Learning from the Past Intrusion Attacks: Digital Evidence Collection to Make e-Commerce Systems More Secure

P. S. Lokhande[1], B. B. Meshram[2],
[1]PVPPCOE, Sion, Mumbai, India, [2]VJTI, Matunga, Mumbai, India

Key words: Digital Evidence, Intrusion detection, Evidence collection , Evidence preservation, E-commerce security violation.

Abstract:

Use of computers, data communication and data storage devices has become so ubiquitous that most of the crimes or civil disputes have involvement in some way. There will be a large demand for computer forensics in the coming days. Computer forensic has four phases: Collection, Presentation, Filtering and presentation.Computer Forensic: It is an art and science of applying computer science to aid the legal process. Computer involvement in crime such as fraud, child pornography and threatening emails. Another situation where computers commonly assist in a crime is intellectual property theft in the corporate environment. Computers were the targets of the crime such as during a Denial of Service (DoS) attack against an E-Commerce site. It is often less obvious than previous cases. Computer contains information that is incidental to the crime such as a database containing the payment and receipts list of gamblers, drug traffickers, and scammers. Pay and receipts (owe) are the documents made in spreadsheets to keep track of their customers and suppliers. In the same cases other innocent bystanders computers, WiFi networks may have hacked to send threatening mail for example mails sent by terrorist group before the bomb Blast in various cities of India.

1 Introduction

Digital evidence is fragile and can be easily destroyed or rendered inadmissible in court due to modification after it is collected. IT incident response teams need to recognize that, if an intrusion or attack has a chance of ending up in criminal prosecution, evidence handling is crucial to winning the case and bringing the criminal to justice.[1] [w3]

The first priority of IT personnel is usually two-fold: to protect the system and network from further harm and to return the system and network to full functionality as quickly as possible. Actions taken to further these goals may directly conflict with best practices for preserving evidence. If a crime has occurred, the best action is often to do nothing – after disconnecting the system from the network so hackers can't erase the evidence itself. Unless you have training in computer forensics and evidence collection, you should leave it up to professionals in that area to make copies of evidentiary data in memory and on the hard disk. They have specialized equipment that makes it easier and makes it easier to prove in court that there was no tampering with the evidence.[1] [3]

2 Basics of Evidence Collection

digital evidence analysis is to identify digital evidence for an investigation. An investigation typically uses both physical and digital evidence with the *scientific method* to draw conclusions. Examples of investigations that use digital forensics include computer intrusion, unauthorized use of corporate computers, child pornography, and any physical crime whose suspect had a computer. At the most basic level, digital forensics has three major phases:[1] [2]

Acquisition
Analysis

Presentation

2.1 The ***Acquisition*** *Phase* saves the state of a digital system so that it can be later analyzed. This is analogous to taking photographs, fingerprints, blood samples, or tire patterns from a crime scene. As in the physical world, it is unknown which data will be used as digital evidence so the goal of this phase is to save all digital values. At a minimum, the allocated and unallocated areas of a hard disk are copied, which is commonly called an *image*.
Tools are used in the acquisition phase to copy data from the suspect storage device to a trusted device. These tools must modify the suspect device as little as possible and copy all data.
2.2 The ***Analysis*** *Phase* takes the acquired data and examines it to identify pieces of evidence. There are three major categories of evidence we are looking for:

Inculpatory Evidence: That which supports a given theory
Exculpatory Evidence: That which contradicts a given theory
Evidence of tampering: That which can not be related to any theory, but shows

that the system was tampered with to avoid identification
This phase includes examining file and directory contents and recovering deleted content. The scientific method is used in this phase to draw conclusions based on the evidence that was found. Tools in this phase will analyze a file system to list directory contents and names of deleted files, perform deleted file recovery, and present data in a format that is most useful.

3 Tools helpful in collecting digital evidence

Using Host Protected Areas (HPA) and Device Configuration Overlays (DCO) as a evidence collection tools: manufacturer hidden areas of a hard disk, specifically Host Protected Areas (HPA) and Device Configuration Overlays (DCO). These areas can be problematic for computer forensic investigators, since many of the common industry tools cannot detect the presence of the HPA and DCO. The Host Protected Area (HPA) as defined is a reserved area on a Hard Disk Drive (HDD) (T13, 2001). It was designed to store information in such a way that it cannot be easily modified, changed, or accessed by the user, BIOS, or the OS. This area can contain information ranging from HDD utilities, to diagnostic tools, as well as boot sector code. An additional hidden area on many of today's HDDs is the Device Configuration Overlay (DCO). The DCO allows system vendors to purchase HDDs from different manufacturers with potentially different sizes, and then configure all HDDs to have the same number of sectors. An example of this would be using DCO to make an 80 Gigabyte HDD appear as a 60 Gigabyte HDD to both the OS and the BIOS. [3]
Investigative Significance
Since an end user can modify and write to the HPA and DCO, allowing them to potentially hide data, forensics investigators need to be aware of these a two areas. As mentioned earlier, the HPA and DCO are hidden from the OS, BIOS, and the user. It is also possible to create an HPA that is approximately the same size as the HDD. This means that the HPA, DCO, or the HPA and DCO combined can potentially store large amounts of information, invisible to the investigator and/or the acquisition and analysis tools. [3] [1]
Certain forensic tools can be used to detect the HPA. These tools include Encase, Sleuth Kit and ATA forensic tool The utilities used by these three methods are dmesg, hdparm, and disk_stat. The first two are built in utilities in Linux and the third one is a tool in the Sleuth Kit.
Forensic Tools

Tool	Programmer/Vendor	Version
The Sleuth Kit	Brian Carrier	2.02
ATA Forensics Tool	Arne Vidstrom	1.1
Encase	Guidance Software	4.20

TULP2G is a forensic software framework for acquiring and decoding data stored in electronic devices. The framework consists of a layered architecture with communicate on, protocol, conversion, and export plug-ins to acquire, decode, and report evidence in customizable layouts. All acquired data is stored in an XML formatted evidence file along with information for auditing purposes. TULP2G is implemented in C# using .NET1.1 and released under a BSD license. http://tulp2g.sourceforge.net/.[w2]
Fenris - razor.bindview.com/tools/fenris/ - is a tool that analyzes program execution. [w3]
Honeyd - http://www.citi.umich.edu/u/provos/honeyd/ - is a command line honeypot program. Honeyd creates virtual hosts for IP addresses matching the specific net. [w4]
Snort - http://www.snort.org - is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP net-works. [w5]
Dsniff - www.monkey.org/~dugsong/dsniff/ - is a command line network auditing and penetration testing tool.[w6]

4 Conclusion

Digital evidence can be exceptionally relevant in any criminal investigation, or legal dispute for that matter, however if one intends using this evidence successfully. We can curb and control the crime, fraud, pornography with the help of various digital evidence collection tools. Day by day the crime is increasing and thus the use of hi tech equipments and computers, there is a need to investigate and integrate the various Digital Evidence collection and decetion tools to make a hybrid model type all in one tool that can be a silver bulet to tackle such incidences.

References:

[1] Christopher L. T. Brown, " Computer Evidence Collection and Preservation", Network and security Series,ISBN:81-318-0015-6, 2007
[2] Fisher, Barry A., Techniques of Crime Scene Investigation, CRC Press 2003.
[3] Carrier, Brian, Joe, " A Hardware Based Memory Acquisition Procedure for Digital Investigations", Digital Forensics Investigation Journal, Volume1 Issue1 Feb-2004

Web References

[w1] http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
[w2]http://tulp2g.sourceforge.net/.
[w3]razor.bindview.com/tools/fenris
[w4] http://www.citi.umich.edu/u/provos/honeyd/
[w5] http://www.snort.org
[w6] www.monkey.org/~dugsong/dsniff

Author(s):

P. S Lokhande(Asst. Professor) Dept of IT
{pslokhande@gmail.com}
Padmabhushan Vasantdada Patil Prathishthans College of Engineering,
Sion, Mumbai, India 400022

Dr. B. B Meshram (Professor) Dept of Computer Engineering,
{bandumeshram@yahoo.co.in}
Veer Jijamata Technological Institute, Matunga, Mumbai, India 400019