Hostile Forensics
by: Mark Lachniet
Version 1.0, August 5, 2011

Table of Contents

1. Overview

Due to recent developments in counter-forensic technologies such as strong encryption, it may soon be necessary for forensic analysts to use system penetration or “hacking” techniques in order to obtain forensic evidence, a process here referred to as “Hostile Forensics”. This issue is not one that has been adequately discussed in the forensic community at large, and as such there has been very little planning or public collaboration to discuss issues and define standards, tactics, strategies and best practices. It is a particular problem for U.S. law enforcement, that currently has few (if any) legal ways to pro-actively obtain permission to use penetrations in a law enforcement operation. This document represents the results of a thought experiment by the author about how one might structure a Hostile Forensics operation with the greatest degree of assurance possible, and to perform an investigation into the issues and approaches of penetration-based forensics.

Whether or not Hostile Forensics would be legal, or indeed even a good idea, remains to be seen, and will vary from place to place and legal context. Certainly, in some very specific circumstances, such as a covert investigation of an organization's own property where consent has been obtained, there is already a case to be made for the legality of these techniques. It is hoped that by detailing a methodology that includes strong internal controls, analysts will be able to provide at least *some* assurance that the evidence obtained is trustworthy. Similarly, with adequate internal controls, the opportunity for an unethical analyst to plant evidence or otherwise “frame” an innocent person should be greatly reduced. In this way, it is hoped that forensic investigators will be able to perform their function for society while still respecting the rights of the individual - a challenge that is sure to become more and more difficult as technologies such as encryption become more wide-spread.

This document has two parts. The first part is an overview of the issues surrounding digital forensics in the modern age, as perceived by a technical practitioner but legal layman. The second part of the paper is an attempt to outline a general methodology and set of controls and techniques that might be used to perform a Hostile Forensics operation. A non-technical reader may be more interested in the first part, whereas a strictly technical reader may be more interested in the latter.

1.1 Disclaimer and Legal Warning

This document represents the personal opinions of the author, an individual without legal training, and is intended as a preliminary analysis of the issues and controls that might be used to implement a Hostile Forensics practice with some degree of assurance. The author is not an expert on forensic lab certification, a law enforcement officer, a military strategist, or a lawyer, and as such it is recommended that this document be used only as a starting point, and that subject matter experts in the tools, controls and laws relevant to the reader's own unique circumstances be consulted to ensure good results and legal compliance. In researching this topic, the author has necessarily investigated a number of complicated legal issues. This research was done from the perspective of a layman, is not informed by legal training and is certainly far from being legally comprehensive. There is a risk, therefore, that a reader might interpret the statements in this document as being authoritative, and this is far from the case. That said, there seems to be a lack of understanding of these legal issues in the forensic and penetration testing communities. Thus, at the risk of possibly introducing inaccurate or misleading information, a layman's interpretation of legal issues will be presented nonetheless. Also, this document is intended for people or organizations that are operating lawfully, and not intended to

advocate or promote illegal activity. Further, the author is a citizen of the United States of America, and may refer to laws and standards that may not apply in other countries and jurisdictions. That said, the author is experienced with penetration testing, digital forensics, and internal control development, and his experiences “in the field” inform this document. Your mileage may vary, please consult a lawyer.

1.2 The Changing Nature of Digital Forensics

The field of digital forensics has seen significant change in the last decade of the twentieth century and first decade of the twenty-first. As technology has become more and more a part of everyday life, the availability of hardware and software systems to protect and make private a user's activities and data has also improved, making reasonably good encryption available free of cost to any who wish to use it. Unfortunately, while protections such as disk encryption are often used for the legitimate purpose of protecting one's rights and personal information, they are also increasingly used to obscure and conceal evidence of crimes on computing systems. These encryption systems can make the job of a forensic analyst exceptionally difficult using the now-outdated approach of physically seizing and analyzing storage media. For this reason, it is the opinion of this author that computer forensic practitioners will increasingly need to perform computer penetrations (i.e. “hacking”) of target workstations in order to obtain the types of information most essential to a modern investigation, notably data that would be lost or encrypted when the system is powered off. By penetrating a target workstation, an analyst may be able to obtain not only conventional volatile data such as the contents of memory, lists of running programs, and network connections, but also passwords and encryption keys that could be used to decrypt data from unmounted media once a system has been physically seized.

Where once most forensic data of interest was found primarily in images, office documents, and electronic mail on computer workstations, the sheer variety of data that is now needed as part of an investigation has expanded to include a wider assortment of operating system artifacts, volatile data such as running programs and the contents of system memory, artifacts from a host of modern software packages such as Skype, iTunes, Instant Messaging, and much more. The physical locations in which potential evidence is processed and stored are also more diverse, including everything from consumer devices such as mobile phones, GPS devices, network-enabled televisions to network devices such as wireless access points and personal firewalls. Similarly, there are vast amounts of information and potential evidence stored outside of systems readily accessible by law enforcement, let alone private investigators. Whereas basic information such as an Internet Service Provider's DHCP[1] leases and subscriber information once were the most common types of external information needed by investigators, it is now far more frequently data in e-commerce sites such as Craig's List and eBay, social media sites such as Facebook, and chat logs within on-line virtual environments and MMORPG's (Massively Multi-player On-line Role Playing Games) like World of Warcraft that are frequent targets of search warrants and subpoenas.

While there has been an obvious expansion in the types and locations of potential evidence, there have similarly been improvements in the ways in which this data can be protected. Although in many cases flawed, protections on individually identifiable information held by service providers and Internet sites have been slowly improving, leaving less information available to casual browsing, and more information obtainable only through legal process. It is also far easier now for individuals to

1 http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

protect their own privacy through free software such as TrueCrypt[2] and operating systems such as Windows 7 Ultimate and Enterprise that come standard with data encryption capabilities via BitLocker[3] and TPM (Trusted Platform Module)[4] hardware. Other popular operating systems such as the Macintosh OS and Linux / UNIX systems now frequently offer folder and file encryption by default as part of the installation process.

Other hardware-level privacy services are also now available that can create difficulty for investigators, such as Toshiba's line of hard drives that can automatically erase their data if the drive is moved from its original host bus adapter to another machine.[5] Some recent developments that impact investigators may not be intentional. For example, researchers have noted that solid state hard drives (i.e. those that use memory chips to supplement or replace rotating magnetic platters) "have the capacity to destroy evidence catastrophically under their own volition, in the absence of specific instructions to do so from a computer."[6] In other words, these modern SSD hard drives may delete data even while connected to write blockers. Even aside from these challenges, the size and scope of data potentially requiring analysis has grown, as the amount of storage space available to computer users has increased over time from megabytes, to gigabytes, to terabytes of storage on the average personal computer.

In addition to the technologies available for both forensics and counter-forensic purposes, there has also been an increased level of awareness amongst computer users, particularly those who have a need for hiding digital evidence. This certainly includes terrorists and criminals, such as child pornographers, who are embracing the use of encryption and teaching other like-minded individuals what they have learned, but it also includes legitimate uses such as protecting personal information, or information that is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA[7]). In some states, the very act of using encryption to hide a crime may be illegal.[8] Although this author is not aware of any reputable statistical studies of the frequency of encryption being used for nefarious purposes, anecdotal evidence in the form of personal discussions with law enforcement officers as well as research by governmental agencies has cited evidence of data encryption being used by many criminals and organizations, including Al Qaeda and other terrorists since as early as the 1990's.[9] [10] As noted above, there is also a great deal of encryption being used by individuals and in legitimate and law-abiding organizations such as hospitals, banks, and insurance companies. Due to recent data breach disclosure laws that have been enacted in many countries, organizations that have been compromised (for example through successful hacking attempts on systems storing sensitive data) or that have "lost" data by means of lost backup tapes or stolen digital media or laptops, are required to announce their breach publicly and attempt to remedy the potential impact of these incidents on those affected. As should be obvious, an organization that must publicly announce that its security systems were compromised and ultimately ineffective will likely suffer a significant loss of confidence, and may also be required to pay regulatory fines and offer credit monitoring or other services to potential victims of their loss. Since most data breach regulations

2 http://www.truecrypt.org/
3 http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview
4 http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary
5 http://sdd.toshiba.com/techdocs/MKxx61GSYG_release.pdf
6 http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf
7 http://www.hhs.gov/ocr/privacy/
8 http://cyb3rcrim3.blogspot.com/2008/10/unlawful-use-of-encryption.html
9 http://www2.fbi.gov/congress/congress01/freeh051001.htm
10 http://djtechnocrat.blogspot.com/2011/02/jihadi-encryption-uk-case-reveals.html

provide a “safe harbor” exception for organizations that use appropriate disk encryption, these organizations may be able to avoid a costly and embarrassing breach disclosure if they can prove that the “lost” data was protected by encryption. Hence, while private and criminal use of data encryption is prevalent, corporate and governmental use is even more ubiquitous, approaching perhaps 80% of regulated companies seen by this author in the course of hundreds of penetration tests and security audits.

Fortunately for analysts, a few of the problems of modern forensics such as the exponential growth of disk space and the need to analyze a larger variety of devices and operating system artifacts seem to be compensated for with faster and more scalable equipment and better tools, at least for those capable of affording it. However, there are still a variety of issues that cannot be easily addressed through conventional techniques as embodied in the “image and analyze” approach to forensics that has been the standard for the last three decades. In the opinion of this author, the issue of encryption is by far the most difficult technical problem to address, although the capture and analysis of volatile data such as operating system memory and processes comes in at a close second place. Indeed, without direct administrator access to the target machine, or at least the keys and passwords required to access encrypted data, it may be cost-prohibitive if not outright impractical to analyze a well-protected system. Although options may exist for the “brute forcing” of encryption keys by guessing passwords or iterating through very long encryption key spaces, these options may require extensive financial and intellectual assets and not produce results in time for the data discovered to be of use.

Briefly put, due to ongoing progress in the sophistication of information security and privacy systems, the forensic practices embraced by many analysts, public and private, are becoming less and less capable of handling the needs of modern forensic investigations. This is particularly true of those “high value” targets that are both willing and capable of protecting their systems with encryption and other counter-forensic techniques. In the opinion of this author, a new paradigm, methodology, and tool set will be increasingly required to deal with these difficult cases, and this approach will necessarily need to be based, at least partly, on circumventing anti-forensic technologies, often by system penetration. This new approach, has been termed “Hostile Forensics” by the author, and represents a significant departure from conventional forensic practices.

1.3 Issues with Hostile Forensics

This document is intended to help individuals and organizations that have a legitimate need and right to use hostile forensic techniques in an organized and repeatable way, such that the process used can promote a maximum amount of trust in the evidence obtained. This is indeed no easy task, as conventional forensic wisdom holds that *any* access to a live system is undesirable, as it “taints” the evidence by mixing the activity of analysts and subjects, presumably making this evidence less trustworthy. The level of trustworthiness of obtained data can be a critical factor in legal proceedings, particularly in criminal proceedings, which (in the United States) holds that the level of proof be “beyond a reasonable doubt” in order to be used to obtain a conviction. It is for this reason that forensic practitioners have historically taken steps such as using hardware write-blockers to minimize the modification to evidence, so that arguments such as “the investigator is trying to frame me” are less likely to succeed in court. Indeed, if an analyst or the I.T. workers who first discovered the evidence did not follow proper forensic techniques while analyzing a live system, there is already ample cause for doubt. This issue is even more problematic in an analysis involving Hostile Forensics as the analyst

will out of necessity be making many modifications to the target evidence, quite possibly even deleting evidence that would be helpful to his own purposes in the process. Even minimally invasive hostile forensic techniques such as installing a small rootkit, running Metasploit[11], or running programs and scripts can over-write potentially interesting deleted files and modify file and folder metadata such as time and date stamps.

Aside from questions about the integrity of evidence, there are a number of issues about the legality of using Hostile Forensics. For example, is the analyst legally entitled to penetrate the system? Is the analyst complying with the laws of his jurisdiction such as wiretap laws? Will a system penetration alert the subject to the fact that they are under investigation and prompt them to destroy evidence as a precautionary step? All of these issues, and more, must be considered before beginning any Hostile Forensics operation, so that the risks and benefits of the approach can be objectively assessed. That said, it is the opinion of this author that due to the barriers created by current privacy and anti-forensic technologies, Hostile Forensics can be the best (and in some cases only) way to perform a successful forensic investigation. In the following sections of this document, some of these issues will be discussed and suggestions for best-practice controls and procedures will be developed.

2. Defining Hostile Forensics

A review of search engines including Google and Bing for the phrase 'Hostile Forensics' in May of 2011 revealed very few results from which to base a definition. Most of the search results at this time dealt with either the hostile capabilities of malware to obtain information from a computer, or counter-forensic techniques. It is quite possible that a more apt and appropriate term has already been established and is simply not known to this author. That possibility aside, it is helpful to more accurately define terms. The Merriam On-line Dictionary (emphasis added by author) defines hostile[12] as:

> *1.a* **:** of or relating to an enemy <*hostile* fire>
> *b* **:** marked by malevolence **:** having or showing unfriendly feelings <a *hostile* act>
> *c* : openly opposed or resisting <a *hostile* critic> <*hostile* to new ideas>
> *d (1)* **:** not hospitable <plants growing in a *hostile* environment> *(2)* **:** having an intimidating, antagonistic, or offensive nature <a *hostile* workplace>
> **2. *a* : of or relating to the opposing party in a legal controversy <a *hostile* witness>**
> ***b* : adverse to the interests of a property owner or corporation management <a *hostile* takeover>**

Thus, in this case, hostile is meant not in the sense of rude or angry, but rather in the sense of an opposing party, as shown in 2.a and 2.b above, although “owner” would sometimes be better interpreted as the individual in possession of an asset, rather than the ultimate owner, In a corporate investigation, the owner and the possessor of an asset may not be the same thing. The Merriam On-line Dictionary (emphasis added by author) defines forensics[13] as:

> 1. an argumentative exercise

11 http://www.metasploit.org
12 http://www.merriam-webster.com/dictionary/hostile
13 http://www.merriam-webster.com/dictionary/forensics

2. plural but sing or plural in constr : the art or study of argumentative discourse
3. plural but sing or plural in constr : the application of scientific knowledge to legal problems; especially : scientific analysis of physical evidence (as from a crime scene)

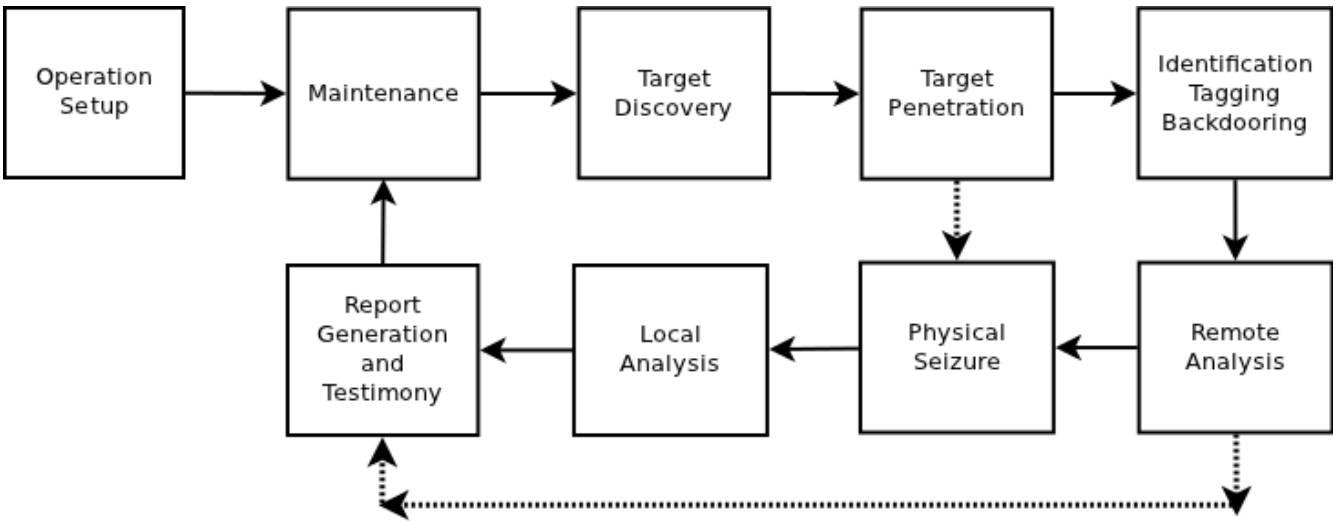
Here again, the meaning should be obvious – the analysis of evidence. It is necessary to be careful here as the evidence, while physical *somewhere*, may not be in the analysts' possession. In the specific example of Hostile Forensics, analysts may intend to gain access to this information through a wide variety of means, possibly including hacking or system penetration. Thus, in order to accommodate for the non-conventional nature of a Hostile Forensics operation, there must also be sufficient controls to promote confidence in the processes used and the evidence so obtained. A working definition of Hostile Forensics may be:

> *The scientific analysis of computer evidence, obtained through computer penetration or "hacking", and performed within a context of legal authorization and appropriate internal controls to promote confidence in the evidence obtained.*

3. Example Hostile Forensics Methodology

As with any repeatable process, if is helpful to identify and use a defined methodology. In this case, the analysts are concerned about the controls and techniques that might be used for a successful Hostile Forensics operation. To this end, a system process diagram has been created. A similar flowchart, with more detail but focused on traditional forensics techniques has been drafted by the U.S. Department of Justice[14] and may be of interest for supplemental reading. The following is a graphical representation of a methodology, developed by the author, that a Hostile Forensics operation might use:

Figure 1 – Example Forensic Methodology



Each of the above stages will be analyzed in further detail, but a high level dialog could be given in the following way. First, an operation will need to establish itself and its system of internal

14 http://www.justice.gov/criminal/cybercrime/forensics_chart.pdf

controls. This will include issues such as legal precautions, the tools that will be used, the members of the team, etc. This will generally happen once, although it may be revisited over time.

Next, before every assessment project a maintenance phase should take place. During this phase, tools and internal controls will be tested, improvements will be made based on previous assessments, and things will generally be validated as being appropriately configured. From this point on, assume that a target has been identified and that the subsequent steps will be relating to a specific analysis instead of the overall operation. During target discovery, the team will analyze the target and attempt to discover as much information about the subject as possible. This is intended to discover any legal requirements pertaining to the assessment, as well as the habits and character of the subject and their computing systems. During discovery, methods for compromising the target will be developed. Next, the target will be penetrated, possibly but not necessarily through hacking. A number of options may exist here, depending upon the context of the project. At this point, it is possible that a live investigation is not necessary, and that the analysts can proceed to seizing the evidence. For example, it may be readily apparent that there are no forensic countermeasures in place, or that physical seizure is in the best interest of the analysis. In general, though, the project would then proceed to the next stage of on-line analysis. Here, the analysts will attempt to clearly and uniquely identify the target system. This may include determining unique characteristics of the target such as disk serial numbers, network device MAC addresses, etc. These unique characteristics can then be used later to tie remote analysis activities to a physical asset if it can later be seized. The analysts may also wish to "tag" the target system, for example creating a hidden text file or registry entry that can further be used to link an on-line investigation to a physical asset. Last in this phase, the team may attempt to configure a back door, or means of getting future access to the system. After this has been completed, an on-line investigation of the target will be performed. This may include hands-on analysis of a live system, copying data from target storage media "over the wire", analyzing volatile data, obtaining encryption keys, etc.

Next, if possible, the asset will be physically seized, and the tags and unique information compared to what was obtained in previous steps to ensure that the physical machine is, in fact, the same machine that was remotely analyzed. Conventional chain of custody practices will be used with this physical hardware. Next, a local analysis of the machine will be performed. This stage is what most closely matches conventional forensic techniques of imaging and analyzing target data. Ideally, any anti-forensic countermeasures that the target may have in place will be circumvented by data obtained during the remote analysis stage. For example, it is hoped that encryption keys and their passwords would have already been obtained. Next, the results of the investigation must be documented in some form of report or deliverable, and these results must be communicated to appropriate parties. This may include informal debriefings, detailed deliverable review meetings, or possibly testimony in civil or criminal legal proceedings. At this point in the process, the specific analysis has been more or less completed, and the process returns to maintenance. At this time, the team should reflect upon "lessons learned", identify and document changes to the environment, and new tools and techniques used, and then update and improve the operation's systems appropriately. The importance of this final step cannot be overstated, as it will help to ensure that the Hostile Forensics operation is able to adapt and grow over time, while still keeping an adequate set of internal controls.

Each of the above steps will be discussed in greater detail in the following sections.

3.1 Operation Setup

The initial setup of the Hostile Forensics operation is almost certainly the most important step. It is during this time that the mandate for the operation will be established, and how best to run an effective operation that complies with the law and provides the greatest degree of assurance possible about the evidence produced by it. The details of what is developed in this stage will obviously be influenced greatly by issues such as budget, available staff, the purposes of the operation, etc. As an example, a Hostile Forensics operation that is run by a military or law enforcement task force will be much different from one run by corporate I.T. or private investigators. However, some tasks which would be appropriate to all operations might include the following:

- **Establish an operation mandate.** No operation should be developed without a clear purpose, and without authorization from a higher power. This is especially true of Hostile Forensics, due to the potentially difficult legal issues that will be involved. In the case of a governmental organization, the mandate might come from a legislature, director or captain. In the case of a corporate operation, the mandate would most likely come from the corporate executive officer, corporate information officer, director of internal audit, board of directors, or similar. In the case of a private investigator, the mandate may be given on a case-by-case basis by the client. In any event, it is in the best interests of the operation to have formal and written approval to perform Hostile Forensics work. If this is not obtained, and legal trouble is later encountered, it may be the employees of the operation themselves that become answerable for problems and the potential target of lawsuits or criminal charges.
- **Establish a budget.** It should be obvious, but no operation will be able to function without a budget – often a large one. digital forensics is an expensive field, and requires not only a great deal of hardware and software, but trained and qualified staff members. The budget may come from a general operating budget, or may be funded through grants or other sources. Ideally, the budget will be recurring, so that there will be a degree of predictability about the future of the operation. Ensure that the budget includes, at a minimum, provisions for hardware, software, internal and external services, staffing and training. Training, in particular, will need to be provided over time, or the operation risks losing the technical edge required to be successful. In the opinion of this author, a minimum of one week of formal, in-class training, should be budgeted for each employee, or more if the employee is required to be competent in multiple disciplines.
- **Identify and hire staff.** Performing hostile forensic work will most certainly be challenging, and hiring staff to do this work will probably be difficult. At a minimum, the operation will require skills in penetration testing and in digital forensics. Having employees skilled in legal issues and management is also helpful, although it may be possible to have these roles filled by part-time or shared resources. Consider issues of accreditation and certification when selecting staff. In some cases, having governmental clearances may be necessary. Looking to individuals who have certifications may also be of value, although in the opinion of this author certifications are not necessarily a good measure of an individual's competence. Given the nature of the work to be performed, a decision should probably be made whether or not to consider applicants who have a criminal history. For example, not all skilled penetration testers have worked within an ethical and legal context, but this does not necessarily mean that they are not honest and reliable, though it should not impede their ability to be adequately qualified to testify. Indeed, hiring individuals that have extensive penetration experience may bring more

skills to the table than would be feasible through other means. Another issue to consider is that of salary. In some organizations, this may be set by mandatory systems (such as a U.S. Government "GS" rating). Hiring qualified individuals will most likely require a higher grade of pay and benefits than many organizations are accustomed to. Remember that you will be competing against large corporations that can easily afford to pay high-end salaries. Another staffing technique that has been used with success is to use interns and other entry-level individuals, and train them up to a higher level.

- **Identify and obtain assets.** At the outset, and over time, it will be necessary to purchase a variety of hardware, software and other assets to support the operation. Some of this equipment may need to be custom-build or programmed, as some cutting edge penetration tools are not commercially available. Access to adequate, anonymous, Internet connectivity will probably be necessary. Some operations will use commercial or residential broadband services such as DSL and cable modems to conduct their penetrations, using a subscriber name that is not immediately obvious as being linked to an investigative operation. Similarly, it may be worthwhile to obtain or purchase access through service providers that can obscure or hide the identity of Internet users. Examples of this might include Internet HTTP or SOCKS proxy servers, perhaps even some that do not keep logs of activity. When purchasing penetration or forensic software it is recommended that due diligence be done before making a purchase, and that the security of any products considered be part of the selection process. Not all forensic tools, for example, are inherently secure, so it would behoove the operation to ask for evidence that third-party security audits have been performed. In governmental organizations, it similarly may be required to purchase assets that have gone through a certification process. In this particular subject area, many of the tools and scripts that would be used for penetration and forensics can be obtained free of cost, such as Metasploit. However, there is an inherent risk in carelessly using free tools, in that these tools could themselves contain hostile code. For example, it is conceivable that a tool that was found on the Internet could contain functions that would "phone home" information about its usage, possibly alerting someone to the investigation, or even worse compromising the forensic environment. In the case of free tools, it would be preferable to select open-source tools, or at least tools where the source code can be analyzed and then compiled by the team before use. In this way, a skilled programmer can validate the tools before they are used. If this cannot be done, then at a minimum the tools should be analyzed in a controlled environment to identify any suspicious activity. Finally, it would be worth mentioning that several companies now have enterprise class forensic tools that are specifically designed to perform across-the-wire data collection on computer workstations. These tools may be an excellent way to analyze a system after it has been compromised, and would be worth investigating during the lab setup phase.

- **Identify legal issues.** Legal considerations are *by far* the most important issue that must be considered at *all stages* of a hostile forensic operation. During the setup phase, the analysts are primarily concerned with the legality of doing the required work in the context of local jurisdictions. In other words, whether or not it is legal to run an operation of this type in the analysts' particular county, state or country. The analysts must also be concerned about the legalities of accessing target workstations in other jurisdictions, but this will be addressed in the discovery phase. It is absolutely critical that the organization promote ethical behavior and comply with legal requirements, or else the evidence obtained is likely to be unusable in court and could result in criminal charges against the operation's employees. Working with legal counsel is absolutely essential, especially at the setup phase of the project.

- **Develop internal controls.** Second only to legal considerations is the establishment of an adequate system of internal controls. The purpose of these controls is to promote confidence in the results of the forensic work so that evidence that was obtained through Hostile Forensics would be considered of high enough quality and trustworthiness to be used. One example of an internal control might be logging of activity performed by penetration testers, such as screen, keystroke and network packet loggers. With this control, an organization would be able to define what actions were in fact taken by an analyst, and then extrapolate this to how the evidence would have been affected by these activities. Another example of why strong internal controls are necessary would be to promote a secure work environment. If a work environment is insecure, for example because it resides on a lightly-protected internal network that could have been easily compromised, it might allow opposing lawyers to question the validity of the results. Developing an internal controls system will be expanded in a separate section of this document.
- **Develop policies and procedures.** There are a wide variety of policies and procedures that would be relevant and helpful for a Hostile Forensics operation. By creating policies, the expectations and standards of the organization can be codified and communicated to team members. These policies may include topics such as data classification and handling, disaster recovery, documentation, rules of engagement and other topics, but will vary widely depending upon the nature of the operation. Similarly, the organization should define and communicate its standards. For example, there may be standards that state that workstations must be installed, configured and hardened in a particular way, or that define how a multi-node forensic software package would be configured to make it more secure. Procedures may also include provisions for activities that are not inherently technical, such as keeping written logs of duties that are performed on a regular basis, details on how to store or destroy information, or maintain a physically secure work environment.

3.2 Maintenance

During the maintenance phase, the analysts are concerned with the ongoing duties of maintaining the operation's equipment, documentation and team. This would include all of the ongoing activities that an organization would be responsible for. This may include specific tasks, such as documenting tools, or may relate to tasks that could pertain to any organization. For guidance in this area, one might refer to general business best practices such as the ITIL[15] standards. Tasks in this phase might include items such as:

- Interviewing and hiring new staff members
- Providing ongoing training for existing staff members
- Performing routine maintenance on systems
- Performing reviews of system logs such as authentication systems, remote access and firewalls
- Validating and documenting existing tools and procedures
- Performing research on new tools, techniques and systems that could be of use to the operation
- Developing new tools and techniques to address specific needs

15 http://www.itil-officialsite.com/

- Maintaining backups, disaster recovery, business continuity and continuation of operations plans and systems
- Review “lessons learned” from previous investigations and improve practices and procedures
- Maintain and monitor key performance indicators to assess how well the organization is meeting its mandate, and adjust approaches accordingly
- Maintain a budget, and estimate employee and capital outlays over time
- Maintain a 3-5 year strategic plan
- Handle, archive and destroy confidential electronic and physical media, including evidence and activity logs
- Maintain a punch-list of work to be performed, tracking projects over time, and managing the employee resources assigned to them
- Perform formal project management on long-term engagements
- Maintain communications within the operation and without, including up the chain of command and with external entities such as law enforcement and the media

3.3 Target Discovery

Starting at the target discovery phase, the analysts have now reached the part of an operation that deals with the investigation of one or more specific computing systems or individuals. At this point, there should already be an idea of who the target or targets of the investigation are, and the analysts must perform several tasks. First, the analysts will need to analyze the context of the investigation and the specific legal issues associated with it, for example the jurisdiction and laws of the target, in addition to those of the analysts. Second, the analysts will do their best to identify the target and their physical and electronic profile. In a physical sense, this may include investigation of where the target lives, works, plays or drinks, and in an electronic sense his e-mail addresses, technologies and systems that he typically uses. Third, the analysts will attempt to identify ways that the target system can be compromised, and create a plan to conduct the penetration. Fourth, the analysts will test the proposed techniques that might be used against the target in a controlled environment to ensure that they work properly, will not alert the target to the investigation, etc. Inherent in all of these activities is a certain amount of documentation, as all of this work should be documented both for future reference (i.e. in court or to present to stakeholders) and to keep other team members aware of the project's status. This planning stage may be a large part of the actual work involved with penetrating the target, as effective planning will help to minimize problems, and allow team members to plan for unforeseen circumstances and develop backup plans ahead of time. While it may be true, as the saying goes (alternately attributed to Karl Clausewitz or Helmuth Von Moltke), that “no battle plan survives first contact with the enemy” it advisable to have a plan none the less, and preferably one with a variety of tested alternate approaches at hand and ready to use. The following are a few issues that must be considered during the target discovery phase.

3.3.1 The Investigative Context

Understanding the context of each analysis is critical to obtaining a favorable outcome. This document assumes that the operation is operating in a lawful context, and that it hopes to obtain evidence that can (hopefully) be used in a court of law. In order to achieve this outcome, however, it is necessary to know the rules of engagement – what can and cannot be legally done – during the investigation. If laws are broken in the course of the assessment, or if work is sloppy, it is likely that the investigators will not be able to use the evidence in court. These rules will vary depending on the context, the desired outcomes, the location of physical and logical evidence, and the right of the analyst to perform the assessment, and in particular the right to penetrate a computer in order to do so. This is a different process from the legal analysis that was done during the operation setup stage. Whereas during operating setup stage, the analysts are concerned with the legality of operations in their home jurisdiction, during target discovery, there is a concern with the laws where the target and their computing systems reside, and possibly the laws of jurisdictions through which those communications flow. A few contexts in which an investigation are most likely to occur are (in order of probability) the following:

3.3.2 As part of an internal investigation

Perhaps the least controversial type of a hostile forensic analysis would be as part of an investigation that is internal to an organization. The investigation could be conducted by the organization itself, contracted out to a private sector firm, or even conducted with the help of law enforcement acting on the organization's behalf. This might be an investigation of an employee by an employer, of a student by a school, or a similar investigation where *consent has already been established.* This would seem most likely to occur in a corporation or school, for example, where an individual has already signed off on an acceptable use policy (AUP) that states that the organization has the right to monitor and manage systems owned by, or connected to, its network. In order for this type of consent to be valid, the organization should show due diligence and consistency in promoting awareness of the AUP. Ideally, an organization will have explicitly trained those subject to the consent document on its contents, verify that they understand the provisions, and require regular sign-off (perhaps yearly) on these documents. Well-run organizations will typically give verbal instruction on the contents of AUP documents at hire-in, and will require a brief “quiz” with a small number of test questions to verify that the employees understand what they are agreeing to. On the opposite end of the spectrum, a poorly run organization might include an AUP as part of a large employee hiring packet that is given very little (if any) attention, and ask them to sign off on the entire packet. Although, in this case, the employee may have *technically* agreed to the AUP, in practice individuals often do not read all of the “fine print” and could argue in court that a reasonable person would not be aware of the rights they had just waived. In any case, it is assumed that the organization has established some formal type of consent of the person being investigated.

The least problematic type of investigation would be one in which the target machine is an asset that is owned by the organization. One might think that if the asset is owned by the organization it already has logical access and passwords for the target system. Indeed, if this is the case, it may not be necessary to actually penetrate the system at all, and conventional enterprise forensic tools could be used. However, it is also entirely possible that an individual might install software such as TrueCrypt on a machine owned by the organization and use that workstation for questionable purposes. It is also not infrequent that employees (especially I.T. workers) may re-install the operating system on their company system and/or change system passwords, effectively locking out the organization from their

own property. In this case, the company may not have a way to discreetly access their own equipment, and would need to use some kind of penetration to get access.

A somewhat more controversial scenario would be an organization that states that it reserves the right to monitor and analyze *any* device connected to its network, regardless of whether it is owned by the organization or not, and gets written consent to this, possibly in corporate or school environments. This might include, for example, a laptop, smart phone, or USB thumb drive that is owned by an individual but used in the organization's environment. In this scenario, it is strongly suggested that legal counsel be consulted to ensure that adequate consent has in fact been granted. It may be determined that the organization does not in fact have rights to access personal property that has been used on its network, despite what users have agreed to. In this case, the organization may still be able to perform investigations of other resources that it *does* have rights to in order to get the information it needs. For example, an organization might retain detailed logs of network activity on firewalls, anti-virus systems or content filters and identify questionable material from these sources. In any case, even explicitly granted consent is not all-empowering, and cannot be used as an excuse to commit crimes. For example, even if an individual were to grant consent for someone to murder them, the act would still be considered murder by law, regardless of this consent.

As was previously noted, an investigation in this context of previously given consent could be performed by a variety of individuals with an appropriate skill-set, including outside consultants. That said, some countries or states (including Michigan) may require analysts to have a Private Investigator's license to perform this kind of work. In states such as Michigan, exceptions may be made for investigations performed by full-time in-house staff, accountants and other specific categories of individual.

3.3.3 As part of a law enforcement or military operation.

While this author will not presume to know the inner workings of sophisticated military, intelligence and law enforcement organizations, it seems likely that hostile forensic techniques are already being used, although possibly not for the explicit purpose of obtaining evidence that can be used in court. Speculation in this area abounds, ranging from assertions that worms like Stuxnet were created by the Israeli or U.S. Government (see Bruce Schneier's article[16] on this topic) to media reports that “a spokesman for the Association of Chief Police Officers” in the U.K. have “carried out 194 hacking operations in 2007-08 in England, Wales and Northern Ireland, including 133 in private homes, 37 in offices and 24 in hotel rooms.”[17] The veracity of these claims are questionable, but given the inevitable need to penetrate high-value systems in order to access physically inaccessible or encrypted systems, it seems likely that operations have been taking place for some time and will only become more necessary over time as anti-forensic technologies such as data encryption are increasingly used.

All speculation aside, there are a variety of issues that would need to be addressed by a governmental or law enforcement agency before a legal penetration of a system can be performed. To this author's limited understanding, the core issues to consider here are the operation's written legal right to perform the analysis, through one of several means, and the reasonableness of their techniques. As of 2011 in the United States, it would appear that it is unusual (or perhaps under-reported) for law enforcement to penetrate a computer and use this evidence in court. Indeed, there does not appear to be any existing mechanism for law enforcement officers to obtain permission to penetrate a system in

16 http://www.schneier.com/blog/archives/2010/10/stuxnet.html
17 http://www.independent.co.uk/news/uk/home-news/new-powers-for-police-to-hack-your-pc-1225802.html

order to analyze it, although less intrusive mechanisms such as warrants and wiretap orders do exist, implying a need for legislative action. The U.S. Department of Justice's manual entitled "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"[18] details many considerations on these legal issues and should be consulted for a more in-depth and authoritative treatment of the subject.

- **With consent**. If a law enforcement operation were given written consent to perform an analysis of a computer, they might be allowed to perform this work legally. This would be very clear in the case of a system that was wholly owned or used by a single individual. At first blush, this would seem to be a trivial example. After all, if the individual had possession of the system, would they not also have the password? But, it is possible to imagine circumstances where this might be useful. For example, the investigation may be looking at a system that was used by a household guest, for an individual that is no longer living or has been incarcerated, or to prove their own innocence (perhaps because they believe that their computer has already been penetrated by some third party). Similarly, the individual may be the victim of an extortion attempt, such as those perpetrated by criminals who encrypt a user's information and require them to purchase a product to decrypt it.[19]

- **Exigent circumstances.** In certain instances, law enforcement may be empowered to perform a warrant-less search (and by extension, possibly a warrant-less intrusion into a computing resource) in order to prevent a serious future event such as a murder or rape, destruction of evidence, or escape of a suspect. These circumstances, known as "exigent circumstances[20]" might be used as part of a legal argument for Hostile Forensics without a warrant or wiretap order. The DoJ document above notes that a "exigent circumstances exception to the warrant requirement generally applies when one of the following circumstances is present: (1) evidence is in imminent danger of destruction; (2) a threat puts either the police or the public in danger; (3) the police are in "hot pursuit" of a suspect; or (4) the suspect is likely to flee before the officer can secure a search warrant." There are some constraints that may apply even to these circumstances, including the fact in some cases an analyst may not be empowered to actually analyze a machine that was seized through exigent circumstances exceptions. Consider, for example, an instance where law enforcement received a tip that a group of child pornographers were discussing the details of a planned rape of a child and production of child pornography, and that these communications were conducted over encrypted channels that could not be decrypted in time to prevent the crime. If Hostile Forensics were used, it might be possible to intercept these communications, obtain clear evidence of an impending crime, and prevent it. In this case, the benefit to society by preventing this heinous act may outweigh the rights to privacy of the suspects.

  Note that one of the exigent circumstances previously mentioned was regarding the protection of potential evidence from destruction. One might argue that the very act of encrypting data *equates directly* with destroying evidence when attempting to disrupt an investigation, in that it makes the potential evidence unavailable. This argument could be further bolstered by the fact that the U.S. Government's Health and Human Services (HHS) department has essentially equated encryption as destruction in its guidance for disclosing breaches under the HIPAA

18 http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf
19 http://www.techrepublic.com/blog/security/ransomware-extortion-via-the-internet/2976
20 http://www.lectlaw.com/def/e063.htm

regulation.[21] The guidance given in this previous reference is intended to deal with defining which situations would require an organization to disclose a security breach to the public. In this document, encrypted data is considered destroyed to such a degree that a "safe harbor" exception is given to any organization that loses control of data thus encrypted. Would it be possible that an exigent circumstance might exist because a suspect planned to encrypt data? A related example of U.S. Law enforcement successfully using exigent circumstances to compromise a remote system can be seen in in the case of U.S. v. Gorshkov[22]. In this case the FBI:

> *"seized the laptop and all the keystrokes made by Gorshkov by means of a sniffer program. The FBI then obtained Gorshkov's username and password that he had used to access the Russian computer. Using the login information, the FBI logged onto Defendant's computer system in Russia and downloaded the file contents of the computer(s) without a warrant. The FBI downloaded and copied the files prior to the warrant being applied for and obtained"*

The court later found these activities to be lawful, in part because of the exigent circumstance that evidence might be lost if law enforcement did not act quickly to preserve it. It should be noted that the target in this case was not a U.S. Citizen and the target systems were not on U.S. soil.

Use of the destruction of evidence exigent circumstances argument via encryption is questionable. One must consider that the HHS guidance is based upon the assumption that the encryption key is unavailable. In the example of an individual encrypting data on their own system, they would indeed have the encryption key and would be able to provide it to law enforcement if they desired. However, this does not mean that a suspect *will* provide the password, creating potential fifth-amendment questions for criminal cases, and one must be cautious about passwords that were obtained under duress. Whether or not passwords can be compelled by law seems to be far from settled, and is outside of the scope of this document.

- **Warrants and wiretap Orders**. These are the conventional means of obtaining physical assets and data on computing systems, although wiretaps are far less common than warrants due to law enforcement being required to demonstrate a more compelling need. Wiretaps are typically required to intercept "live" communications such as e-mails in transit and telephone calls, although some exceptions do exist. Notably, as stated by the DoJ document, the "*Computer Trespasser Exception"* allows law enforcement to intercept the communications of a computer trespasser "transmitted to, through, or from" a protected computer if certain requirements are met, notably authorization from the "owner or operator of the protected computer". Although means exist, there are few examples of law enforcement going beyond these mechanisms (i.e. using system penetration) to obtain data. A few examples do exists, however, such as Glazebrook[23] and Scarfo[24]. In the Glazebrook case, law enforcement officers apparently used a piece of software to record the suspect's keystrokes with a piece of software called "computer and Internet protocol address verifier," or CIPAV. This piece of software recorded information about the workstation on which it was installed, including such things as IP addresses and URLs visited, but was specifically designed to avoid capturing the contents of communications and

21 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
22 http://itlaw.wikia.com/wiki/U.S._v._Gorshkov
23 http://www.wired.com/politics/law/news/2007/07/fbi_spyware
24 http://epic.org/crypto/scarfo.html

could thus be installed without a wiretap warrant. In the Scarfo case, law enforcement compromised a citizen's system with the explicit purpose of obtaining passwords to encryption software (in this case, getting the Pretty Good Privacy encryption password using a key logger). For more information, the Electronic Privacy Information Center citation above contains extensive information about the case. In cases of international, non-domestic surveillance (and possibly intrusion) the Foreign Intelligence Surveillance Act[25] provides powerful mechanisms that appear to have a far lower level of required oversight. As any Hostile Forensics operation that must obtain authorization using these legal mechanisms will be far better versed in such matters than this author, discussion on this topic will be left for more capable treatment by others.

Once the legal issues have been dealt with, and a plan for compromising the system has been devised, the plan will be put into action.

3.4 Target Penetration

During this stage of the Hostile Forensics operation, the actual compromise of the target's computing resources is performed according to the relevant laws of the operation's and target's jurisdictions. Ideally, the methods of this compromise have been identified and tested prior to use, and controls such as screen and packet logging have been used to improve the level of trust in the evidence that might be obtained. It is not the purpose of this document to detail the ways in which a system can be compromised, and in any event each system is unique. However, it makes sense to categorize some of these approaches and discuss at a high level how they might be enacted.

3.4.1 Physical Access to Target

If physical access to the target is available, for example if the operation is empowered to gain access to the target's residence, place of work, Internet service provider, or other environments in which the target or their computing resources reside, it may be possible to obtain the requisite access without the difficult task of actually "hacking" a system. In general, these approaches are better geared towards *logging* of information, rather than changing a system, and in some cases may be wholly passive. Some approaches that might be taken would include:

- **Wireless networks**. If an analyst is able to get a strong wireless signal, often possible while at a nearby property, they may be able to "crack" the target's wireless access point using software such as Aircrack[26]. This may already be a standard practice by law enforcement in the U.S.[27] A wireless attack such as this can be passive (only in monitoring mode) or active (injecting packets to reduce the time required to crack). Once cracked, network traffic can be viewed, for example using a program such as Wireshark[28] and in some cases manipulated. Most security-aware targets will use protocols that require encryption, so that much of the most interesting network traffic will be obscured. However, some information such as DNS[29] requests, and even the IP addresses of network traffic, can be of interest. Also, once an analyst has the ability to access a network to send packets, it allows for other attacks, such as man-in-the-middle and

25 http://epic.org/privacy/terrorism/fisa/
26 http://www.aircrack-ng.org/
27 http://www.wired.com/threatlevel/2009/04/more-fbi-hackin/
28 http://www.wireshark.org
29 http://en.wikipedia.org/wiki/Domain_Name_System

direct attacks on network services. Note that in some more sophisticated environments, targets may employ wireless intrusion prevention systems that can detect and alert on some attacks, so care should be taken.

- **Wired networks**. Similarly, it may be possible to get access to a target's local wired network. In the event of a residence, this is probably going to be limited to a small switch or access point, which may not support monitoring, and in any event would be fairly obvious. In the event of an individual plugged into a larger network such as a school or workplace, they are likely to be plugged into an enterprise-class switch, and several options may exist. Specifically, many switches can be configured to mirror a specified Ethernet port to a second Ethernet port for read-only monitoring[30]. In addition to the switch in which the user is plugged into, other switches and routers that are part of the target's network communications may pass relevant network traffic and be monitored as well.

- **Service manipulation**. Internet services rely on a number of standard protocols such as TCP/IP, ARP[31] and DNS in order to function properly. Usually, but not always, manipulating these services requires physical access to the physical environment, or an environment that is part of the network traffic stream. It is generally assumed that these services will function "as intended" and are often not well understood by non-technical users. By manipulating these protocols, it is often possible to perform attacks on client machines that would otherwise be difficult or impossible. For example, if an analyst is able to get control of the target's DNS servers either at the ISP or whatever network they are plugged into, they may be able to trick the user into connecting to an "impostor" network host in order to obtain information such as password hashes. This approach was used, for example, to disable the Mega-D botnet[32]. Similarly, many protocols such as ARP are vulnerable to "man-in-the-middle" attacks, whereby a target can be tricked into routing their connections through an arbitrary host that is controlled by the analyst. See the program Ettercap[33] for an example. Similarly, an attacker may be able to simulate a software update site, and deliver malware by means of false software updates using a tool such as ippon[34]. Indeed, there are attack packages such as the Social Engineers Toolkit[35] that are specifically designed to conveniently implement Man in the Middle and social engineering attacks. By means of these attacks, the machine in the middle of the communications may be able to obtain passwords, hijack connections, or even install software on the target system.

- **Password hash grabbing**. If the target system is the right version of Windows and does not have full-disk encryption, it is possible to use a boot CD or DVD to extract the encrypted passwords (known as password hashes) and crack these hashes using a rainbow table[36] attack. This method is a consistently successful way to obtain the plain-text password of a Windows system. The passwords could then be used to log into the computer, and perform further analysis or system modifications, including possible access to encryption systems that rely on operating system credentials.

30 http://en.wikipedia.org/wiki/Port_mirroring
31 http://en.wikipedia.org/wiki/Address_Resolution_Protocol
32 http://en.wikipedia.org/wiki/Mega-D_botnet
33 http://ettercap.sourceforge.net/
34 http://code.google.com/p/ippon-mitm/
35 http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29
36 http://en.wikipedia.org/wiki/Rainbow_table

- **Hardware modification.** Finally, there are a number of attacks that could take place if an analyst had physical access to the target machine, not the least of which is a hardware key logger that could intercept keystrokes without requiring access to the operating system. These devices, such as the KeeLog[37] apparently have capabilities that include the ability to be plugged in between a keyboard and a computer and transmit user activity through e-mail via a wireless network, or store the activity until it can be physically retrieved. Similarly, the same site offers a "VideoGhost" device that will record images of the screen every few seconds and store them, which might be ideal for child pornography cases. There are also a number of attacks using devices such as U3 flash drives and software such as the Universal Customizer and attack ISO images to simulate an optical CD device. When plugged in, these U3 flash drives can trick some operating system into initiating the autorun sequences on the disk to install malware, copy password hashes or perform other attacks. In the event that the system is configured to disallow autoruns, some Windows systems could be compromised by using a "Teensy USB" device with attack software[38] that simulates a keyboard rather than a storage device.
- **Attack system backups.** If the system is backed up, for example to a tape library, Windows Backup file, ghost image, or virtual machine backup, it may be possible to restore this backup to another machine, and then compromise it. In particular, with any backup that contains operating system (i.e. Windows "system state") or application passwords (such as iTunes) it may be possible to obtain the plaintext passwords to use on the actual target, or even identify evidence directly on the backup media. For home users, external hard drives and network attached storage are likely candidates for storing system backups, as they are capable of holding large amounts of information.

There may be any number of other ways to compromise a machine if the analyst has physical access. This list is not intended to be comprehensive, nor is it intended to provide adequate detail to perform any specific compromise, but rather intended as being demonstrative of some of the typical methods often employed.

3.4.2 Remote Access to Target

When physical access to the target is not possible or advisable, it may be necessary to compromise the system remotely. There are a variety of ways to do this, depending upon the target's habits and unique computing profile. Here again, a comprehensive description of how to compromise a system in order to gain access to it is outside of the scope of this paper. That said, there are a few categories of attack that readily come to mind.

- **Remote management with access**. If the analyst has access to the target system with some form of privilege, it may not be necessary to perform any type of "hack" attack at all, but rather use the built-in management features of the system to obtain information. This would especially be the case of in-house investigations by organizations that are able to manage their assets, such as systems that are joined to a Windows Active Directory environment. Similarly, if the analysts were able to obtain the password with other means, they may be able to connect to the system and manage it in this way. This type of interaction with the target system is preferable in that it is less likely to be adversely affected by anti-virus software which might block the investigator or alert the system user to the investigation. Given a valid password,

37 http://www.keelog.com/
38 http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle

simple methods such as creating a command shell over the network using psexec[39] or ssh[40] may be more than adequate for the purposes of the investigation.

- **Remote management without access**. If the analyst can identify and connect to the target system, but does not have legitimate credentials on the system, it may be possible to use conventional "hacking" techniques to compromise the system. This might include taking advantage of un-patched software using tools such as Metasploit, using default passwords or performing password guessing attacks, or taking advantage of improper configurations to escalate privileges. Although it is possible, this type of attack is typically more difficult than other types, creates more fourth-amendment issues, and is less likely to be successful with any one given machine. Often, it is easier to compromise a system that is *trusted* by the target machine, and use that trust relationship to compromise the machine itself. For example, in a corporate environment, there are often many servers that all participate in a Windows Active Directory network. If even one of these can be compromised, it may be possible to escalate this access to domain administrator, and then use this access to compromise the target workstation. Using this approach makes the field of potential targets much larger, and hence increases the chance of finding a way in. In any event, remote network attacks are often thwarted by local firewalls (both hardware and software) and by anti-virus software, and could alert the system user to what is happening.

- **Phishing and social engineering**. An approach that is generally more successful for compromising a target machine is by enticing the user to compromise themselves. This may include tricking them into installing software containing malware, attacking them through web sites controlled by the analyst, exploiting Cross-Site Scripting vulnerabilities[41] or through sending e-mails containing malicious content. One often-successful approach involves sending HTML e-mails to a target and tricking the Windows operating system into authenticating to a remote server (and thereby obtaining the user's password hash) in order to obtain the HTML images it needs to render properly[42]. The Social Engineers Toolkit, mentioned previously, has a number of modules that can be used for remote compromises, and is intended to make this task easy to perform.

- **Service manipulation**. As with physical access, if it is possible to compromise the underlying systems upon which a target relies, it may similarly be possible to compromise the target itself. This is especially true of directory services, DNS, e-mail services and similar.

Again, there are any number of ways to attack a system remotely, and these attacks will typically require not only skill but creativity to do successfully. A variety of training options exist to improve an analyst's skills in these techniques, but none are better than experience.

3.4.3 Bypassing Remote Analysis

It is conceivable that during the target penetration stage it will be determined that there is a compelling reason to immediately seize the equipment and employ conventional forensic techniques. This is especially the case if, for example, it is determined that no encryption is in use on the target system and that a valid user credential has been obtained and tested. Similarly, there may be concerns

39 http://technet.microsoft.com/en-us/sysinternals/bb897553
40 http://en.wikipedia.org/wiki/Secure_Shell
41 https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29
42 http://www.foofus.net/?page_id=63

that the target will obscure evidence, possibly physically destroying it, before it can be examined. In these instances, a Hostile Forensics operation may simply seize the machine and use the information and access already obtained while in custody of the computing systems. Obviously, this would require legal authorization to seize the equipment.

3.5 Identification, Tagging and Backdooring

Once the analysts have gained access to a system, they will want to clearly identify the system and may want to create ways to access the system in the future. In particular, the ability to link a machine that has been accessed remotely with a piece of physical hardware is essential. If an analyst wishes to use evidence that was obtained remotely, for example evidence that was seen and recorded using screen-capture software while accessing the system over the Internet, they will probably need to be able to ultimately link that activity to a specific piece of hardware, and hopefully the hardware's user. Similarly, one of the first tasks to perform when getting remote access to the system is to ensure that future access will be possible. Regardless of the method used to initially access the system, be it a valid administrative password or an exploit, it is possible that this method will be unavailable in the future, which could put an end to the remote analysis.

3.5.1 Identification

In order to uniquely identify the target system, the analysts will want to identify and record as much information about the target as possible. Ideally, this will be information about hardware, rather than software, as it will allow analysts to match the information obtained remotely with the information obtained by a physical analysis of the hardware. On Windows systems, it would behoove the investigator to make complete copies of system and user registries, as these may contain useful identification data. Some pieces of information that *should* be unique to one, and only one, piece of physical hardware include:

- **Ethernet MAC addresses**. Each wireless or wired Ethernet card should have a unique Media Access Control[43] (MAC) address. This MAC address can be obtained using software queries, and then compared against the physical hardware later. MAC addresses are used by the ARP protocol, and can often be tracked within network equipment to find the physical location of a device. For example, given a MAC address, a system administrator may be able to find the exact switch port that a machine is plugged into, and then trace that wire to a specific physical location such as an office. It should be noted that MAC addresses can be forged or spoofed very easily, and virtual machines hosted by software such as VMWare may also not have unique MAC addresses.
- **Computer serial numbers**. These are sometimes accessible through queries to the BIOS. In Windows[44] and Linux[45] using available software and scripts. Major hardware manufacturers such as Dell, IBM, and Hewlett Packard typically store machine serial numbers in the BIOS.
- **Volume and disk serial numbers**. Each hardware disk and the logical data volumes residing on them have a unique serial number associated with them. The analyst should be aware that there are significant differences between hardware and logical serial numbers, and different

43 http://en.wikipedia.org/wiki/MAC_address
44 http://support.microsoft.com/kb/558124
45 http://www.nongnu.org/dmidecode/

ways of obtaining them. In Windows and Macintosh, a physical serial number might be obtained using software such as DriveDetect[46], and in Linux using hdparm[47]. Volume serial numbers, where used, can be pulled from the Windows registry using software such as RegRipper[48].

- **Identify encryption hardware and software.** The analyst should attempt to identify any unique encryption hardware such as key fobs, dongles, two-factor ID devices, One-Time Password software on mobile devices[49], Human Interface (HID) security devices or even removable media that may contain encryption keys. This information may sometimes be found by looking for devices that are plugged into USB or other communication ports on the system. It may also be possible to identify the use of these devices through key loggers. For example, it is common to see two-factor ID tokens used in such a way that the analyst may see key-logged login sequences with a user ID, followed by the enter key being pressed, followed by a password consisting of a consisting of a 4-6 character PIN number plus a 6-character random number. In this case, the 4-6 digit pin number is likely the "password" and the remaining characters generated by a hardware device. Many encryption software packages require that a device be plugged into the computer or otherwise used (for example reading a changing two-factor ID number from a device) before drives can be decrypted. With luck, these devices will still be plugged into the system after it has been booted so that it can be identified through probing of the hardware. On-site physical observation of the computer boot-up process would be an ideal way to identify if external hardware is required. Even if the analyst is able to later determine the password for encryption software, this information may be useless without the hardware devices used by the encryption software. If these hardware devices are not identified, they may not be seized later, thereby making any encryption passwords obtained unusable.

3.5.2 Tagging

Once the system has been uniquely identified, the analyst *may* want to "tag" or leave behind some change on the system that can prove that they were able to access the machine. This may mean creating a small file, a registry entry, or some other piece of unique identification such as a case number and employee ID number. Then, when the system has been physically obtained, they can view this tag to verify the machine's identity. Whether or not to leave a tag should be decided ahead of time, and the tag itself should be small and unique so that no two systems contain the same tag. Even a modification as small as this tag goes against conventional forensic best practices, in that the analyst is actively modifying data on the target system. For example, it is possible that simply by making this tag, some small (but critical) piece of data may be over-written. It is up to the operation's management to decide if the risk of data loss is outweighed by the importance of uniquely matching hardware to on-line activity.

46 http://www.seagate.com/ww/v/index.jsp?locale=en-US&name=How_To_Find_Model_and_Serial_Numbers&vgnextoid=3bd256390c14e010VgnVCM100000dd04090aRCRD
47 http://en.wikipedia.org/wiki/Hdparm
48 http://regripper.wordpress.com/
49 http://motp.sourceforge.net/

3.5.3 Backdooring

Even more controversial than tagging a system is creating a "backdoor[50]" or way to get subsequent access to the system. This may mean creating new user IDs, changing passwords, or installing software on the target. Again, the decision of whether or not to create a backdoor should be decided by the operation's management based on an analysis of the risks versus the gains of doing so. In this case, the operation needs to be concerned not only that they may delete critical information by placing data on the system, but also that the backdoor itself might be abused by others. There has been precedent for backdoors being so abused. For example, software deployed in video games by Sony (without the user's knowledge) as part of their Digital Rights Management platform has indeed been abused by third parties[51]. If a backdoor is installed, care should be taken that this backdoor cannot be easily discovered and used by others – perhaps by locking down use to specific IP addresses, programming it to automatically delete itself after a certain amount of time has elapsed, or other controls. If backdoors created by third parties are used, they should be reviewed through code analysis to ensure that they do not contain functions that could compromise the investigation such as undocumented passwords or "phone home" technologies. Even if the backdoor that is used is of known quality and cannot be easily abused by third parties, there is still a risk of this action being negatively perceived in court, or that the suspects may use the "malware defense" whereby the target may attempt to create doubt about whether it was indeed their actions that were observed, or if there was some third party "doing all of the bad things." Also, backdoor software may be detected by anti-virus software and alert the user to the investigation. This can sometimes be circumvented by first disabling anti-virus systems, creating new backdoor software using new techniques, or using executable encryption and packing[52] technologies, but this is not guaranteed to be successful and could allow a system that was previously secure to become insecure due to the analysis. If a previously secure machine were compromised due to analysts' actions, this could expose them to legal liability or cause other problems for the investigators. In order to prevent future malware from infecting the system during the analysis, restarting the anti-virus software is recommended when possible. While installing a back door may help to ensure long-term access to a system, it certainly creates significant legal and technical issues that should be carefully considered.

3.6 Remote Analysis

Using the remote access obtained during previous steps, the system can be analyzed and searched for evidence. There are a number of open source and commercial tools for this purpose, often marketed as "enterprise forensic" products. These tools can be used to perform a live analysis of storage media, running programs, network activity, and memory content, or even image (copy the contents of) the machine over the target's network or the Internet. There are such a large variety of tools and options that can be used during this phase that any information documented here would soon be out of date. It is recommended that an analysis of the current best-of-breed open source and commercial software be performed to determine which best matches the budget, features required, and employee skill set of the forensic operation.

50 http://en.wikipedia.org/wiki/Backdoor_%28computing%29
51 http://www.kaspersky.com/news?id=173737204
52 http://en.wikipedia.org/wiki/Executable_compression

3.6.1 Remote Analysis Tool Capabilities

Remote analysis can be conducted in a very simple way from the command line, through a remote desktop or similar graphical user interface, or (more typically) using an agent/server system. The following list includes a number of features that would be advantageous in a remote forensic tool. Some inspiration for this list was provided by a document entitled "Design and Implementation of a Remote Forensics System " by FoundStone[53].

- **Secure**. The software components are reasonably free of security flaws. Evidence of a third-party security audit of the software should be obtained from the vendor, if commercial, or source code reviewed if open source. A security assessment of the tool should be performed before it is used. Testing should include, at a minimum, any database, web and components that interact with the network. Verify that the tool is free of issues such as SQL injection, that databases are secured, etc. Tools should be built or compiled from reviewed source code, rather than downloading executables or through package management tools whenever possible. Use tools such as Nessus[54] for general assessments, and WebInspect[55] for web components. Similarly, there should be specific guidance on how to securely deploy the product, and this guidance should be used to configure the product.
- **Role-based access control**. Ideally, the tool will uniquely identify users, enforce strong passwords, and allow for role-based access control. For example it is typical to see cases assigned to individual analysts within the tool based on a need-to-know basis, and varying levels of access such as administrator, analyst, and report viewer defined.
- **Use of encryption.** The tool should use strong encryption for all network communications. This includes communications between the agent and server components, as well as between the various layers of the server application itself. For example, if a web interface is provided, HTTPS encryption should be used. If a database is used, the database connection should be encrypted. In general, any place in which one component talks to another should be validated as supporting encryption, with a special emphasis on any communications that take place with the target or across a network.
- **Cross-platform support**. A good forensic tool will allow for analysis of Windows, Macintosh and UNIX-like operating systems. There are a number of unique issues with each operating system, and the tool should be able to analyze their unique characteristics.
- **Application support.** The tools should be able to process forensic artifacts for commonly found applications such as Internet browsers and servers, Instant Messaging, archivers, e-mail clients and servers, and programs such as iTunes that are of interest to a forensic analyst.
- **Stealth capabilities.** For a Hostile Forensics operation, the ability to remotely analyze a machine without alerting the target to this activity would be ideal. This may be as simple as not displaying a GUI or icon on the taskbar, or as complicated as actively attempting to evade notice from anti-virus software and in running process lists.
- **Remote imaging support**. The product should be able to remotely image the target system over the Internet. This should include random access memory, physical drives and logical

53 http://www.mcafee.com/us/resources/white-papers/foundstone/wp-design-implement-remote-forensic-system.pdf
54 http://www.nessus.org
55 http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA1-5363ENW&cc=us&lc=en

drives. Native support for encryption products would be helpful, as this would allow the imaging process to access the physical drive more directly, but logical volume imaging can be used as a last resort to image encrypted volumes that are mounted and active. Having a built-in rate-limiter to control how much network traffic is used at any given time for imaging will help avoid drawing attention to the tool's use. Similarly, a tool that can dynamically *increase* the amount of bandwidth it uses based on computer usage (for example while the computer is idle) could help to reduce the amount of time needed to create the image. The ability to take "snapshots" and identify only those disk sectors or files that have changed, and to create a "differential" image would also help in an investigation that takes place over an extended period of time.

- **Memory analysis and volatile data collection**. The tool should be able to enumerate running processes, network communications, shared library use, open file hooks and other volatile data. A strong memory-analysis component will help to identify sophisticated software such as malware that may attempt to hide itself from conventional operating system functions. For an example, see Mandiant's free Memoryze tool[56] or similar.

- **Minimal footprint.** Ideally the tool will create a minimum of changes to the target system. Having agents that run, for example, only in memory or that have a small size when stored to disk will help to minimize the amount of modification to the target system, and hence the amount of explanation that might be required when presenting evidence in court.

- **Minimal operating system trust.** In many cases, the state of the remote target's operating system will be unknown, and could have malware already present such as rootkits. As such, the target operating system should not be considered trustworthy. To address this problem, the tool should use low-level interactions with hardware to the greatest degree possible. Similarly, if shared libraries (i.e. DLL files) are required, these should be statically linked to the executable so that the operation of the tool will be predictable.

- **Scripting support.** A tool should support custom-written scripts and reports that can be developed ahead of time and used to quickly and consistently gather data or perform analysis of the target system. Use of open scripting languages such as Perl[57] or forensic-specific scripting languages such as EnScript[58] are frequently used.

- **Hash set support**. A tool should be able to identify known-good and known-bad files by querying a hash set database such as those provided by the National Science Reference Library's RDS project[59] or links at the e-evidence info[60] and hashsets.com[61] web sites. Using these hash databases can be especially useful for identifying anti-forensic software such as encryption that an analyst would want to circumvent. Similarly, hash sets exist for known child pornography and hacking software which could be useful for remotely identifying evidence.

- **Logging.** As one of the greatest issues with a Hostile Forensics analysis is likely to be proving exactly what actions were taken by analysts, the tool will ideally have built-in logging and

56 http://www.mandiant.com/products/free_software/memoryze/
57 http://www.perl.org/
58 http://download.guidancesoftware.com/AP3mq7h/Ya2fXpTBP6G2wMiiUBXHFyGGc4N4Qg+hR1vM8dGC1yhIfQkUeLnnDIN0
59 http://www.nsrl.nist.gov/nsrl-faqs.html
60 http://www.e-evidence.info/projects.html
61 http://www.hashsets.com

auditing capabilities. It should be possible to log from the agent to a management server, as well as locally on the agent.

- **Evidence preservation and chain of custody**. Tools should attempt to store, track and protect original and derivative evidence including images, collected data, notes and reports adequately. This will include controls such as hashing of evidence, performing read-only access to file systems, and other controls typically associated with the preservation of computer forensic evidence.

Again, the above list is not intended to be comprehensive, but may be a good starting point for a set of criteria that can be used for developing or purchasing a remote forensic tool.

3.6.2 Remote Analysis Tool Goals

The goal of the remote analysis phase is to identify evidence on a remote system, often volatile data that would not be available on a machine that is powered down, and to minimize the risk of anti-forensic software such as encryption from adversely affecting the investigation. Each case will be different, and may have different goals, ranging from identifying hacking activity to intellectual property theft to child pornography. With that in mind, some tasks that might be performed remotely could include:

- **Identify software**. The analyst will want to identify what software is used on the target system, with a specific emphasis on security systems such as encryption, cache cleaners, drive wipers, password safes, etc. Identification of common software applications and versions such as Adobe Acrobat, Java Runtime Engines, etc. can be helpful in identifying attacks that could be used to gain future access to the system. Identify client software that may be frequently used to connect to servers such as databases, accounting systems, etc. Identify software that has on-line communication capabilities, including video games such as World of Warcraft. Also attempt to identify malware, as these programs may compete with the analyst for resources, draw attention to the software running on the system, or cause difficulty in court.
- **Analyze operating system configuration.** It is useful to know how the operating system is generally configured. For example, is it part of a Windows domain? Does it have hard-coded information such as DNS servers or host to IP address mappings? Does the machine use Windows update over the Internet, or to an internal server? Are complex passwords required and when was the last time that passwords were changed? What disks and volumes have been connected to the system? Does the system have file roll-back or journaling capabilities such as Windows' Volume Shadow Copy[62] or Macintosh's Time Machine[63]? Can the machine be remotely interacted with via remote desktop or VNC?
- **Identify system users and passwords**. Having access to system passwords and password hashes can greatly facilitate the speed and depth of a forensic analysis. Consider both operating system and application passwords, especially for e-mail and web sites. Beware of obtaining, and actually using, passwords for third party systems such as e-mail, forums, etc. as this may be illegal, especially when performed by non-law enforcement analysts. In terms of system passwords, be alert for administrative level accounts that could be used to manage the server, or used to gain access to other systems for which a trust relationship exists.

62 http://computer-forensics.sans.org/blog/2008/10/10/shadow-forensics
63 http://www.apple.com/macosx/what-is-macosx/time-machine.html

- **Profile system usage.** In addition to those items identified in previous phases, identify how the target system is typically used. For example, does the system have more than one user? what web sites do they typically visit? What time of day is their system used? What type of data is stored on the system? What Internet history records exist? Are there Internet history records for driving directions or hotel / airline reservations? Are there pictures with GPS metadata in them? With whom does the user typically communicate? What networks has the user connected to? Is the system backed up, and if so how?
- **Obtain volatile system data**. Obtain information about running processes, network connections, contents of the Windows registry, etc. If possible, update this information regularly, as the target may use certain software infrequently. Obtain a copy of system memory, either by imaging hardware RAM or by obtaining swap or temporary files.
- **Obtain system log data.** Obtain data such as Windows event logs, IM chat logs, network usage (especially wireless access points discovered, as this may help in linking a remote system to a physical asset) and syslogs which may contain data that could be quickly removed or overwritten. They may be useful in linking a specific individual to a specific machine. For example, if an analyst were able to prove that a target logged onto a system using a two-factor authentication token[64], this would greatly help in proving that it was indeed the target's activity that has been discovered.
- **Data imaging**. Image (copy) the contents of memory as well as files or whole volumes, depending upon the circumstances. Use file hashing, where possible, to identify files and whether or not they have been modified.

Obviously, there are any number of things that an analyst may want to look at, and this list is far from comprehensive. Regardless of what is done, however, it is essential that the analysts understand what impact they are making on the system through their activities. For example, when doing a live system analysis, new files, registry and log entries may be created, and file metadata such as the last time of access may be modified by the analyst. These effects must be understood so that they can be explained at need, especially in a way that could be understood by a non-technical judge or jury. When the impact of a particular tool or procedure is not known, it is advised that it be tested on a test system first. Additionally, it is preferable to have a script or written procedure to use when performing live system analysis, as this will reduce errors as well as make the process easier to explain and repeat.

It may be the case that the investigation will for some reason not include a seizure and physical examination of the evidence. In this event, the process may move directly to report writing. This is more often the case in incident response projects, where an analyst may be investigating an attack on a production server that cannot be taken down because of the impact on business operations. It may also be the case that the physical system is outside of the jurisdiction of the examiners, or that it has been destroyed or hidden and cannot be found. Any evidence gathered in an investigation of this type may be difficult to use in a court setting, which typically requires that trustworthy primary physical evidence be at hand. However, legal proceedings are not always the goal of a Hostile Forensics operation. For example, the machine may only be analyzed in order to gain access to other systems that *are* of interest and might be penetrated as part of the investigation. It may be determined that a target workstation is encrypted with software that the analyst cannot bypass, but that there are backup encryption keys stored on another machine or in directory services. This is especially the case of Windows Encrypting File

64 http://en.wikipedia.org/wiki/Two-factor_authentication

System[65] (EFS) when used in an Active Directory environment. In this event, an on-line only investigation might be used to obtain these credentials, which could then be used to unlock the evidence that is of interest. In these types of examples, documentation and a good report are still necessary components of a hostile forensic process.

3.7 Physical Seizure

After a period of remote analysis, it is likely that the physical workstation will be seized. Consult the Department of Justice Search and Seizure guide discussed earlier for more guidance on this topic. As extensive information exists on this topic, and different jurisdictions may have different requirements, this topic is considered out of scope for this paper. However, as noted previously, the analysts do need to prove that the computer they are seizing is in fact the same machine that has been analyzed remotely. To this end, the analyst should validate that the information such as computer serial number, disk drive serial number, and Ethernet MAC addresses correctly match. Ideally, photographs of the serial numbers will be taken. Serial numbers for computers are usually located on external sticker or tags. Serial numbers for hard drives are typically located on the top of the drive itself, thus likely requiring that they be partially removed from the computer. Serial numbers for Ethernet MAC addresses are sometimes printed on very small stickers on the Ethernet cards, or in the case of a laptop on the service tag.

During seizure, it is important to attempt to obtain volatile data from the target system one last time before unplugging it or turning it off. Hopefully, passwords were obtained previously that could be used to unlock any locked consoles or software packages. As before, notes should be kept on what steps are taken so that they can be explained later if necessary. As should be obvious, one risk that analysts face at this point is that the system may lose power or reach some other condition that causes the system to shut down, lock, unmount an encrypted volume, or otherwise inhibit analysis. If the workstation is already unlocked it may be helpful to disable screen savers or console locking features. In the latter case, it is in fact possible to unplug a computer from the AC wall outlet and keep it powered up without the console locking until a more stable power source can be found using products such as Wiebtech's mouse jiggler[66] and HotPlug[67] devices. This may allow an analyst to move a powered-up machine to a lab environment for a more detailed analysis of volatile data.

It is also important to secure computing and data storage devices that are stored near the target workstation or on the person of the suspect. For example, this may include flash drives, memory chips, external hard drives, two-factor ID devices, cell phones, digital cameras, CDs and DVDs, MP3 players and anything else that could be used to store data. Be aware that some storage devices can be very small or cleverly hidden. At the time of this document's authoring, a Micro-SD memory chip with 32 Gigabytes of data measuring only 11mm x 15mm x 1.0mm can be obtained for less than USD $60 and can store an extensive amount of evidence. These chips can be easily hidden in books, be taped to the undersides of desks, placed under stamps, or even swallowed or otherwise concealed on the suspect's person. Flash drives may also be hidden in glue sticks[68], devices that look like cigarette lighters[69], bottle openers[70] or toys, among many other possibilities. Not only can these devices directly store data,

65 http://en.wikipedia.org/wiki/Encrypting_File_System
66 http://www.wiebetech.com/products/MouseJiggler.php
67 http://www.wiebetech.com/products/HotPlug.php
68 http://www.geekologie.com/2009/05/geekologie_reader_make_usb_glu.php
69 http://www.thinkgeek.com/gadgets/electronic/aacd/
70 http://www.thinkgeek.com/homeoffice/kitchen/e00f/

they may also store encryption keys (small files of information required to decrypt data). If all digital media are not identified and seized, it is possible that an analyst might obtain a target's encryption key password but not be able to use it because they were not able to find the storage device containing the encryption key that it matches.

3.8 Local Analysis

As analysis of a physically seized workstation is well documented elsewhere, the primary issue for this paper is the circumvention of the target's anti-forensic features. Obtaining a comprehensive copy of unencrypted data, including deleted data still in existence on the hard drive, is the most important issue. Some issues that may be experienced by analysts include the following:

- **Circumventing disk encryption.** Hopefully, the analyst has obtained the information required to access the computer, even after it has been turned off and restarted. Often, it is whole-disk encryption that is in place, and this will require a valid encryption key[71] and password before the system can be booted or imaged. Usually, whole-disk encryption uses keys that can both encrypt and decrypt data, but other systems such as file and e-mail cryptography may use more sophisticated public-key cryptography[72]. Imaging an encrypted hard drive without the key will result in unusable data. In some cases, it may be possible to mount this encrypted drive image on another machine or in a virtualization environment using software such as LiveView[73] and decrypt it with a password, but this is not always the case (especially for encryption that uses a hardware trusted platform module). In some cases, disk encryption software will store the encryption key locally on the computer and only a password will be required to use it. However, this is not always the case, and some encryption programs will require a two-factor ID token, a cryptographic hardware module, cell phone, or a flash drive. Some encryption software may also contain features that will wipe or otherwise destroy encrypted media when a "duress password" is entered. Hopefully these required items have already been identified during the on-line analysis and included in the warrant. It is *very* important to carefully identify and seize any devices that could be used in this way. In some cases, target workstations may use the same password for disk encryption that they use for logging into the operating system. In this case, simply cracking the locally stored password (in the Windows SAM file or /etc/passwd file) may suffice. It may also be the case that the disk encryption software can be unlocked through administrative rights to the machine (for example a Windows Domain Administrator) or an emergency encryption key with a weak password stored on a disk somewhere. In general, most disk encryption vendors *do not* keep an administrative back door or recovery method, but this should be verified in the event of an emergency.
- **BIOS passwords.** As it may be required to create a logical image of a data volume after the system has booted, it is possible that a boot password will be configured to protect the machine. These boot passwords are stored in the BIOS and must be entered before the disk is accessed. In some cases, it may be possible to use a default password installed by the vendor, physically replace the BIOS chip with a chip with a known password, set a jumper to clear the BIOS settings, or perform other attacks. However, be aware that cryptographic information or disk locking information might be stored in the BIOS, and could be *permanently lost* if not carefully handled. If the machine can be booted to a floppy drive, CD or USB device, or network server

71 http://en.wikipedia.org/wiki/Key_%28cryptography%29
72 http://en.wikipedia.org/wiki/Public-key_cryptography
73 http://liveview.sourceforge.net/

it might be possible to temporarily disconnect other bootable devices on the system and boot a device with a password reset or recovery boot disk.

- **Hard drive locking.** Some computers will be configured so that a specific hard drive must be plugged into a specific computer in order to access that disk. Worse, as noted previously, it is possible that the target system may actively attempt to delete data when it is plugged into a different system. For this reason, check the hardware's capabilities before taking any steps. If hardware security is in place, consider creating a disk image by using a boot disk on the target workstation and imaging to an external hard drive or across the network.
- **Solid State Drives.** As previously noted, some solid state drives may perform "garbage collection" routines that could actively delete data on a target's media, *even when connected to a write blocker.* At the time of this document's authoring, methods to stop this from happening appear to be few and difficult to implement. It may be necessary to develop customized SSD controller circuit boards that do not perform these cleanup routines or analyze the memory chips outside of the SSD platform in order to avoid this issue. If a SSD is identified, it is important to leave this device powered off until an approach can be devised. Unfortunately this recommendation is directly opposed to the recommendation to capture volatile data on the scene. The decision on how to proceed might be based on whether or not there is any indication that the user recently deleted files – perhaps because they were aware of an impending search and seizure operation.
- **On-site hacking over time.** It is possible that physical evidence that has been seized simply cannot be adequately accessed by the analysts. However, if the system boots up and a long enough period of time has elapsed, the analysts might get lucky and be able to penetrate a system months or years after it has been obtained. For example, if the machine automatically obtains and IP address on the network and does not use a local software firewall, it may be possible to penetrate the machine using tools or exploits that did not exist when the machine was seized. Similarly, it may be possible to defeat some hardware counter-measures such as disk locking through new techniques. Periodically revisiting old cases and systems over time may turn up new evidence, although analysts must be careful to comply with the requirements in warrants or other legal processes that were originally used to obtain the media.

Once a readable and unencrypted copy of the target's media has been obtained, conventional forensic techniques can be employed to identify evidence. It is assumed that the Hostile Forensics team is qualified and capable of performing this work, and that proper chain of custody controls will be used.

3.9 Report Generation

A key component of any forensic process is the proper documentation of findings. If the Hostile Forensics operation does not already have a template, there are a number of guidelines and examples from Internet sites such as ForensicsFocus.com that can be used as a starting point. Useful guidance from the U.S. Department of Justice's National Institute of Justice's document entitled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement"[74] provides the following tips for a items to include in a good report:

- Identity of the reporting agency.

74 http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

- Case identifier or submission number.
- Case investigator.
- Identity of the submitter.
- Date of receipt.
- Date of report.
- Descriptive list of items submitted for examination, including serial number, make, and model.
- Identity and signature of the examiner.
- Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
- Specific files related to the request.
- Other files, including deleted files, that support the findings.
- String searches, keyword searches, and text string searches.
- Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity.
- Graphic image analysis.
- Indicators of ownership, which could include program registration data.
- Data analysis.
- Description of relevant programs on the examined items.
- Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.
- Results/conclusions.

In addition to these, some additional documentation that is specific to a Hostile Forensics operation might also be included:

- Description of target, as determined during target profiling, including items such as on-line habits, forums visited, networks used, individuals communicated with, etc.
- Description of procedures used during the physical compromise of the machine. For example, how was the wireless network cracked, or a monitoring switch port configured. If services such as DNS were compromised in order to gain access to the system, describe how this was done.
- Description of the investigative process, with an emphasis on how long the on-line phase took place, what IP addresses and physical locations were observed, key events, etc.
- Description of the on-line methods used to gain access to the remote workstation, and their likely impact on physical evidence. For example, what penetration tools such as Metasploit were used? Was data stored to disk, creating the possibility that some files may have been lost? Was file metadata such as time of last access changed during on-line searches? Were Most

Recently Used[75] (MRU) registry entries or prefetch files created by the analyst? Were user IDs created? Was software installed or modified?

- Description of anti-forensic controls in place on the target system and how they were circumvented (if appropriate). If supplemental hardware such as key fobs were seized and used, provide a description of how these systems work. Detail if software packages such as privacy disk wiper software were modified or disabled.
- Identification and analysis of volatile data such as network connections, memory contents, running programs, etc.
- Identification of system passwords and hashes obtained, and the method used to obtain them (key loggers, rainbow table attacks on password hashes, etc.) Identify any chain-of-trust relationships between target machines, such as shared administrator passwords.
- Matching of unique system characteristics discovered during the on-line investigation (Ethernet MAC address, disk serial numbers, etc.) with physical evidence obtained after search and seizure. In addition to physical evidence, create a clear link between data volumes observed while on-line with those physically seized and analyzed.
- Summary of findings and identification of future systems that should be analyzed, new tools or techniques to develop, or other recommendations for improvement either in the investigative process
- Summary of the internal controls of the Hostile Forensics operation that would increase the trustworthiness of the evidence.

4.0 Internal Controls on the Hostile Forensics Operation

As noted above, establishing an adequate system of internal controls will be a critical factor in the success of any Hostile Forensics operation. Simply saying that an analyst saw certain types of evidence, or even taking screen shots of evidence, is not likely to be considered adequate to obtain a criminal conviction. A more convincing set of assurances will likely be needed to convince interested parties that the analysis occurred as stated. Indeed, it is possible that no amount of explaining or internal controls will be able to convince a judge or jury beyond a reasonable doubt. In some cases, it may be enough to simply link the on-line data with physical evidence through such things as serial numbers, but this may not be enough. For example, what if the analyst observed (and even documented) some piece of critical evidence that was seen during the on-line assessment, but this data cannot be found during the physical assessment? It could well be that the data is lost and is not recoverable. In this case, having additional controls that promote confidence in the evidence may make the difference whether or not it can be used. Internal controls will need to be established both for the operation itself, such as how the lab is controlled and protected from malicious use, and for the on-line and physical analysis work as well. In the former example, the analysts may be be interested in controls such as a formal machine build and hardening system, log review to identify abuse, or secure deployment of penetration and forensic tools. In the latter case, they may be more interested in controls such as screen and key loggers that can be used to document what was seen and done.

75 http://www.forensicswiki.org/wiki/MRU

4.1 Operation Accreditation

The process of identifying and establishing internal controls is complex, but a variety of resources are available to do this, including accreditation agencies such as the American Society of Crime Lab Directors[76] which lists 385 accredited labs as of June, 2011. Of these, the vast majority are law enforcement operations.

The controls that any specific Hostile Forensics lab will require will vary by location and over time. Indeed, as this is relatively uncharted territory, which controls are considered most appropriate for a Hostile Forensics operation have yet to be determined through standing precedent. That said, the benefits of a well-controlled lab are clear. In a good article entitled "Building FBI digital forensics capacity: one lab at a time"[77] by Douglas A. Schmitknecht, the author gives the following rationals for accreditation of a Regional Computer Forensic Lab (RCFL)[78] by an organization such as the ASCLD:

- *Improves quality* - Accreditation will heighten the quality of the RCFLs services because an independent, impartial and objective team of experts will review the laboratory's findings and operations.
- *Strengthens operations* - Accreditation ensures that an RCFL is abiding by criteria that are designed to assess performance, while also strengthening operations.
- *Establishes standards* - With accreditation, the general public and the users of the RCFL are assured that the laboratory is following established and widely accepted standards.
- *Enhances quality control* - Accredited laboratories must follow appropriate quality controls and quality assurance procedures.
- *Guarantees Examiner qualifications* - ASCLD/LAB requires that laboratories have certified Examiners on staff. All RCFL Examiners must undergo the FBI's CART[79] certification process, and may not perform examinations independently until doing so. (Trainees may need anywhere from six months to a year of training before they are certified.) Certification implies that an individual has a certain body of knowledge, and counters a recent trend where an investigator is deemed an ''expert'' after taking a short course in digital forensics.
- *Protects evidence* - ASCLD/LAB accreditation focuses on evidence handling procedures, to ensure that evidence is not damaged or misplaced.
- *Ensures accurate results* - Accreditation can enhance forensic results by requiring sufficient written protocols that serve as an empirical basis for the most basic and complex procedures.

The opinions of the author cited above seem a good summary of the benefits of not only the ASCLD process, but of any well-run Hostile Forensics operation. However, not every organization has the time, resources or motivation to go through such a formal process. Similarly, it may be the case that the process of Hostile Forensics is sufficiently different from conventional forensics that the very process of penetrating a remote workstation in order to circumvent anti-forensic techniques would render an operation unable to obtain an outside accreditation. In the following section, a method for developing an internal controls framework will be discussed.

---

76 http://www.ascld-lab.org/
77 http://www.rcfl.gov/downloads/documents/DigitalInvestigator.pdf
78 http://www.rcfl.gov/
79 http://www2.fbi.gov/hq/lab/org/cart.htm

4.2 Internal Controls Development

In order to develop a documented system of internal controls, it is helpful to have a framework to work within. In the experience of the author, the combination of a Business Impact Analysis (BIA), often used as part of Disaster Recovery / Business Continuity Planning, combined with an appropriate set of formal security controls, may suffice. Ideally, the Hostile Forensics environment will be compartmentalized in order to limit the scope of the systems for which controls must be developed. Thus, it is preferable to have, for example, a standalone lab that is "air gapped" from the rest of the environment, with the possible exception of Internet access. In this way, the analyst will not need to develop internal controls for every single device in the organization, but rather only for that subset that actually involved in the forensic process. This will make developing internal controls less expensive and less time consuming. Another factor to keep in mind when developing these controls is that they *must* be documented and repeatable. Simply developing ad-hoc standards that are (presumably) followed by staff will not be sufficient to impress stakeholders and clients with the authenticity and trustworthiness of the evidence that is produced. One way to think about the level of formality needed is to look to the Capability Maturity Model[80] (CMM), and its associated levels.

4.2.1 The Capability Maturity Model

The Capability Maturity Model is particularly adaptable to assigning an objective rating to the security controls that the organization has established. There are five levels defined along within the CMM. In general, the more effective the control is, the higher the rating will be. As per the Wikipedia.org reference given above, the five levels can be described as follows:

1. **Initial** (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.
2. **Repeatable** - the process is at least documented sufficiently such that repeating the same steps may be attempted.
3. **Defined** - the process is defined/confirmed as a standard business process
4. **Managed** - the process is quantitatively managed in accordance with agreed-upon metrics.
5. **Optimizing** - process management includes deliberate process optimization/improvement.

So, for the purposes of a Hostile Forensics lab, the operation will need such things as preservation of evidence and chain of custody having a high ranking, around 3 or 4, as this is a critical factor to the trustworthiness of evidence. However, not all controls will be as easy as this to plan out ahead of time, especially controls such as documentation for hands-on forensic or penetration work. In these cases, it may be reasonable to see a new tool or technique used in an ad-hoc fashion while keeping notes (levels 1-2) the first time, then documented adopted as a standard procedure (levels 2-3) and possibly even monitored and improved over time to see how often the process is successfully used (levels 4-5). Although the author does not recommend pursuing formal CMM certification or implementing a large and complicated set of CMM-based controls, keeping the CMM in mind when developing internal controls can be a very useful tool, and is used in the following BIA methodology.

4.2.2 The Business Impact Analysis

Arguably one of the more difficult tasks is analyzing and documenting business processes. The first order of business is to identify which individuals will be working to establish controls on the

80 http://en.wikipedia.org/wiki/Capability_Maturity_Model

Hostile Forensics operation. This would likely consist of representation from each of the disciplines (penetration and forensics) as well as at least one manager, and ideally a lawyer. The individuals in this workgroup will attempt to map business processes at a high level down to specific technological assets at the lowest level. The ultimate goal of the BIA process is to come up with a good list of specific assets including hardware, software, services and information that can then be mapped to a set of internal controls, as will be shown in the following sections. Obviously, the exact details of what processes and controls will be used will vary widely from organization to organization, but good documentation of these is essential.

The BIA process developed by this author has five discrete phases, which are found in different tabs in the BIA worksheet:

- **I** – Identify Business Processes (BP). Often mapped directly to a specific department or team. For example, a penetration team or administrative team.
- **II** – Identify Process Tasks (PT). This maps to tasks that are regularly performed by the business units, for example, performing Nessus scans or hashing and storing log data.
- **III** – Identify Required Resources (RR). These are the assets that must be available in order to perform the tasks. In the example of Nessus, you might need AC power, a local area network, an Internet connection, an Internet router, a firewall, a server, the Nessus software and a valid license. Required resources can be hardware, software, information, or services. While identifying these resources, attempt to identify all of the system's dependencies that may not be immediately apparent, such as license keys and services provided by third parties such as DNS and encryption vendors.
- **IV** – Identify Internal Controls (IC). These are the systems and procedures that are in place in order to promote security, consistency, and reliability of the Hostile Forensics operation. Ideally, these controls will help in producing evidence that is trustworthy. For example, internal controls might include video recording of analysts' screens, documented hardening procedures, employee pre-employment screening, firewall logging and log review, system patching, etc. These controls will ultimately be mapped to specific resources identified previously.
- **V** – Map controls to resources. At this point, a matrix will be made that lists resources and the controls which apply to them. This will help the analysts to keep track of the various documents and procedures that will be created and maintained over time, and will also help the analysts to identify systems that may be lacking in controls.

For the purposes of this exercise, imagine a small, private sector Hostile Forensics operation called “Sycophant Incorporated” that helps large companies with internal incident response and forensics. Using the BIA process, the first order of business will be to document business processes (BPs), which might be in four very simple categories:

I	BUSINESS PROCESS	DESCRIPTION
BP.1 Administration		Includes staffing, payroll, budgetary work, coordinate with legal counsel, project management, managing the evidence inventory,maintains documentation and maintains shared resources such as the department file server, etc.
BP.2 Penetration		Performs profiling and penetrations of remote systems, configures physical systems such as network monitors and sniffers, cracks passwords, installs keyloggers and backdoors, etc.
BP.3 Remote Forensics		Performs remote forensic investigations of systems, especially volatile data and memory analysis. Responsible for devising ways to circumvent anti-forensic controls such as encryption. Limited disk imaging, operating system and filesystem artifact analysis.
BP.4 Local Forensics		Assists in search and seizure, circumvention of anti-forensic controls on seized hardware, detailed analysis of operating system and filesystem artifacts.

Once these business processes have been established, the next step is to detail what these functional groups do on a day-to-day basis. At this level, Business Processes (PTs) are identified within these business processes as in the following examples:

II	IDENTIFICATION OF BUSINESS PROCESSES & PROCESS TASKS	
Business Process	**Description**	**Process Tasks**
BP.1 Administration	Includes staffing, payroll, budgetary work, coordinate with legal counsel, project management, managing the evidence inventory,maintains documentation and maintains shared resources such as the department file server, etc.	BP1.PT1. Maintain Internet Connectivity
		BP1.PT2. Maintain E-Mail and IM Servers
		BP1.PT3. Internal File and Print
		BP1.PT4. Maintain evidence locker and custody info
		BP1.PT5. Maintain Documentation & Report Templates
		BP1.PT6. Maintain Project Workload & Change Mgt.
		BP1.PT7. Internal and External Communications
		BP1.PT8. Staffing and Training

II	IDENTIFICATION OF BUSINESS PROCESSES & PROCESS TASKS	
Business Process	**Description**	**Process Tasks**
BP.2 Penetration	Performs profiling and penetrations of remote systems, configures physical systems such as network monitors and sniffers, cracks passwords, installs keyloggers and backdoors, etc.	BP2.PT1 Maintain and Use Nessus Server
		BP2.PT2 Maintain and Use Metasploit Server
		BP2.PT3 Maintain and Use Exploit Script Database
		BP2.PT4 Maintain and Use Wireless attack equipment
		BP2.PT5 Maintain Hardware Keyloggers and Sniffers
		BP2.PT6 Research and Development of Tool as Needed
		BP2.PT7 Maintain Cracking Server and Rainbow Tables
		BP2.PT8 Report authoring

II	IDENTIFICATION OF BUSINESS PROCESSES & PROCESS TASKS	
Business Process	**Description**	**Process Tasks**
BP.3 Remote Analysis	Performs remote forensic investigations of systems, especially volatile data and memory analysis. Responsible for devising ways to circumvent anti-forensic controls such as encryption. Limited disk imaging, operating system and filesystem artifact analysis.	BP3.PT1 Maintain and Use Enterprise Forensic Tools
		BP3.PT2 Maintain and Use Memory Analysis Toolkits
		BP3.PT3 Maintain and Use Incident Response Toolkits
		BP3.PT4 Develop and Install Backdoors as needed
		BP3.PT5 Report Authoring

Once process tasks are identified, the final step in the BIA process is to identify the specific hardware, software, information and services required for each process task.

III	APPLICATIONS & RESOURCES USED IN PROCESS TASKS			
Business Process		**Process Tasks**	**Required Resources**	**Notes**
List one business process per worksheet		*List the high-level tasks identified in previous worksheets.*	*List the systems and storage devices where data for this business process is stored, processed, or transmitted through*	*Describe any special conditions or notes*
BP1. Administration		BP1.PT1. Maintain Internet Connectivity	RR1. DSL ISP Router	Maintained by Qwest
			RR2. Cisco ASA 5520 Firewall	ASA 8.2 OS
			RR3. *SRVLOG*	SRVLOG hardware – Compaq DL360
			RR4. Windows 7 Enterprise on SRVLOG	OS on server SRVLOG
			RR5. Sawmill on SRVLOG	Software on SRVLOG
			RR6. OSSEC on SRVLOG	Hostbased intrusion detection / prevention on SRVLOG
			RR7. Kiwi Syslog on SRVLOG	Software on SRVLOG
			RR8. Internet Service from Qwest	DSL 5120k / 640k Router
		BP1.PT2. Maintain E-Mail and IM Servers	RR10. *SRVWEB*	SRVWEB hardware – Compaq DL320
			RR11. Ubuntu 10.4 on SRVWEB	OS on SRVWEB
			RR12. Squirrelmail on SRVWEB	Primary mail server on SRVWEB
			RR13. SILC Server on SRVWEB	Real-time encrypted messaging server, IRC
			RR14. OSSEC on SRVWEB	OSSEC HIPS on SRVWEB
		BP1.PT3. Internal File and Print	RR15. SRVFILE	SRVFILE hardware – Compaq DL360
			RR16. Ubuntu 10.4 on SRVLOG	OS on SRVFILE
			RR17. Samba on SRVLOG	Windows-compatible file sharing software
			RR18. OSSEC on SRVFILE	OSSEC HIPS on SRVFILE
		BP1.PT4. Evidence locker and custody	RR19. Inventory of Evidence bags	
			RR20. Chain of Custody Records	Printed documents and plastic tabs in locked cabinet
			RR21. Locked Evidence Room and Keys	Locked room, keys distributed only to manager

Once the assets have been identified, the internal controls that will be applied to them must be detailed. For guidance on general internal security controls, consider using the excellent National Institute of Standards and Technology library of documents[81], and in particular the document 800-53 Revision 3, 800-86[82] for forensics and incident response, and 800-72[83] for PDAs. For an overall control framework, also consider ISACA's CoBIT[84]. ITIL best practices documents also contain helpful guidance. For specific internal controls related to a forensic operation, consider the items required to become ASCLD accredited, as discussed previously. In general, any control identified on this list will have one of the following kinds of documentation:

- Procedural documentation – i.e. a written plan on how to do something, such as hardening an analyst's workstation, how to review logs (and what to look for), or how logging systems are to be configured.
- Compliance documentation. - i.e. a written checklist, log book, or other system that keeps track of activities performed. For example, it may be a list of all the tasks that need to be performed by an analyst each day, and the analyst will check off and initial that he completed each of the tasks that day. Or, it maybe be documentation that a procedure has been performed on a specific resource, such as tracking that each system has in fact been hardened. This is intended to ensure that workers are doing everything they should be doing, and that they can prove this to an auditor should it be necessary.
- Log documentation – i.e. raw data from the various tools and systems. This may include nessus scanning logs, operating system logs, packet logs, or anything else that is generated during the work day. These logs must be uniquely identified (for example with a SHA-1 hash) before they are moved into long-term storage.

Although far from complete, a list of internal controls might look something like the following:

IV	Common Name	Description
IC1.	Tool Vetting	Tools are analyzed by source code or behavior
IC2.	Activity logging	Log all OS, App and packet data
IC3.	Log Analysis Review	Review Sawmill report daily
IC.4	Screen recording	Analyst screens video captured daily
IC.5	System Hardening	Documented procedures to harden software
IC.6	Daily review, checksum and storage of activity logs	Video and packet logs hashed SHA-1 daily and stored
IC.7	Yearly Security Training for I.S. staff	SANS / CSI classes, local Infragard
IC.8	Yearly account access audits	Look for out of date accounts, bad passwords

And finally, it is now possible to create a mapping or cross-referencing between resources and controls. Note that in the following example, rather than designating just a “yes” or “no”, a numeric value that maps back to the CMM rating is used. If a simpler system is desired, one could alternately use a simple X to designate compliance. Or, if more detail is desired, one could make three columns for each control, designating whether procedural, compliance and log documentation is maintained for each control.

81 http://csrc.nist.gov/publications/PubsDrafts.html
82 http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
83 http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf
84 http://www.isaca.org/Knowledge-Center/cobit/Pages/Products.aspx

Required Resource	Note	IC1. Network ACLs	IC2. Activity logging	IC3. Log Analysis Review	IC.4 Screen recording	IC.5 System Hardening	IC.6 Daily review, checksum and storage of a	IC.7 Yearly Security Training for I.S. staff	IC.8 Yearly account access audits			
RR1. DSL ISP Router		3	3	3		3	3		1			
RR2. Cisco ASA 5520 Firewall		3	3	3		3	3		1			
RR3. *SRVLOG*						3	3		2			
RR4. Windows 7 Enterprise on SRVLOG			3	3		3	3		2			
RR5. Sawmill on SRVLOG						1			1			
RR6. OSSEC on SRVLOG			2	2					1			
RR7. Kiwi Syslog on SRVLOG												
RR8. Internet Service from Qwest												
RR10. *SRVWEB*						3	3		1			
RR11. Ubuntu 10.4 on SRVWEB		2	3	3	3	3	3	1	2			

Obviously, this internal controls system is not the right solution for every organization, and the list of controls is far from complete. That said, this simple system may be of use to starting organizations, and does at least provide a framework in which the operation could develop its controls in a documented and understandable way. A copy of the spreadsheet used here will be provided as an appendix to this document.

4.2.3 Example Controls – Sycophant, Inc.

To better illustrate an example of a Hostile Forensics organization and its internal controls, once again consider the fictitious private-sector company, Sycophant Incorporated. The reader may assume that this organization already has in place many of the typical internal controls that would be expected of a mature I.T. operation such as change control, disaster recovery, regular vulnerability assessments, etc. In addition to these, the following controls might be used:

- **Segregation of duties** – Administrative duties are separated from the technical groups, limiting administrator access to servers and software. Physical access to the facility and its evidence is restricted only to the administrative team. Role based access control is granted on a need-to-know basis, and administrative passwords are not shared between groups unless a compelling business need exists. When sensitive tasks are performed that involve segregated individuals, two or more individuals will formally acknowledge the tasks completion. For example, both the administrator and an engineer may both need to review and "sign off" on the daily activity logs. Information from one department, such as the programmers who create backdoor software, will not be shared with those who will be regularly using it, except in as much as is necessary to perform their regular job function.
- **Network Segmentation** – Systems used for local analysis are "air-gapped" or disconnected from other network systems. The administrative networks running file shares and e-mail

systems are on a separate network from penetration and remote analysis systems. Internet access is allowed only on the administrative and remote analysis networks, and users must authenticate before gaining outgoing access. Egress filters block outgoing access except for a small set of protocols such as DNS, HTTP, and SSH for non-penetration networks.

- **Hardened forensic software** – The team has created a formal hardening document for their main forensic tool Access Data Lab. Encryption is used for communications between components. A unique database password has been created. Role based access control is used to limit analyst access to a "need to know" basis. Software firewalls are used to allow access only to those ports which are explicitly required for client and inter-system access. Systems are scanned for security flaws regularly using Nessus.
- **Tool validation** – Tools are evaluated before being used. Ideally a source code review will be performed. If source code is not available for commercial products, external certification or accreditation is used, and proof of a third-party security audit is required. For binaries for which source code is not available, tools are tested and monitored both in a hardware test lab, and in a virtual machine lab, to identify questionable activity.
- **Anonymous Internet and proxy services** – Two broadband Internet connections have been purchased (DSL and Cable modem) with an "undercover" subscriber name. TOR Onion routers are used on an as-needed basis to obscure the source of network traffic, and an anonymous SOCKS proxy service is contracted from www.proxyshop.net. Ideally, these services will be hosted in data centers with fast network connections that can absorb Denial of Service attacks.
- **Secure backdoor software** – The backdoor software that is installed on target machines has been designed to be highly secure. The software performs extensive logging and requires a two-factor ID token with a constantly changing authentication key in order to log on. These tokens are stored in the evidence cage each night, and distributed by the administrator each morning.
- **Hardware key loggers** – Hardware key loggers are configured on analysts' workstations. Each morning the administrator plugs in the key logger before booting up the computer, and notes the serial number of which logger was used with which system. At the end of the work day, the key loggers are removed by the administrator, and the text file of keystrokes is downloaded to the server. A SHA-1 hash is created for each log file before it is stored. A spreadsheet listing the day, computer, analyst and SHA-1 hash is maintained. A written work log is kept by the administrator noting the tasks performed. Key loggers are kept in a safe, and the combination is known only by the administrative team.
- **Screen recording software** – TechSmith's Camtasia software is used to record the video from analysts workstations. These video files are SHA-1 hashed by the administrator at the close of business each day and compressed. A written work log is kept by the administrator noting the tasks performed.
- **Wireshark packet logs** – A network SPAN port is configured to mirror network activity from the penetration and remote analysis networks. A fast computer workstation is configured with the WireShark protocol analyzer, and full packets are captured to a local hard drive. Logs are rotated at every 10 Megabytes. Packet logs are SHA-1 hashed by the administrator at the close of business each day and compressed. A written work log is kept by the administrator noting the tasks performed.

- **Random inspection and log review** – The administrator randomly visits analysts throughout the day to discuss the state of the project and what is being done by the analysts at that time. For example, noting the time of day, which systems and tools are in use, what IP addresses are involved, etc. This information is recorded by the administrator. Periodic spot checks are performed by the administrator by reviewing key logs, video capture logs, and packet logs to match visually observed behavior with the log files. If there is a discrepancy, it is noted and investigated.
- **Evidence and information management** – A formal evidence room is maintained by the administrator according to best practices in preservation of evidence and chain of custody. A database is used to track items within lockup. All items entering or leaving the cage are signed for by two parties (one receiving the item, and one releasing it). Periodic backups of captured activity logs are stored to an external USB hard drive and to tape daily after close of business and placed in the lockup. Full backups on encrypted tapes are taken off-site to Iron Mountain weekly.
- **Mandatory training and vacation** – All employees are required to obtain at least one week per year of specialized security training, preferably with SANS.org or equivalent, and employees are encouraged and compensated for obtaining industry certifications. Cross-training is encouraged. Employees are required to take vacation each year, during which time they will have no access to systems within the operation, which might allow detection of deceit that would otherwise be detected if the employee were there to cover it up.
- **Anti-fraternization policy** – There is an explicit policy forbidding the fraternization of employees in the administrative and technical groups outside of work. An anonymous ethics hot-line is established and advertised, so that anonymous complaints or concerns can be submitted for review. Failure to comply with this policy will result in disciplinary action, up to and including termination of employment and possible legal action.
- **Project management** - There are one or more individuals formally tasked with tracking the status and activity of each case. These individuals will be in a separate segregated group, and will report to an individual outside of the group (not the department administrator). These individuals will serve as an additional control against possible collusion, as well as being responsible for conventional project management duties.
- **Tool documentation** – The tools that are analyzed and used by the Hostile Forensics group are documented, and this documentation can be provided to internal and external stakeholders to better understand how these tools function, including opposing counsel. This information should be kept up to date, and protected from modification or disaster.
- **Time synchronization** – The target workstation and the systems actively used by the Hostile Forensics operation will either be time-synchronized, or the time delta (difference) between the systems will be recorded each day before work is performed. This will help to better match analyst activity with the resultant artifacts found on the target systems.

While not perfect by any means, the above set of controls is demonstrative of what might be found in a controlled Hostile Forensics operation. As might be obvious from the above list, there is a strong emphasis on separation duties – particularly between the administrative team and the analysts and logging the activity of workers. These controls are tracked in detail, and can be audited by third

parties, and thus may help in creating evidence that is considered trustworthy. In order to access a target system, it is necessary to have access to a two-factor ID token that is stored in a locked location when not in use, minimizing the risk of an analyst attempting to access the system outside of the work environment. Due to there being three types of logs that are collected and hashed each day, it would be difficult, although not impossible, for an unethical analysts to "frame" a target and attempt to modify the activity logs at a later time to cover it up. In order for this to occur, it would most likely require collusion between the administrator(s) and the analysts, which is hopefully limited by the anti-fraternization policy. These controls protect not only the operation, by making the evidence more trustworthy, but also the target, as it would be much more difficult for an unethical employee to take inappropriate actions such as "framing" a suspect.

5. Conclusions

Whether or not Hostile Forensics, as described here, will ever become a commonplace practice remains to be seen. In many situations, the penetration and subsequent analysis of a remote system may not be the most productive investigative approach, and may not even be a good idea due to the myriad legal and technical issues. This could be addressed through legislative action designed to allow Hostile Forensics activities within a legal context, although hopefully in a way which does not infringe upon the rights of the individual. I hope that the ideas and guidance outlined in this paper will at least present a starting point for how a Hostile Forensics operation might be structured with at least some level of oversight and transparency, and perhaps even one that could produce usable results. I also hope that should hostile forensic methods be used, that they will be done in an ethical way that protects the rights of the a suspect as well as the Hostile Forensics operation.

6. Acknowledgements

In addition to the many excellent resources referenced in this document, I would like to thank the individuals who assisted with reviewing and commenting on this document prior to publication, including Dave Ihnat, Peyton Engel and others who have declined to be identified.

7. About the Author

Mark Lachniet is a security engineer for a large fortune-500 company and frequent presenter at security conferences and seminars. Mark has performed hundreds of security projects including penetration tests, forensic investigations, and practices and procedures audits over more than a decade. Mark is a licensed private investigator in the State of Michigan, and holds a number of industry certifications including a SANS GIAC Certified Forensic Analyst (GCFA) Gold, Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) among others.