Digital Battlefield Forensics

Eric Imsand and John A. Hamilton, Jr., *Auburn University*

Abstract – Discussion on cyberwarfare or information warfare has been dominated by visuals of high tech command centers with giant plasma screens. Tactical exploitation of captured enemy digital devices: laptops, handhelds, PDAs, cell phones, etc. is sometimes neglected. One of the growing challenges posed by the growth of digital information and digital devices is how to train the existing combat force for safe exploitation of captured digital devices. Auburn University researchers have been participating in an ongoing training effort to re-task injured service members to serve as digital investigators. We have also been preparing course modules that will train ground forces to properly handle, process, and preserve digital information that is seized on the battlefield – an increasingly common occurrence. Feedback from these courses has indicated interest not just in the law enforcement aspects of digital forensics, but in the battlefield exploitation of captured digital devices.

Index Terms – Digital Forensics, Combat Operations, Education & Training

I. Introduction

Considerable attention has been paid recently to the topic of cyberwarfare. While the importance of true cyberwarfare cannot be overstated, it seems as though the other ways in which digital information is now part of modern combat has been overlooked. Modern combatants on both sides of every conflict now rely upon digital devices to help them achieve their objectives. And when those devices are captured on the battlefield, one side has an opportunity to gain an advantage over the other *if* they know what to do with them.

Eric Imsand {eimsand@auburn.edu} is an Assistant Research Professor in the Department of Computer Science and Software Engineering at Auburn University. John A. Hamilton, Jr. {hamilton@auburn.edu} is a Professor in the Department of Computer Science and Software Engineering at Auburn University.

As of September 2008, the uniformed personnel strength of the US Department of Defense was roughly 1.4 million men and women (Air Force Association 2009). Such a large group clearly represents a considerable resource when discussing a digital conflict, whether that conflict is on the battlefield or in cyber-space. Auburn University has launched two different programs designed to address the shortage of trained digital forensics investigators. These two programs are aimed at preparing service members to properly handle and process digital devices when they are encountered "in theater" as well as preparing service members for careers in digital investigation as they transition back into the civilian workforce. (Cullison 2004)
The remainder of this paper is organized as follows. In section two we describe our ongoing program for teaching digital forensics to wounded service members. In section three we discuss the possibilities of teaching active combat personnel the basics of digital forensics, a subject we call "Digital Battlefield Forensics". In section four we will discuss some of the very real and pressing concerns that stem from providing this type of training to increased numbers of people. Finally in section five we conclude.

II. Training of Wounded Veterans

Auburn University has partnered with Mississippi State University and Tuskegee University to provide training in digital forensics to wounded members of the US armed forces (Imsand and Hamilton 2010). This training is on-base and for free to the veterans, bases, and branches of service. The equipment is provided by the university teaching the course, so the only thing required of the base is a room to hold class and interested and motivated students.

The objective of this training program is to fill this country's need for more digitally capable investigators. Most of the law enforcement departments in this country do not have sufficient expertise to process and analyze digital

ISBN 1-933510-96-X/$15.00

evidence. At the same time, an increasing amount of digital evidence is being seized at crime scenes every day. Whereas a few years ago personal computers were the only digital devices likely to be encountered at a crime scene, the rise of cell phones, digital video recorders, game consoles, MP3 players, etc. have dramatically increased the number of items to be processed.

While the country is coping with an ever-increasing amount of digital evidence and a digital worker shortage, many service members are returning from overseas wanting and needing a new career direction. All too frequently, service members suffer serious injuries that leave them physically incapable of performing the jobs they had prior to their combat tours. With this in mind, the Auburn, Mississippi State, and Tuskegee team has developed a digital forensic training program that provides wounded service members with an opportunity to acquire a new skill and experience at no cost to themselves. This digital forensic training program is based on the highly successful digital forensics training program developed at Mississippi State. At the completion of the training, service members have a basic understanding of how to process digital evidence, familiarity with concepts such as lawful search and seizure and chain of custody, as well as hands on experience with the tools and procedures used to process this evidence. Veterans who complete the program are well prepared to tackle the professional certifications needed to work professionally in the field of forensics. Those that decide that law enforcement is not the right path for them have increased their understanding of computers and digital devices, knowledge that will undoubtedly serve them well regardless of which career path they choose.

The following is a brief description of the curriculum (developed by Mississippi State) taught to the service members.

- *Computer Basics* – a brief overview of the basic components of a computer (hard disk, RAM, motherboard, operating system, applications, etc.).
- *Introduction to Cyber Crime* – a description of the types of crime frequently resulting in digital evidence.
- *Forensic Tools & Techniques* – an overview of common forensic tools, such as write-blockers and hardware imagers, as well as an introduction to common investigative best practices.
- *Imaging & Hashing* – a discussion of imaging (copying a piece of evidence for analysis or archive) and hashing (verifying the integrity of the copy). This lesson also includes many hands-on exercises in which students practice with commercial imaging packages.
- *Analysis* – trainees are provided with a basic overview of how evidence is analyzed. This includes a description of forensic meta-data as well as common locations of meta-data within popular file types.

The basic program consists of roughly forty hours of instruction. Because this program is dedicated to helping wounded warriors, the program is typically taught in a four hours per day format, allowing the service members the other half of the day for medical appointments, rehab, and other duties. Occasionally, depending on the needs of the base and the students, the program is offered in an eight hours per day format. The eight hour per day format is typically only offered to service members who are nearing the end of their rehabilitation and are therefore do not require daily meetings with medical staff. The hosting base typically makes a determination about which format suits their veterans for their population.

Figure 1 -- Auburn Instructors Teaching Injured Soldiers

Thus far Auburn has conducted a total of eight courses at military bases around the country. Based on survey data collected from participants at the end of the course, the following conclusions have been reached:

- These courses have increased the number of service members who would

consider a career in digital investigation after leaving the service.
- These courses have increased technical skill and proficiency self-reported by the participants.
- These courses have increased awareness of digital information, when information is retrievable, and when it is truly destroyed.

A. Planned Revisions to the Current Course

One thing that was discovered in working with the various Warrior Transition Battalions and Warrior Transition Units was that the demand for the training program frequently outpaced supply. In other words, we frequently encountered situations in which we were unable to accommodate all of the service members that wanted to participate in the course. Furthermore, there were an equal or greater number of wounded service members that were interested in the course who were unable to participate due to unavoidable scheduling conflicts.

In order to provide the training to a larger number of people, as well as to provide the training at times that are agreeable to everyone who wants it, we are exploring ways in which the training can be ported to an online environment. Online training poses unique challenges. This is particularly true in a discipline like digital forensics – a discipline in which trainees are frequently required to physically interact with the materials they are examining. Overcoming these challenges and providing meaningful training in this area over the Internet are the long-term goals for us.

III. BATTLEFIELD FORENSICS

Like any other large organization, terrorist groups have recognized the utility of modern computers. This is evidenced by the large number of digital devices that are retrieved during raids and attacks on terrorist encampments (Hesseldahi 2005), (Kelley 2003). Through the judicious application of digital investigative techniques, critical information is frequently extracted from these systems (Cullison 2004).

There are no public reports that the majority of the digital devices captured from terrorists thus far have employed any effective anti-forensic techniques. Anti-forensic tools are tools that prevent the extraction of data from the computer. While this is clearly a good thing, it is also a condition that is bound to change in the near future. The facts overwhelmingly support this conclusion: anti-forensic tools are cheap (and often free), easy to use, and highly effective. Once activated, these tools make the recovery of information from the protected computer extraordinarily unlikely. Frequently the window of time during which the tools can be deactivated or stopped is very small, meaning that the "first responders" (i.e. the first people to handle the seized computer) must be trained to handle digital equipment properly when they encounter it, otherwise there is a real danger that the information stored on that device may never be recovered.

The information extracted from captured digital devices is of value to a large number of people operating at different levels of the conflict. In addition to the tactical information that may be useful to planners back at headquarters, there might also be information pertinent to the commanders on the ground: enemy troop locations, numbers, etc. Unfortunately, novice attempts to find the desired information could result in damaging or destroying information that would otherwise be retrievable. This is another example of why combat forces need training on digital forensics: ensuring that overeager combat forces do not destroy delicate – and critical – information stored on the seized device.
In short, there are three primary reasons why combat forces require training in digital forensics:

1. Captured devices may be booby-trapped or configured with anti-forensic software.
2. Field commanders searching for battlefield relevant intelligence might damage the information stored on captured devices.
3. Captured devices may become damaged simply through improper storage and handling.

The objective of this type of training is to provide soldiers with the theory and practice needed to accomplish the mission and little more. Such a curriculum should not provide instruction on networking topics since the Internet is not a factor in most battles. Offensive capabilities should likewise be avoided to avoid situations in which unauthorized offensive actions are taken over computer networks.

ISBN 1-933510-96-X/$15.00

Before progressing, a quick note regarding our use of the term "Battlefield Forensics" may be in order. Traditionally forensic science has been used in the context of law enforcement investigations in a retrospective manner. What is being proposed here is the use of common computer analysis and recovery techniques for the purpose of planning future activities. In some respects this activity might be more accurately described as "intelligence gathering" rather than forensics. We feel the term "digital battlefield forensics" is appropriate for two reasons. First, there is growing precedent for pursuing criminal cases against terrorists seized in foreign countries and in these cases items that are seized must be handled in a proper way to ensure their admissibility in a US court. Secondly, it is our personal opinion that much of the security and obfuscation technologies that terrorists are using, and will continue to use, have arisen from the field of anti-forensics (e.g. terrorists storing critical information in a drive's slack space to avoid discovery). Given these reasons we choose to use the term "digital battlefield forensics" but can find little fault with critics who say this activity is more accurately described as inteligence gathering.

A. Computer organization

In order to understand some of the mechanics for what will follow in later lessons, attendees must be given a brief introduction to computer hardware, drivers, file systems, etc. While it is unreasonable to expect a complete novice to participate and comprehend this material, it's equally unreasonable to expect every participant to hold undergraduate degrees in computer science and engineering. For this reason a small amount of time needs to be dedicated to providing participants with a briefing on the underlying theory and organization of the computers on which they will be working.

B. System Analysis

It goes without stating that a battlefield is probably the last place anyone would want to attempt to recover/preserve digital information. When possible, digital equipment should be shipped back to a secure facility where it can be systematically examined and analyzed. Unfortunately, the presence of tools such as anti-forensic utilities and encryption sometimes make this impossible, as the window of time for intervention is frequently quite small. The challenge becomes determining when a system can be safely packaged for later analysis, and when a system needs to be analyzed and preserved immediately. Therefore, service members receiving this type of training require instruction in the area of system analysis. The goal of this type of training is to train participants to recognize potential storage devices, determine what types of storage devices are in use, whether or not there are (software or hardware) booby-traps present, whether encryption has been used (and if so, what kind and implementation), etc.

C. Persistence of Data

Because the overall objective of this course is to enable ground forces to recover and preserve data on seized digital devices, the participants need to receive training on the basics of digital forensics. This includes an overview of digital storage, how data is organized, and how to use the tools that can safely access the sensitive data.

D. Intro to Cryptography

Because so many of the defensive strategies make heavy use of cryptography to secure data, it makes sense to provide participants with a cursory briefing on the basics of cryptography. The objective of this portion would not be to focus on complex mathematics, but instead provide "advanced user" training on cryptography. This might include topics like key management and storage, a general overview of asymmetric vs. symmetric key cryptography, and an overview of cryptanalysis.

E. Anti-Forensics

As described earlier in this paper, a number of operating systems now include anti-forensic pieces like partial and whole disk encryption. This includes all modern versions of Windows (Microsoft Corporation n.d.) as well as Mac OS (Apple, Inc. n.d.). Furthermore, each successive release of an operating system sees the use of encryption become more transparent, easier to configure, and more tightly integrated with the core operating system. All of these factors make it likely that operating systems are likely to be continuously hardened against the precise activities that we seek to train soldiers to undertake.

ISBN 1-933510-96-X/$15.00

In addition to the anti-forensic pieces featured in many operating systems, a variety of freeware and shareware utilities now exist which can also be used to secure data on seized devices. Packages like TrueCrypt render data effectively inaccessible when used properly. Training soldiers to recognize the presence of these systems when they encounter them could provide analysts with access that they ordinarily would never obtain.

Anti-forensics also covers additional unconventional software like booby-traps. It is common for criminals to attempt to booby-trap a system so that, in the event of capture, the system destroys data or itself before it can be used by law enforcement. It stands to reason that terrorists will engage in similar strategies to ensure that their sensitive information does not fall into enemy hands. Therefore any course that focuses on seizing digital evidence from hostile forces should also cover the discovery and removal of software booby-traps such as drive wiping programs.

F. System Cracking

In some situations it might be necessary to attempt to gain access to information on a secured digital device "in the field", rather than shipping the seized device back to base. In these cases, participants require instruction on cracking into systems that have been hardened by the adversary. This might include items like resetting BIOS passwords, resetting the Windows administrator password, or decrypting the computer user's password(s). In some cases, this might involve using specialized utilities to recover encryption keys from the hard disk if an encryption suite has been activated.

IV. Practical and Ethical Concerns

After offering digital forensic training to wounded veterans for almost two years, we have yet to receive any complaints regarding the skills being taught to the veterans. This is to be expected given what is being taught. The course for wounded veterans focuses on the analysis of digital evidence after it has been seized with proper authority. The course for veterans does not teach any "offensive" techniques that might allow a user to "hack" into another computer.

Clearly the Digital Battlefield Forensics course is very different in this regard. This course is expected to teach a variety of offensive techniques designed to circumvent the security systems of the seized computer. In light of this, it is only right and natural for there to be questions concerning the skills being conveyed to the soldiers.

First, it is important to realize that the proposed curriculum presented is not suited for every service member. Clearly some discretion would need to be exercised when deciding which soldiers, sailors, and airmen received this training. Just as no one would suggest that a university should teach "Hacking 101" to every freshman, neither should each soldier, sailor, or airman receive this type of "battlefield digital forensic" training.

On the other hand, every member of the armed forces is taught skills that must be used judiciously. Weapons training, hand-to-hand combat, and explosives training are just a few examples of skills that a large number of service members receive that have no use in the civilian world. Clearly these skills are crucial to accomplishing their objectives, as are the offensive skills needed to compromise digital devices seized on the battlefield.

Furthermore, just as soldiers are not allowed to drive a tank off-base, so too will the offensive software used in the exercises be tightly controlled. Programs used to break into systems (ex: OphCrack) will not be provided to class participants. It is undeniable that some trainees will find their own copies of these programs on the Internet, though it can be argued that this is analogous to soldiers purchasing their own firearms for personal use.

The other mitigating factor regarding Digital Battlefield Forensics is the scope of the training. This training will be limited to systems the student has physical access to. The course will not teach "Internet hacking" as it has no bearing on the objective of the course and, it could be argued, would be counterproductive to the goals of agencies engaging in legitimate cyberwarfare.

V. Summary

Auburn University has undertaken a program to make use of veterans and members of the armed forces in the realm of digital warfare. This program is comprised of two efforts: digital forensic training for wounded veterans leaving

ISBN 1-933510-96-X/$15.00

the service, and Digital Battlefield Forensic training for members of the armed forces that might be required to deploy. Both of these programs can be beneficial in dealing with cyber-augmented warfare, i.e. traditional warfare that makes use of cyber-capable devices.

VI. ACKNOWLEDGEMENTS

We wish to thank our colleagues at Mississippi State University for the partnership and mentorship they shared with us while working with wounded service members.

The training program for Wounded Warriors is sponsored by the National Science Foundation, award number 0753305.

VII. WORKS CITED

Air Force Association. "2009 Air Force Almanac." *Airforce-magazine.com.* May 2009. http://www.airforce-magazine.com/MagazineArchive/Magazine%20Documents/2009/May%202009/0509facts_fig.pdf (accessed March 1, 2011).

Apple, Inc. "Mac OS X 10.4 Help -- About FileVault." *Apple.com.* http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1877.html (accessed February 25, 2011).

Cullison, Alan. "Inside Al-Qaeda's Hard Drive." *the Atlantic.* September 2004. http://www.theatlantic.com/magazine/archive/2004/09/inside-al-qaeda-rsquo-s-hard-drive/3428/ (accessed March 1, 2011).

Imsand, E, and J.A. Jr. Hamilton. "A Digital Forensics Program to Retrain America's Veterans." *Annual Symposium on Information Assurance.* Albany, NY, USA, 2010. 1-5.

Hesseldahi, Arik. "From the Laptops of Terrorists." *Forbes.com.* April 29, 2005. http://www.forbes.com/2005/04/29/cx_ah_0429tentech.html (accessed February 19, 2011).

Kelley, Jack. "Seized Laptop Lists al-Qaeda Hideouts." *USA Today.* March 12, 2003. http://www.usatoday.com/news/world/2003-03-12-bin-laden-usat_x.htm (accessed February 19, 2011).

Microsoft Corporation. "BitLocker Drive Encryption Overview." *Microsoft Windows.* http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview (accessed February 25, 2011).