in ongoing investigations and law enforcement communities around the nation. Only the first one hundred teams that actually submit solutions are eligible to compete but there is no limit to the number of teams that can request the challenge package. Each team, consisting of no more than four members, must complete the DC3 challenge application. Individuals may also participate but their eligibility is limited to one team only. Anyone can participate in the challenge but only U.S. citizens can attend the DoD Cyber Crime Conference which is held in St. Louis, Missouri. This is an annual event that is conducted in January of the following year.

The participants of the challenge face several scenarios covering a variety of current digital forensic problems and trends which assist in law enforcement investigations and also enhance national computer forensic techniques. A few of the challenges include issues related to encryption, data recovery, image analysis, and steganography. Teams are required to submit their solutions using a standardized form and their "game clock" ends when their solution is received, so everyone has the benefit of the same start time. Teams submit a copy of each proprietary tool used to recover the data, but they retain their rights to those tools. The winning team receives an award for their achievement along with a trip to the DoD Cyber Crime Conference in order to be formally recognized for their innovative solution. The trip includes fees for the conference admission, government per diem (which will cover the team travel, accommodations, and food), as well as public recognition at the conference. The following sub-sections describe each of the challenges for the 2007 competition and the amount of weighted points awarded for each challenge. This information is taken from the challenge instructions distributed by DC3.

3.1 Audio Steganography – 3000 Points

For files that contain steganography, identify the program used to hide the data and then extract and decrypt the hidden data.

3.2 Password Cracking – 2750 Points

Examiners must develop and document a methodology used to determine the password for each file. Points will be awarded for each successfully accomplished task.

3.3 PAX Cracking – 2750 Points

Open and view the two Pick Ax (PAX) encrypted files and read the message inside.

3.4 BitLocker Encryption Cracking – 5000 Points

Examiners must develop and document a methodology used to discover the payload of the BitLocker encrypted partition image located on the Challenge Digital Video Disk (DVD). Examiners will be expected to identify the individual files and folders contained within the image, as well as the data results contained therein.

3.5 Image Analysis: Real vs. CG – 1050 Points

Examiners must develop and document a methodology used to determine whether the images on the Image Analysis folder are Computer Generated (CG) or real. Examiners will be expected to identify the nature of each picture.

3.6 Image Analysis: Manipulated Images – 1000 Points

Examiners must develop and document a methodology used to determine the steps taken to manipulate each image in the Manipulated Images folder. Examiners have to break down each individual action or function that has been performed on each image in the order that it was executed.

3.7 Damaged Media #1 – 1500 Points

Examiners must develop and document a methodology used to recover data from a damaged DVD. Examiners will be expected to recover a piece of known data from the DVD. Points will be awarded for successfully extracting data from the DVD.

3.8 Damaged Media #2 – 2000 Points

Examiners must develop and document a methodology used to recover data from a piece of a Compact Disk (CD). Examiners will be expected to recover a piece of known data from the CD. Points will be awarded for successfully extracting data from the CD.

3.9 Damaged Media #3 – 3000 Points

Examiners must develop and document a methodology used to recover data from an erased Compact Disk – Read/Write (CD-RW). Examiners will be expected to recover a piece of known data from the CD-RW. Points will be awarded for successfully extracting data from the CD-RW.

3.10 Damaged Media #4 – 5000 Points

Examiners must develop and document a methodology used to recover data from a broken and erased CD-RW. Examiners will be expected to recover a piece of known data from the CD-RW. Points will be awarded for successfully extracting data from the CD-RW.

3.11 Damaged Media #5 – 1000 Points

Examiners must develop and document a methodology used to recover data from a scratched DVD. Examiners will be expected to recover a piece of known data from the DVD. Points will be awarded for successfully extracting data from the DVD.

3.12 Damaged USB Thumb Drive – 2000 Points

Examiners must develop and document a methodology used to recover data from a damaged Universal Serial Bus (USB) thumb drive. Examiners will be expected to recover a piece of known data from the thumb drive. Points will be awarded for successfully extracting data from the thumb drive and documenting the process.

4. Cyber Warrior's Challenge Results

Even though the labs in the digital forensics course are difficult, the challenges from the DC3 competition

are even more so. In this section, we describe the actions performed by our team to solve three of the problems, password cracking, damaged USB thumb drive, and damaged media. Although every student in the digital forensics course had the opportunity to compete in the DC3 competition, only one team submitted solutions.

As a forensic challenge, answers must have enough detail to satisfy questioning in a court of law. Although taught in class lectures, chain-of-custody issues were not a part of this challenge. DC3 instructions stated that examiner's solutions must include a meticulously detailed explanation of the steps taken to complete the challenge, to include tools and techniques used, that reviewers could follow to reproduce the examiner's work and check for authenticity.

4.1 Password cracking

The password cracking challenge was to find the open/modify password for a Microsoft *Word* document burned to a DVD. Three files (one *Word* document and two archived files) were provided as part of this challenge. The students first tried to determine the complexity of the password. A sample directional worksheet provided by DC3 listed a dummy file with its password consisting of 18 characters and a character set that included upper case, lower case, numbers, and special characters. If this was any indication of the password on the Microsoft Word document, the students were looking at cracking a password with a character set of at least 94 characters. A password of this length and complexity could not be brute-force cracked inside of several hundred years. Therefore, another means of finding the password was attempted.

The students first tried to open the *Word* document with the Windows *WordPad* application. If *WordPad* could interpret the document, it would be easier to debug than if opened with *Word* because the linked libraries for *WordPad* is much smaller than those for *Word*. Unfortunately, *WordPad* could not read the file. The students next used the Linux utility "strings" on the *Word* document to pull out any interesting text. The results of this utility were saved to a file and would be used later (futile as it might be) in a brute-force cracking attempt. The students then ran the *Word* document through a file identifier program called *Trid*. It reported the document as a *Word* document [22].

The students next tried to exploit a flaw in Microsoft *Word* and *Excel* where two documents encrypted by the same algorithm with the same key length are saved with any modification between the two documents [23]. The flaw occurs when an encrypted document gets modified and saved, but the initialization vector remains the same. With the initialization vector remaining the same, it is the only thing that remains the same between the two encrypted documents. When the documents are XORed together, the initialization vector drops out. Unfortunately, the documents provided by DC3 were exactly the same, so this particular attack would not work. Alas, the students succumbed to attempting a brute-force attack using a high performance cluster that was unsuccessful in identifying the password in the allotted time.

Even though the students did not find the password to open/modify the *Word* document, their efforts were dutifully recorded and they earned points for that. More importantly, this challenge built upon and extended several of the skills taught in class such as analysis of encryption techniques, reading of binary data, bypassing security mechanisms, identifying differences in system files, and password cracking.

4.2 Damaged USB Thumb Drive

This challenge was nicknamed "Sizzling Thumb Drive." This name led our team to believe the device had an excessive amount of voltage applied to it. An investigation into the design of a USB device and knowledge of direct hardware interfacing played a role in the completion of this challenge.

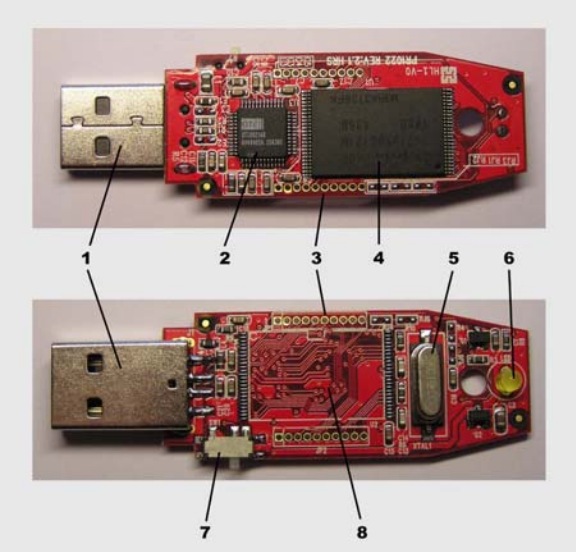

Figure 2: USB Flash Device Components.

The process of extracting data started with an examination of similar devices and studying available online materials on the subject. Matching device serial numbers with a particular vendor provided a datasheet

of the timing, communication, and pinout of the USB device. The students decided there were three options for reading the information off the chip: 1) Extract the chip completely and utilize a flash test device to read it, 2) Keep the chip in place and jump all the pins to a similar device, and 3) Keep the chip in place and attempt to interface directly with additional hardware. Initially, complete removal of the chip was considered the most viable option, but it had the risk of damaging the device. The data medium was a small integrated circuit that may have been destroyed in the process and would have proven difficult to replicate easily for the judges. Keeping the chip in place bypassed extensive soldering that the first option required, and represents little risk to the device itself. Thus, jumping all pins to a similar device became the attempt to extract the flash drive's information.

The first step in removing the data from the USB device is an examination of the interior structure and components. A typical USB flash drive contains the following parts as illustrated in Figure 2: 1) USB connector, 2) USB mass storage controller device, 3) Test points, 4) Flash memory chip, 5) Crystal oscillator, 6) LED, 7) Write-protect switch, and 8) Space for second flash memory chip.

Figure 3: Severely damaged DVD disk

Physical inspection of the USB connector revealed no visible damage or electrical shorting. An excessive voltage would not likely destroy the flash memory chip as the controller chip is logically between the connector and the storage medium. Besides, the object was to recover the data from the device and this would not have been possible if the flash chip was damaged. Therefore, our team attempted to link together the control logic from a known good device with the data chip on the damaged device.

After opening the case of the USB device, our team discovered the flash drive was based upon a Hynix flash chip, part number HY27UF081G2M. An online search revealed a data sheet with all required interfacing data. The signaling of our damaged device was extremely similar to a SmartMedia storage device. The plan was to attach the appropriate lines between the flash chip connected with via a Thin Small Outline Packages (TSOP) clip and a SmartMedia storage reader and get a direct read of the flash memory.

Though the plan was feasible, it was not successful. The software required to read the flash media did not operate properly. It appeared the software could "see" the chip, but could not correctly interpret the data. Once again, our team did not fully complete the challenge. But, what they did accomplish was forensically sound and, with the proper software interface, should have been able to read the data from the damaged USB device. This particular challenge was very difficult and required extensive knowledge of hardware. Additionally, skills learned in class such as protection of magnetic media and readings of binary data from magnetic media were valuable in the completion of this challenge.

4.3 Damaged Media #5

The damaged media challenge contained two tasks: 1) Develop and document a methodology used to recover data from a severely scratched DVD, and 2) recover any data possible from the DVD. Figure 3 is a photo of the disk that was to be analyzed. The disk contained several heavy scratches that prevented it from being read in a normal DVD reader.

The team was able to determine that the damaged disk was a DVD+R, 8X disk. As Figure 4 illustrates, a DVD+R is made up of four layers: 1) graphics, 2) polycarbonate disc, 3) reflective layer, and 4) 2nd polycarbonate disc. The polycarbonate disks not only protect the reflective layer, but also help to focus the laser. On the underside of the disk is an empty center, then a clear area, followed by a silver area. These areas are used to support the disk on the drive. Outside the silver area is a blue area known as the Burst Cutting Area (BCA). Though rarely used, this area is a permanent ring of information burned by the DVD manufacturer. It holds such data as the unique disk identification and manufacturer information.

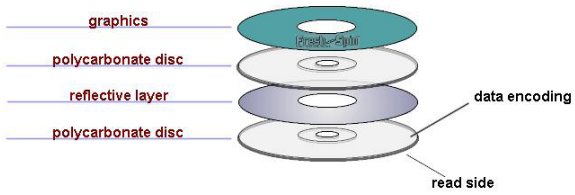

Figure 4: DVD+R layers

When burning a session onto a DVD, the session begins just outside the BCA on the disk. A DVD+R can contain multiple sessions, and each session has a lead-in, a data area, and a lead-out. In multi-session disks, the lead-in zone contains addresses of the subsequent sessions. Furthermore, a session can contain multiple tracks. A track is a break in contiguous sectors for the purpose of changing from one track to the next. This is usually done to allow a player to distinguish between songs, or in the case of a DVD, between videos. The data zone can have 1 to 99 tracks. Our DVD only had one track.

The lead-in zone consists of the Table of Contents (TOC) for the session and includes information about the session: the starting and ending addresses for the tracks within the session. If the session has not been closed or the disk is not full, then the TOC also contains the next available address for the start of the next session. The TOC starts at physical sector 0 and, for our DVD, only contained information for one session and one track. Outside the BCA blue area is the shiny lead-in area. Just outside of that is a dull brown area known as the data zone. Outside of the data zone is the lead-out area. It is not written until the session is closed.

Once the students understood the physical layout of the DVD, they were ready to attempt reading of a damaged disk. They burned a DVD+R with known data and then damaged it similar to the challenge DVD, being careful to scratch the same physical areas on the test DVD as those on the challenge disk. The students discovered that as long as one could hold the disk up to a bright light and not see through the reflective layer, the data should be intact. The challenge was to smooth out the polycarbonate layer to allow the laser to shine through unobstructed.

Our team tried many methods to smooth out the scratches that didn't work. They were as follows: 1) *Toothpaste* –the abrasive white toothpaste, not the gel, did an excellent job on really minor smudges, it was not good enough for deep scratches. 2) *Brasso* – This worked better than toothpaste at getting out minor scratches, but an afternoon of multiple coats did nothing to help the deeper scratches. 3) *Disk Resurface Machine* – the local game store used a commercial disk resurface machine. This process took out the most scratches thus far and left the DVD with a nice clear surface, but there was a maximal scratch level that the resurfacer couldn't get through, no matter how many times the DVD was resurfaced.

What finally worked for our team was to use fine sandpaper to smooth out the scratches. The team first used 1000 grit sandpaper to sand the scratched side of the disk, constantly rinsing the sandpaper to remove the sanded plastic from the paper. The students had to ensure all major scratches were removed from the brown data area and inward to the center of the disk. They then used 2000 grit sandpaper to remove the smaller scratches. After this process, the team had a really smooth but hazy disk. The next step was to get rid of the haziness. Our team used Maguire's PlastX clear plastic cleanser and polish. As the haze cleared, the brown area of the disk became clearer. This section of the disk needed to be as clear and bright as possible.

The team next put the DVD into a DVD reader and created an optical image of the file on the disk. This step was necessary because the OS could not put the damaged file together and make sense of it. This process mirrors that of image analysis and forensic copying as conducted in our course and labs. The last step was to read the optical image with *WinHex* [24]. When this step was performed, the text "QDueling is legal in Paraguay as long as both parties are registered blood donors" was repeated for several hundred megabytes. This resulted in the completion of the challenge. Course material that contributed to the completion of this challenge included reading of magnetic media, preservation of digital data, analysis of binary data, and imaging of digital media.

5. Conclusions

The DC3 Digital Forensics Challenge has proven itself as an extremely powerful motivator and education tool to supplement our digital forensics course. This paper describes a successful cyber security education curriculum where students not only learn the concepts, but they apply them in an actual competition. The students respond well to hands-on instruction. Feedback from the students consistently indicates the cyber courses are among their favorites and the lessons learned are internalized.

We recognize that using any competition exclusively in a course is not educationally sound, as the skills we teach our students are applicable to more situations than those presented in the competition and not just technical explorations into a limited problem subset. However, the reinforcement of instruction with application creates a truly thorough understanding of

network and system security (as in the CDX) and also in digital forensics (as in the DC3 challenge). We find that students genuinely enjoy the hands-on environment of the CDX and DC3 challenge and would rather spend their time in the lab, learning by doing—a well known technique for this type of environment [25].

The AFIT curriculum thrives on the thrill of competition, and the competition thrives on the rigorous curriculum of schools like AFIT's. In the end, the students are well prepared for future competitions either in the academic arena, or the arena of life!

6. References

[1] DC3 Digital Forensics Challenge, http://www.dc3.mil/challenge/, May 2008.

[2] B. E. Mullins, T. H. Lacey, R. F. Mills, J. M. Trechter, and S. D. Bass, "The Impact of the NSA Cyber Defense Exercise on the Curriculum at the Air Force Institute of Technology," *Hawaii International Conference on System Sciences (HICSS-40)*, Waikoloa HI, 1-9, Jan. 2007.

[3] M. Gettle, "Air Force releases new mission statement," *Air Force Print News*, http://www.af.mil/news/story.asp?storyID=123013440, last accessed 15 June 2006.

[4] 8th Annual Cyber Defense Exercise, http://www.nsa.gov/releases/cdx.cfm, May 2008.

[5] DoD Cyber Crime Center, http://www.dc3.mil/dc3/home.htm, May 2008.

[6] P. Craiger, "Training and Education in Digital Evidence," *Handbook of Digital and Multimedia Forensic Evidence*, Humana Press, 11-22, Dec. 2007.

[7] A. Yasinsac, R. F. Erbacher, D. G. Marks, M. Pollitt, P. M. Sommer, "Computer Forensics Education," *IEEE Security & Privacy*, 1(4): 15-23, 2003.

[8] "A Road Map for Digital Forensic Research," *DFRWS Technical Report*, DTR-T001-01, 2001.

[9] M. Carney, and M. Rogers, "The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction," *International Journal of Digital Evidence*, 2(4), 2004.

[10] B. D. Carrier, and E. H. Spafford, "Defining Digital Crime Scene Event Reconstruction," *Journal of Forensics Science*, 49(6), 2004.

[11] P. Gladyshev, and A. Patel, "Finite State Machine Approach to Digital Event Reconstruction," *Digital Investigation*, 1(2), 2004.

[12] P. Stephenson, "Modeling of Post-Incident Root Cause Analysis," *International Journal of Digital Evidence*, 2(2), 2004.

[13] E. Casey, "Digital Evidence and Computer Crime," Academic Press, Cambridge University Press, Cambridge, 2000.

[14] Department of Justice, computer crime and intellectual property section, http://www.usdoj.gov/criminal/cybercrime/searching.html, June 2006.

[15] The American Society of Crime Laboratory Directors, http://www.ascld.org, June 2006.

[16] Snort, http://www.snort.org/, May 2008.

[17] Wireshark, http://www.wireshark.org/, May 2008.

[18] Eagle X, http://www.engagesecurity.com/products/eaglex/, May 2008.

[19] K. Mandia, and C. Prosise, "Incident Response and Computer Forensics," 2nd Edition, MacMillan Publishing, 2005.

[20] National Institute of Justice, http://www.ojp.usdoj.gov/nij/, June 2006.

[21] U.S. Air Force Office of Special Investigations, http://public.afosi.amc.af.mil/, June 2006.

[22] Trid, http://mark0.net/soft-trid-e.html, May 2008

[23] H. Wu, "The misuse of rc4 in Microsoft Word and Excel," *Cryptology ePrint Archive*, Report 2005/007, 2005.

[24] WinHex, http://www.x-ways.net/winhex/, May 2008.

[25] R. M. Felder, and R. Brent, "Learning by Doing," *Chemical Engineering Education*, 2003, 37(4): p. 282-283.

7. Acknowledgements

We thank the reviewers for their constructive and insightful comments. We also thank the Department of Defense Cyber Crime Center (DC3) organization for their cooperation in the writing of this paper. The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.