Annual ADFSL Conference on Digital Forensics, Security and Law

2011
Proceedings

May 26th, 1:30 PM

Digital Forensics Investigation in A Collegiate Environment

Robert E. Johnston
CISSP, System Office, Connecticut Community Colleges, Hartford, Connecticut, rjohnston@commnet.edu

DIGITAL FORENSICS INVESTIGATION IN A COLLEGIATE ENVIRONMENT

Robert E. Johnston, CISSP
92 Carriage House
Enfield, CT 06082-6042
Telephone: 860-776-2055 Cell: 860-539-9206
Fax: 860-741-6418 (by arrangement)
E-mail: bjohnston@e-computer-security.com

Connecticut Community Colleges
System Office
Connecticut Community Colleges
61 Woodland Street
Hartford, Connecticut 06105
Telephone: 860-244-7763 Fax: 860-244-7886
E-mail: rjohnston@commnet.edu

ABSTRACT

Creating, building, managing a cost effective digital forensics lab including a team of qualified examiners can be a challenge for colleges [1] with multiple campuses in multiple towns, counties and states. Leaving such examination responsibilities to each of the campuses results in not only disparity in the results but more than likely excessive duplication of efforts as well as the potential for compromise of evidence. Centralizing the forensic efforts results in a team that is not subject to the political pressures of a campus and virtually eliminates the possibility of examiner favoritism. Learn what it takes to create a cost effective centralized digital forensics lab. It sounds simple but is truly quite complex when you consider the chain-of-custody issue as well as the management support needed during initial implementation. There will be resistance at some of the campuses while others will welcome the removal of a burden. We will also examine why such a lab is necessary and what can be learned about compliance to existing policy as well as the possibility of identifying the need for additional policy/standards.

Keywords: digital forensics investigation malware criminal chain-of-custody centralized lab

1. THE CHALLENGE

Implementing centralized digital forensics investigation within a widespread enterprise can be difficult. There are numerous fiefdoms involved, many of which hold self-serving interests which are contrary to such a project. No matter how much sense it may make it is not uncommon to meet massive resistance. The initial acceptance of the concept will often be the greatest challenge its advocate will ever face!

Knowing your organization including the individuals involved in blocking or supporting such a project is usually necessary in the collegiate environment. After all, commonly each campus is quite independent from central management whose role is primarily that of obtaining funding and setting budgets with some over site relative to more sensitive issues which certainly vary from college to college and private versus the public sector. Some intelligence gathering is often essential to achieve success.

Do not jump in whole hog without knowing the terrain. Plan….plan….plan….

2. JUSTIFYING THE PROJECT

Your greatest challenge is the justification. The balance of effort will be a piece of cake in comparison but quite tedious at times. Care must be taken to ensure clarity and understandability. Often the justification will be read by those who are unfamiliar with information technology and especially the whole concept of digital forensics. To many digital forensics is just another term and very possibly is simply an adaptation of the term forensics which has become so popular today in the field of law enforcement. Many cannot relate that forensics in science and information technology is an analysis technique which ensures that should illegal activity, whatever that might be, be found that the evidence is preserved in a manner consistent with that which is acceptable to law enforcement and the courts.

More than likely very few if any digital forensic investigations regarding malware infestations will uncover criminal activity. However, it is entirely possible and you must be prepared. How embarrassing would it be to the college if a staff or faculty member was detected with sums of child pornography on the system including trading/sale of same but could not be prosecuted due to inadmissible evidence? Take it a step further and envision that identifying that staff member to law enforcement results in a determination that the staff member is also a child molester yet could not be prosecuted due to the principle of “fruit of the poisonous tree” [2]. Surely, this something everyone at every level wishes to avoid.

Preservation of evidence is not the only justification. The remainder relates to traditional management concepts/needs.

2.1 Control

In order to ensure that the evidence (the malware infected device; specifically, the hard drive in the case of an infected computer) is preserved in a manner satisfactory to law enforcement, etcetera it is imperative that effective control is maintained throughout the process commonly referred to as the “chain of custody” [3].

This requires the creation of detailed records of the handling and storage of a physical drive from the time it is taken into possession by the information technology staff through and until the drive is successfully and properly forensically imaged. In an ideal world the physical drive would be preserved until it is established that there is not a criminal concern. However, in reality this is not practical in most environments. The number of duplicate drives at each site likely would be excessive.

While efficient, this centralized process does tie up each drive for several days even with the creation of a forensic image archive. There is the transportation in both directions as well as the time in the forensic lab. Unless generously configured there will be times when a drive sits for two to three days at the forensic lab until it has been successfully archived. As a result the average amount of time a drive to be investigated is out of service is likely five business days. Also, the drive will remain unusable for another day or so until it is wiped and reimaged. Thus, it is impractical to leave the impacted user without a computer. Therefore each campus will need to keep a sum of drives on hand and ready to go when infections occur.

In addition there is the issue of control while in the forensics lab. As will be seen later, there are additional control benefits in the decentralized lab.

2.2 Savings

The question to be answered is whether the work which needs to be done is being accomplished and, if so is it complying with all of the issues relative to evidence preservation? If no, an analysis is required to determine why and identify the savings that can be realized through centralization. If yes, then the issue is a comparison of costs between the current processes versus that of centralization.

More than likely if you are considering a centralized digital forensics lab either the current process is not effective or does not exist but there should be a perceived need. Need takes many forms, constant reinfection being one of them along with compromise of PII [4] or PCI DSS [5] information as well as other information under development which should not be disclosed until ready; in other words competitive information which also exists in the collegiate world, especially within the private sector.

2.2.1 Constant Reinfection

The primary cause of constant reinfection is the failure of a specific campus that does not follow proper procedures when an infection occurs. With a centralized digital forensic lab such failures become readily apparent and corrective actions can be initiated.

2.2.2 PII Compromise

When PII is compromised the rules/regulations/laws vary from jurisdiction in addition to the ethical obligations. Hopefully your college already has a published policy regarding compromised PII. When compromised PII is detected by a centralized digital forensic lab you are assured that the resulting actions meet current requirements. The embarrassment that might occur should non-compliance be discovered and reported by the media could result in incalculable damage.

2.2.3 PCI DSS Compromise

Failure to comply with the Payment Card Industry Data Security Standard [5] likely will result in unfavorable media coverage as well as the real potential for the loss of rights to process payment cards on campus in a convenient manner.

2.2.4 Compromise of Competitive Information

Development of new majors/minors and other strategies including the development of new for fee services are commonly business confidential until they are made public.

2.3 Staffing

The initial staffing size is difficult to calculate but certainly should be far less than when such examinations are conducted at each campus. Staffing size is also dependent upon the working model. Experience indicates that the decentralized lab requires a smaller staff in addition to offering other advantages and efficiencies. In a typical environment, when a thorough examination is conducted of each case to include production of a written report that can be read and understood at the campus by non-information technology professionals, the average time per case is two hours.

2.4 Influence, Bias, etcetera

In a centralized model the examiners are sheltered from all forms of overt influence and bias as well as friendships. It is quite common in a collegiate environment to “protect their own”, especially when the unknown or misunderstood is encountered. All too often senior staff and faculty become concerned that the case may impact their career, especially when they are unaware of peers encountering similar problems. Dealing with the matter centrally and properly managing the entire process can and should eliminate this concern.

3. CREATING, BUILDING AND MANAGING A COST EFFECTIVE DIGITAL FORENSICS LAB

This is not a seat-of-the-pants project. Careful planning will result in successful implementation with little or no disruption to existing operations. Key to this process is choosing the appropriate model and while there are perceived advantages to both, the decentralized model offers greater flexibility and opportunity.

3.1 Models

3.1.1 Traditional Lab

The traditional lab is totally centralized and frequently is completely isolated from all other information technology activities. This represents a great deal of cost which can be minimized in the decentralized model. Typically, in the traditional lab the forensic examiners are solely responsible for all activities from creating the archives to mounting the drives to be examined on their dedicated forensic examination work station. Commonly, the examiner works from the console of the work station.

There are variations, many of which will be described in the decentralized lab. However, most of the initial costs of the traditional lab cannot be avoided.

3.1.2 Decentralized Lab

The concept of a decentralized lab is foreign to many yet much of its structure is similar to the traditional lab and many of its features can be implemented in the traditional lab.

Basic Concept: Compartmentalize the many responsibilities of the digital forensics lab thus ensuring a higher level of confidence and trust in its integrity while allowing some of the activities to be performed “remotely”.

Forensic computers: Locate in a truly secure data center, preferably not located on the campus of any of the colleges. Day to day support of the forensic computers is performed by operations staff to the extent necessary to mount and dismount cases being examined.

Examination/Archive copies: Examination and archive copy functions are commonly created by the same operations staff which supports the forensic computers. Thus, once a drive to be examined arrives on site only operations staff trusted to support forensics ever handles the original physical drive as well as all copies.

Forensic Examiners: Examiners access their assigned forensic computer remotely even when they are physically based on site. Thus, examiners can be located anywhere they are able to connect securely into the forensic network. Thus, should there be qualified forensic examiners on one or more of the campuses they can be reassigned to the new forensic team. In addition, in today’s world of digital mobility a valued team member can be retained should it be necessary for that team member to not live in the region.

Forensic Network: The forensic network must be carefully architected to be isolated from the balance of the college network and access to that rigidly managed and monitored as well as restricted to forensic staff only! Logical maintenance of the forensic computers is the responsibility of the assigned examiner. Physical maintenance is the responsibility of forensic trusted operations staff.

3.2 Building the Lab

The cost of building such a lab can often be minimized if the college’s network architecture already has a centralized data center providing common services to all of the campuses. For those without this option must consider whether to co-locate on an existing campus or completely off-site. Costs can be minimized with co-location providing that the forensic staff work environment is isolated from the general campus environment. Failure to do so compromises many of the benefits of a centralized digital forensics lab.

3.2.1 Hardware

Hardware must be robust but not necessarily state-of-the-art. Forensic tools have not been that quick to jump to the latest hardware architecture and likely will not abandon support for earlier platforms which support XP. There may be some concerns regarding XP relative to Internet access yet since such actual access should only be performed in a virtual mode that is not likely to be a near term issue.

Clearly, XP platforms being replaced with Win7 etcetera can be utilized in the lab. Components of the platform will require replacement for best performance as well as maximizing memory and external ports. Also, some hardware write blocks, at least one per forensic computer will be needed. As hard drives keep growing in size it may be appropriate to examine the case drive directly and based on the result determine whether an archive image copy is needed.

3.2.2 Software

There are numerous software tools available. While there are other examination tools, serious consideration should be given to choosing Encase [6]. It does require some training/experience to be effective with Encase, but in the end it is the tool which is trusted in law enforcement circles should they become involved. Beyond Encase, a trusted VM tool is needed as well as several other tools which should be considered:

- Automated registry decoder; e.g., Registry Ripper [7]
- View the Registry in native mode; e.g., Registry Viewer [8]
- Tool to locate and identify PII/PCI DSS data; e.g., Identity Finder [9]
- Tool to evaluate links; e.g., Link Examiner [10]
- Linux-like environment for Windows making it possible to port software running on POSIX systems (such as Linux, BSD, and Unix systems) to Windows; e.g., Cygwin [11]
- Possibly a network meeting tool; e.g., TeamViewer [12]
- VM tool; there are many to choose from.
- Sandbox Tool; e.g., Sandboxie [13]
- Key Recovery; e.g., Recover Keys [14]

3.2.3 Staffing

All members of the forensic team must be chosen for their skills, experience and trustworthiness. Fortunately it is very likely that you will be able to identify within your current professional staff. If not, perhaps within faculty. In today’s job market it is possible you can locate key staff locally at reasonable cost. Choose your staff carefully as their duties require not only competency and loyalty but also trustworthiness.

4. LEARNING OPPORTUNITIES/ADVANTAGES

Unlike having forensic examiners at each campus, operating a centralized digital forensics lab will provide benefits difficult to achieve without one.

4.1 Image Maintenance

Hopefully there are image [15] standards in place. Due to the challenge of distribution and installation from a centralized facility most colleges provide imaging standards on each campus. Ideally, there are standards set centrally which describe image content, frequency of refresh, etcetera.

Forensic examinations can readily identify where those standards are not being maintained and thus corrective action can be initiated.

4.2 Consistent Practices

One of the challenges of managing multiple locations is that of consistency. In addition, it is not that uncommon to come across practices at one location which are an improvement over that which is practiced at other sites. Whether the result is that of bringing all sites into alignment or learning what is better than a current practice, it is nothing but distinct value.

Another concern is that of inconsistency; for example, a situation develops that results in management/clients/media noting a problem that could have been avoided had it followed a practice at site D, and why aren't sites B, C and E also following site D's model?

4.3 Building Trust/Confidence with the Campuses IT [16] Security Staff

While it is not uncommon for the IT Security teams at each campus to be initially wary when a centralized digital forensic facility is created, when done carefully it will result in a trust relationship which otherwise might not have been built. Over time it is more than likely that a query will be received from an IT Security staff member or manager regarding a specific incident. When clear concise explanations are offered while avoiding the implication of blame, trust develops; especially when it is possible to point out how such situations can be avoided in the future.

5. SUMMARY

Selling the concept of a centralized digital forensics facility/lab in the collegiate environment can be challenging. The basic premise of campus independence/autonomy will always be an issue. However, the fact of the matter is that there is much to be gained and learned through centralizing digital forensics as well as a potential significant cost savings.

No two colleges or campuses are identical. For campuses, location in terms of distance from the college is a large consideration/influence. None-the-less, a serious examination of the potential benefits of a centralized digital forensics lab should be performed.

6. AUTHOR'S BIOGRAPHY

Robert E. Johnston, CISSP, is an experienced information security professional, Bob has performed security services from coast-to-coast, and overseas, regarding all aspects of information security, including contingency planning, for large and small businesses. Having been the senior information security officer for major financial institutions he brings the vision and experience of a senior corporation executive and the broad knowledge developed while servicing his consulting clients. Bob maintains technical competence in critical areas including Networks/Internet/Intranet components (e.g., HTML, JAVA, Active-X, TCP/IP, Firewalls, E-mail), Information Security (e.g., PGP, RACF, CA-Top Secret, CA-ACF2, CICS, Cryptography), LAN/WAN (e.g., Windows 95, 98, NT, W2K, XP, Vista, Win7) as well as all hardware platforms, security concepts, standards and policies. He has served as an expert witness in Federal/State criminal/civil cases and GAO Administrative hearings and, conducted several successful computer forensic investigations within the financial services sector as well as within the undergraduate collegiate sector. A recognized expert, he has made more than 100 presentations worldwide and has written more than 100 articles published in numerous periodicals and journals. As a highly skilled information security professional, the International Information Systems Security Certification Consortium (ISC)^2 awarded him the designation of Certified Information Systems Security Professional (CISSP) in 1995.

7. REFERENCES

[1] college – For the purposes of this paper a college is defined as the parent college of a group of colleges at varying locations. Often the colleges not on the primary campus are run quite independently; almost as if they are not truly affiliated with the parent college.

[2] fruit of the poisonous tree – https://secure.wikimedia.org/wikipedia/en/wiki/Fruit_of_the_poisonous_tree

[3] chain of custody – https://secure.wikimedia.org/wikipedia/en/wiki/Chain_of_custody

[4] PII – https://secure.wikimedia.org/wikipedia/en/wiki/Personally_identifiable_information

[5] PCI DSS a.k.a. Payment Card Industry Data Security Standard – https://secure.wikimedia.org/wikipedia/en/wiki/PCI_DSS

[6] Encase – https://secure.wikimedia.org/wikipedia/en/wiki/EnCase and http://www.guidancesoftware.com/

[7] Registry Ripper a.k.a. RegRipper – http://regripper.net/?page_id=120

[8] Registry Viewer – http://www.softpedia.com/get/Tweak/Registry-Tweak/Registry-Viewer.shtml, http://accessdata.com/media/en_us/print/techdocs/Registry%20Viewer.pdf and http://accessdata.com/downloads/current_releases/rv/AccessData%20Registry%20Viewer.exe

[9] Identity Finder – http://www.identityfinder.com/

[10] Link Examiner – http://www.simplecarver.com/free/ and http://www.analogx.com/contents/download/network/lnkexam/Freeware.htm

[11] Cygwin – http://www.cygwin.com/

[12] Team Viewer – http://www.teamviewer.com/en/index.aspx

[13] Sandbox Tool – https://secure.wikimedia.org/wikipedia/en/wiki/Sandbox_%28computer_security%29 and http://www.sandboxie.com/

[14] Recover Keys – http://recover-keys.com/

[15] image – operating system image; http://publib.boulder.ibm.com/infocenter/tivihelp/v13r1/index.jsp?topic=/com.ibm.tivoli.tpm.img.doc/bootsrv/csfi_images.html

[16] IT – information technology; https://secure.wikimedia.org/wikipedia/en/wiki/Information_technology

APPENDIX – SAMPLE FORENSICS EXAMINATION OPERATION

AUTHOR

Robert E. Johnston, CISSP, November 1, 2010, eMail: bjohnston@e-computer-security.com

OVERVIEW

This paper was prepared for a professional discussion group that wanted a basic explanation of a forensics lab. Since the group consisted of virtually all private sector business security professionals you will find that it avoids reference to the collegiate environment and I tried my best to make it usable in the private sector. Common abbreviations are not explained and abbreviations created for convenience in the paper are "explained" the first time they occur. In addition, you will find for your convenience a complete list of abbreviations at the end of this document.

INTRODUCTION

Forensics Labs can take many forms. The reason for preparing this model is that it was requested by someone who wanted "model procedures" to which I responded that there is not truly a model that is uniform to all situations. I believe that the following dissertation will make that abundantly clear yet possibly assist him in his assignment/endeavor.

This is based on an existing "successful" lab supporting an enterprise consisting of 12 remote locations and a central office, all within a single state. Some of the practices contained herein clearly will not work due to physical distances elsewhere. Understand that the distance from the central office to any remote site does not exceed 60 miles with the majority within 30 miles. On the other hand, why does the lab exist?

After all, there are commercial labs committed to the recovery of information; criminal labs intended to identify illegal activity as well as many others including the enterprise which focuses upon network compromise including PII, PCI and HIPAA issues. The lab to be illustrated is concerned with network compromise, PII and to a limited extent PCI matters. At the same time such labs cannot ignore the possibility of the discovery of illegal activity whether fraud, extortion, child pornography or other criminal activity. While an enterprise might consider such possibility to be infinitesimally small, the possibility should not be ignored!

Once one starts examining a hard drive, it is amazing what might be discovered. It truly ranges from criminal activity to massive waste of resources and time as well as proper usage of enterprise resources. While, for the most part the discovery of such activity not in the best interest of the enterprise must be concluded on an individual basis, that option does not exist for some activity that must be reported to law enforcement as the result of legislation. Thus, it is incumbent upon every forensic activity to ensure that the "chain of custody" is maintained lest damage to the image of the enterprise and/or violation of law occur when such activity is revealed but cannot be prosecuted and possibly the offender cannot be reprimanded under corporate guidelines.

CHAIN OF CUSTODY

When an event occurs at a Remote Office (RO) a notice is sent to the Central Office (CO) advising of the issue and requesting advice as to the necessity of a forensic examination. A prompt reply is provided confirming the need or offering technical advice when one is not needed.

Systems to be forensically examined have their drive(s) removed by authorized IT personnel at the RO and a record kept of that individual as well as the reason for submission and details regarding the drive's identity on the RO Control Sheet (CS). The drive(s) is/are transported to the CO by one of several authorized individuals and their identity is recorded along with the date and time on their CS. The CO CS will record all drive handling from imaging through to return. The forensic examiners (FEs) never touch the original drive, imaged drive or the archived version.

THE FORENSIC LAB

Forensic labs are designed in many forms while, hopefully, meeting the objectives of management and excellent business practices. All sorts of issues must be taken into consideration including available resources (space, staff, objectives and etcetera). Many labs are the actual work space of the examiners. Others adopt a more flexible environment by placing the lab in the data center environment where the operations staff supports the forensic computers and the examiners connect to them remotely, never having physical contact with the hardware.

Having operations perform all of the drive handling issues ensures knowing where the responsibility lies as well as having the FEs totally focused upon their responsibilities of case examination and reporting.

There clearly are advantages to both, but when all is said and done, procedurally many find the latter arrangement to be the most advantageous. Once the drive is imaged and archived the image drive is mounted on a forensic computer and the responsible FE notified; all of which is documented on the CO CS.

THE EXAMINATION

FE activity commences with the creation of a virtual drive for a malware scan for all cases. However, before the malware scan may be started specific “history files” must be created so that the result of the malware scan and further activity can be properly documented. Using a naming standard created for the forensic examinations all of the preliminary work of creating the temporary storage directory (TSD) and propagating much of the content including copies of all quarantined items, an extract of each of the major components of the registry and a boiler plate copy of the FE’s report (FER) to be populated as the FE continues through to completion is created by a custom program created for this activity. The FE then initiates the rescan directing the result be stored in a sub-directory of the TSD.

Then, a copy of the RO notice is created in the TSD and a summary of its content entered into the FER. Dependent upon the reason for examination the FE proceeds to review the many resources captured in the TSD while the malware scan continues to completion. Once completed any malware infestations detected will be documented in the FER. When necessary, commonly for every examination, the drive will be opened with a forensic examination tool and the details of the content of the drive will be examined for the specifics needed to document and close the case.

When completed the FE will submit the FER to management for final disposition. From the FE’s perspective the case is closed and all documentation is noted as closed including entries in the CS of the RO and CO. Drive final disposition is also documented in the CS and the content of the TSD is transferred to the permanent history file.

Other summary reports are created on a monthly basis from the FERs for use by management in understanding just what is being examined and understanding the issues which might warrant further action to preclude repetition.

ABBREVIATIONS

CO – Central Office

CS – Control Sheet

FE – forensic examiners

FER – forensic examiner’s report

RO – Remote Office

TSD – temporary storage directory