Author(s): Jahankhani, Hamid; Beqiri, Elidon
Title: Memory-Based antiforensic tools and techniques
Year of publication: 2008
Citation: Jahankhani, H.; Beqiri, E. (2008) 'Memory-Based antiforensic tools and techniques' *International Journal of Information Security and Privacy*, 2 (2) pp.1-13.
Links to published version:

- http://dx.doi.org/10.1080/09505430903122760
- http://www.igi-global.com/Bookstore/Article.aspx?TitleId=2478

DOI: 10.1080/09505430903122760

Memory-Based Antiforensic Tools and Techniques

Hamid Jahankhani, University of East London, UK

Elidon Beqiri, University of East London, UK

ABSTRACT

Computer forensics is the discipline that deals with the acquisition, investigation, preservation, and presentation of digital evidence in the court of law. Whereas antiforensics is the terminology used to describe malicious activities deployed to delete, alter, or hide digital evidence with the main objective of manipulating, destroying, and preventing the creation of evidence. Various antiforensic methodologies and tools can be used to interfere with digital evidence and computer forensic tools. However, memory-based antiforensic techniques are of particular interest because of their effectiveness, advanced manipulation of digital evidence, and attack on computer forensic tools. These techniques are mainly performed in volatile memory using advanced data alteration and hiding techniques. For these reasons memory-based antiforensic techniques are considered to be unbeatable. This article aims to present some of the current antiforensic approaches and in particular reports on memory-based antiforensic tools and techniques.

Keywords: *antiforensics; data hiding; live CD; memory-based antiforensics; wireless antiforensics*

INTRODUCTION

The advent of information technology and personal computers has transformed significantly our way of living. Most of our day-to-day activities rely heavily upon the use of electronic devices and digital communications. More people are relying on these technologies to learn, work, and entertain. In 2003, the USA Census Bureau estimated that 62% of the households had access to a personal computer while 55% had access to the Internet (Census Bureau, 2003). Without doubt, digital communications can be considered as one of the greatest inventions of the last century because of its impact and benefits on the society.

On the other hand, digital communications have provided new opportunities for criminals and shaped the ways they commit crime (Shinder, 2002). Criminals are now exploiting digital communications to commit a wide range of crimes such as identity theft, online piracy, financial fraud, terrorism, and pornography distribution. Furthermore the incidences of some of types of crimes increased significantly with the introduction of digital communications and personal computers. For example, Internet communications have escalated the problem of child pornography by increasing the amount of material available, the efficiency of its distribu-

tion, and the ease of its accessibility (Wortley & Smallbone, 2004).

According to Bruce Schneier, electronic crime is flourishing because of three main reasons: a) automation, b) action at distance, and c) technique propagation (Schneier, 2000).

a. Automation: Software packages are used to perform repetitive tasks and cross reference more and more data.
b. Action at distance: We live in a global digital communication era. Criminals perform electronic crimes in distance and with a high rate of anonymity.
c. Technique propagation: Successful electronic crime techniques and malicious software is propagated easily through the Internet.

Law enforcement agencies have started dealing with crimes involving electronic devices and communications since the 1970s when these technologies were introduced. These were coined as electronic crimes since electronic devices and digital communications were used to commit them; while electronic evidence was defined as information or data of investigative value that are stored or transmitted by electronic devices (Ashcroft, 2001).

Law enforcement investigators initially considered electronic evidence as any other type of evidence; however they realised soon that this was not the case and that the conventional approach was not suitable to collect, preserve, and analyse electronic evidence. This is because 'conventional evidence lives in an analog world, whereas computer-derived evidence comes from a digital world and the transition between these worlds is not always as smooth as one would hope' (Johansson, 2002).

Computer forensics was then established as a discipline to support law enforcement agencies in their fight against electronic crime. Computer forensics deals with the acquisition, investigation, preservation, and presentation of digital evidence in the court of law with the final objective of finding evidence that would lead to prosecution. Computer forensics is also known as cyber forensics since it deals with crimes committed in the cyber world (electronic world). The main areas of searching for evidence are hard drives, removable devices, volatile memory, deleted or hidden files, password protected files, pornographic material, and so forth.

The most important input of a computer forensic investigation is the digital evidence. Digital evidence can be envisaged as the counterpart of fingerprints or DNA in the digital world. Criminals will attempt to cover the traces of their malicious work by using antiforensic methods to manipulate and tamper the evidence or interfere directly with the process (Harris, 2006).

Antiforensics is the terminology used to define the activities of hackers or other cyber criminals aiming to undermine or mislead a computer forensic investigation. There are no well-established definitions regarding this discipline since it is quite new and it is yet to be explored. Peron and Legary define it as 'four categories of evidence destruction, evidence source elimination, evidence hiding and evidence counterfeiting' (Harris, 2006), while Grugq (Ruxcon, 2004) defines antiforensics as '[the attempt] to limit the quantity and quality of forensic evidence.'

Although antiforensics is a field under development, however, there are already categories of available tools. Grugq seems to be one of the most dedicated antiforensic researchers so far. With more than five years of antiforensic studies, he ended up losing his job after publishing *Art of Defiling: Anti-Forensics* (Ruxcon, 2004).

The Metasploit Anti-Forensic project by Vincent Liu is part of the Metasploit project which targets audiences interested in penetration testing. Liu's presentation titled 'Bleeding-Edge Anti-Forensics' which was copresented with Francis Brown for an Infosec World Conference was the most descriptive work of what he did so far about antiforensics.

There are number of techniques that are used to apply antiforensics. These techniques are not necessarily designed with antiforensics dimension in mind. For instance, folder shielders

have been designed in order to primarily provide a level of security and privacy, but they can be used as an antiforensic tool since they can hide data (Jahankhani, Anastasios, & Revett, 2007). The others are:

- **Digital media wiping:** A proper wiping of the media that contains the digital evidence; will simply make the evidence disappear.
- **Steganography:** Someone can use steganography to hide a file inside another and make the investigator unable to take advantage of the evidence.
- **Privacy wipers:** These are tools that aim to delete any privacy traces from operating systems, applications, or both. If properly used the investigator might find no evidence at all inside the digital media.
- **Rootkits:** Rootkits can subvert the operating system kernel and even react to forensic acquisition processes by hijacking the way the operating system uses areas like process management or memory management to extract the evidence.
- **S.M.A.R.T antiforensics:** This kind of technology can be used by an attacker to suspect if a hard drive has been taken out for a forensic duplication process.
- **Homographic attacks:** Such an attack can mislead an investigator since some letters that look similar to the human eye can be replaced with others in such a way to make a malicious file look legitimate.
- **File signature modification attacks:** Someone can purposefully change the file signature of a file to make it look something else.
- **Encryption:** This can be used almost in every antiforensic stage in order to obscure and make unreadable and unusable the evidence.
- **Metadata antiforensics:** Information about data (metadata) can be altered in order to hide user actions.
- **Slack space antiforensics:** Someone can hide malicious software in areas that operating system might not use, like slack space, because they might be considered as reserved or empty.
- **Secure digest functions (MD4, MD5, etc.) Collision generation:** Someone can alter a file and then use antiforensic software to make this file having the same MD4 or MD5 value like before the alteration, thus bypassing a forensic integrity check.
- **Digital memory antiforensics:** There are programs that are able to hide processes or other evidence from memory.
- **Misleading evidence:** Someone can leave evidence in such a way to mislead the forensic investigation.
- **Packers/binders:** Someone can use such a program in order to transform a file by changing its structure, thus it can bypass security mechanisms that searches for malicious behaviour patterns inside files.
- **Forensic tools vulnerabilities/exploits:** There are already implementations available to show that some of the computer current forensic tools can be bypassed or exploited.
- **Resource waste:** To purposefully leave traces in a big network in order to make the forensic investigator waste valuable resources and time.
- **Forensic detection:** Someone can install a mechanism to be triggered after any computer forensic-related presence.
- **Anonymous actions:** It includes every action that can be done by a fake or unknown identity. The result from the investigator is to fail to trace back the malicious activities.
- **Antiforensics in flushable devices:** Someone can take advantage of devices that can be flashed (like PCI cards or BIOS) and install malicious code inside them, thus they can remain unnoticed.

The aim of this article is to present three of the current antiforensic approaches and focuses only on memory-based antiforensics known as antiforensic live CDs. Memory-based bootable live CDs are specially built Linux operating systems that boot directly from the CD drive

into the random access memory (RAM) area. These packages do not load into the hard drive, change files, or alter other variables in the target system unless specified by the user. Live CDs are used mainly for penetration testing and other security related tasks and they include a variety of software packages used for antiforensic purposes.

ACTING ANONYMOUSLY

From a forensic scope, anonymity can be considered as a major antiforensic approach. Below are some of the tools that are used.

Anonymous Mail Accounts

These are accounts that are created using services available on the Internet that facilitate anonymous mailing. This will make the process of e-mail tracking more difficult as the mail headers are altered and no Internet protocol (IP) address details will be available (Greene, 2003).

Figure 1 shows that the sender is an anonymous authority, in this case the domain of 'bananasplit.info.' There is also an e-mail address (abuse@bananasplit.info; not visible in the picture) where more information about the sender's IP could be requested by the forensics team.

Anonymous Proxies

Nowadays there are plenty of anonymous proxies on the Internet with a significant number of them being free (Anonymous INET, 2006; Free Proxy, 2006). Although these proxies promise Internet anonymity, they do not always talk about the level of anonymity service they provide.

Below is the result of a test on a high anonymity service in order to find out the amount of information on the user's identity. The anonymity has been checked against a Web site (anonymitytest.com) that shows the IP address of the visiting address along with a service ('whois') that aims to trace back the IP.

It is important to note that in special cases even a high anonymity server can reveal all the information regarding its users. All someone has to do is to monitor and analyse the traffic patterns coming to and from that proxy (Gibson, 2006).

Figure 2 shows that high anonymity proxy puts its own IP number to the visited Web page in order to keep the client anonymous.

An attempt to trace back the address will come up with the details of the proxy server and not the user's figure below.

In order to get more information about the real visitor's identity, the anonymous proxy provider has to be contacted. Here are the problems someone might face:

Figure 1. Anonymous mail details

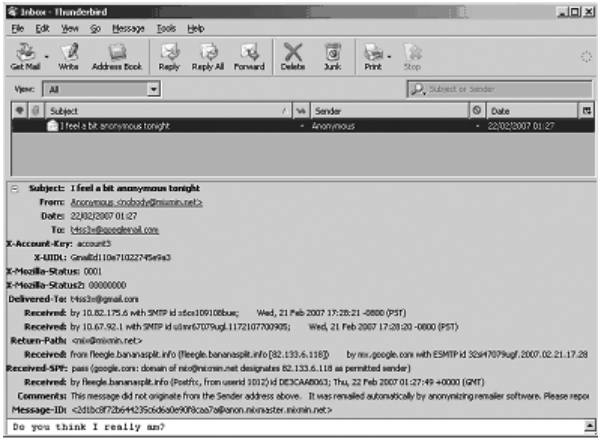

Figure 2. Anonymity service

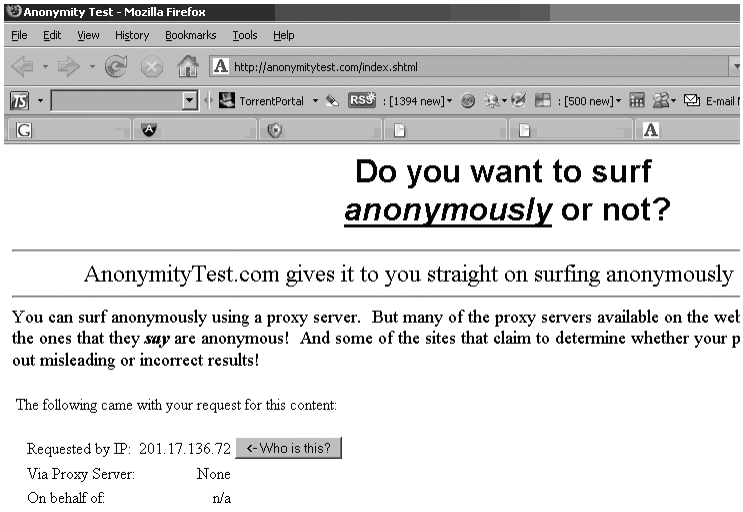

Figure 3. Proxy server details

```
nic-hdl-br:  DSS30
person:      Diego Santos Soares
e-mail:      virtua@virtua.com.br
created:     20000424
changed:     20070128

nic-hdl-br:  RII19
person:      Ricardo Ide
e-mail:      ricardoide@globocabo.com.br
created:     20011010
changed:     20011010

remarks:     Security issues should also be addressed to
remarks:     cert@cert.br, http://www.cert.br/
remarks:     Mail abuse issues should also be addressed to
remarks:     mail-abuse@cert.br

% whois.registro.br accepts only direct match queries.
% Types of queries are: domains (.BR), BR POCs, CIDR blocks,
% IP and AS numbers.
```

1. There are cross boarder legal issues. In this case the domain ends with 'br' which means that the proxy owner is located somewhere in Brazil.
2. The anonymous proxy provider—no matter the geographical location—might claim that all the logs are deleted and nothing is saved regarding their clients (anonymous visitors). In that case, only a government regulation which enforces IP logging would provide a connection to the client's IPs.

It is important to note that someone can be a part of an anonymous network—like Tor—in order to achieve anonymity. In this case it is not feasible even for the governments to totally follow an IP or a packet, since the information is going through a variety of interconnected nodes with some encrypted links through several countries. This is a more efficient way to keep the users anonymous.

The only way for someone to monitor an amount of Tor's traffic is to set up a fake Tor server and monitor the traffic of some other

servers as well. In a crackdown of a recent crime investigation in Germany, police seized 10 Tor servers for suspicion of a child porn investigation (Oates, 2006).

WIRELESS ANTIFORENSICS METHODS

How about if someone launches an attack using multiple access points from roof top of a high building in the middle of a crowded city with the help of a strong directional antenna?

Raul Siles, in his excellent two-part article 'Wireless Forensics: Tapping the Air' unveils some 'de facto' and some new wireless antiforensics methods. Some of the major approaches are (Siles, 2006, 2007):

- The use of illegal channels, like channel 14 in U.S. and Europe
- The use of strong layer-2 encryption
- The modification of the 802.11 specification (Raw Covert, madWifi patches)
- Wireless MAC spoofing

While in theory the forensics investigator should monitor every single packet of every channel available around the suspect, in reality the post incident response could end up quite dramatically. This could be due to ignorance regarding the channels and access points used, legal barriers between the access point and the forensics acquisition, noncooperative ISPs, and so forth. The forensic process should be enhanced with security mechanisms which would upgrade the post-incident reaction to real time. The real-time acquisition tools should have capabilities of capturing activity of all the wireless point within a respectable distance.

MEMORY-BASED BOOTABLE ENVIRONMENTS

There are plenty of 'live CDs'—commercial and freeware—in the market that are made to meet certain user's needs. These are like data recovery (SystemRescueCD, ERD Commander), security (BackTrack, NST), PC benchmarking (StressLinux, Ultimate CD), gaming (LLGP, Freeduc-games), or even alternatives for a fully functional operating system (Knoppix, Kanotix). There is also a Web site called Frozen Tech (2006) that lists a vast majority of the live CDs (if not all of them) (Brand, 2006)

A live CD is nothing more than a compact disk, DVD, or USB drive which contain an operating system image file and a boot loader program, used to start or boot a computer system. An image file is a single compressed file that contains the entire operating system programs and files. Bootable CDs, also known as LiveDistros, are mostly available freely open source license agreement. According to this agreement 'anyone can modify and redistribute the original operating system without asking for permission of retribution from the author' (Opensource.org, 2007).

The concept behind using removable media for storing operating systems is not new. In the early introduction of personal computers, operating systems (such as MS-DOS) were loaded into the memory from removable media (usually floppy disks). With the advent of mainframes (considered the first generation of computer systems), the instructions to hardware components were given by punched cards, which although did not constitute an operating system in per se, did introduce the concept of OS. It is worth mentioning though that punched cards were not effective as live CDs since extensive processes required hundreds of them (Gochioco, 2004).

Mainframes were not the only computer systems that used removable media for storing instruction programs or operating systems. For example, diskless computer systems do not have operating systems installed; instead they load from a copy of the operating system located in a network server. Either operating systems such as MINIX are distributed mainly in removable media (i.e., CD, floppy, etc.) because of its extremely small size; MINIX kernel counts only 4000 program lines whereas other operating systems rely on millions of lines of code (Minix, 2007).

Although live CDs are the preferred tools of trade in conducting memory-based antiforensics, most of them were designed for security

testing purposes. Good collections of security testing tools are distributed with these portable media and are usually used by computer security professionals to troubleshoot their computer systems and networks. Unfortunately, even malicious users are making use of these specially build packages to perform illegal activities, amongst all antiforensics.

The majority of memory-based packages used for antiforensic purposes are built on UNIX oriented platforms, although there are similar packages built on platforms such as Windows, Apple MAC, MS-DOS, MINIX, and so forth.. There is a reason behind this. Most of UNIX operating system platforms are built on open source code (nonproprietary) and for this reason a lot of security focused tools are developed and distributed online. UNIX systems are also the platform of choice for security specialists and hackers because of their reliability, flexibility, and amount of accessible security tools. Typically, the graphical user interface (GUI) of a live CD is either a KDE or gnome interface. These are the most popular user interfaces in UNIX platforms.

Live CDs manage to recognise and work with a variety of hardware components thanks to its device manager called 'udev' (Qlogic.com, 2007), which is the device manger for most of UNIX/LINUX based systems. Device managers are programs designed to handle hardware components of a computer system. Having a device manager that interacts with most of hardware devices promotes the interoperability and portability of LiveDistros. All the removable media attached to the system are viewable from the LiveDistros interface.

The OS loaded from the live CD can view, access, or copy all the files and programs created by the native operating system (these are stored in the secondary memory area). Linux-based operating systems treat all attached devices as files. When the live CD start running it checks for hard drives, removable media, and other devices attached to the motherboard. When found, these devices are mounted (connected) to the operating system; at shut down the connection is dropped. Hard disks contents are viewable, can be copied, but no alterations can be made to files from the live CD interface. From a malicious user point of view, this is a good opportunity to explore, since information in the native hard disk can be accessed easily without leaving traces. Most of the operating systems run security services which keep records of users or systems that access its files. However, since these systems are not running, no records will be added to the log files of the native OS.

Furthermore, important system files can be copied, scrutinised, and important data disclosed. For example, in Windows platforms 'SAM' file is the recipient of system passwords. These passwords are encrypted, but if copied and then attacked, systems passwords can be identified. Live CDs provide the necessary tools to unveil the encrypted passwords copied from the hard disk (e.g., Kain, John the Ripper), compromising seriously the security of the system. From the interface of the live CD, the native OS security files such as 'SAM' can be copied and saved in ramdisk or in a removable device to be attacked at a later stage. A fully detailed demonstration of this attacking technique will be provided in the next article.

Network services are fully accessible from the live CD interface. Connections to Internet or local computer systems are easily implemented permitting the user to perform most of the tasks available in operating systems that run from the hard disk.

Memo-based antiforensics techniques are difficult to beat for a variety of reasons. The most important advantages of using these techniques are:

1. Lack of digital evidence
2. Compatibility, flexibility, and portability
3. Anonymity
4. Availability of tools
5. Freely distributed

SecurityDistro.com, a site dedicated to memory-based security tools, lists over 40 memory-based packages (Securitydistro.com, 2007). Most of the packages offer similar tools

and interfaces. Among these packages are Backtrack, Anonym.OS, Helix, Penguin Sleuth, and Auditor collection which have a wide range of security tools that might be used to deploy antiforensic activities.

In this article, Backtrack antiforensic tools were used, which are freely available. The selection is not casual. Backtrack does provide the user with the opportunity to use a well-established security focused framework, metasploit (Metasploit.com, 2007). Metasploit framework is a collection of security tools used to test the security side of computer systems, penetration testing, and exploitation.

Furthermore, metasploit contains a special module called antiforensics, which is a collection of antiforensic tools (e.g., timestomp, sam juicer, slacker, transmogrify, etc.) that can be loaded and used directly from the live CD.

According to Vinnie Liu, a well known antiforensic researcher, these tools are designed to tamper with or break well recognised industry tools such as Encase, new file technology system (NTFS), and PGP desktop, with the final objective of manipulating the digital evidence and compromising the investigation findings (Liu & Stach, 2007).

Once Backtrack is downloaded, the Linux based operating systems can be burned in a bootable CD and be ready for use. Instructions on how to accomplish this task are available on various sites online.

Stealing Passwords

Backtrack live CD can be used by malicious users to steal and then crack passwords used to log in computer systems. Windows operating systems store password information locally in the hard drive in a system file called security accounts manager, otherwise known as SAM file.

This file is very important from the security point of view since it contains all system user passwords in an encrypted format. Encryption of user passwords is performed by Windows using a proprietary encryption utility called system key which uses 'strong encryption techniques to secure account password information that is stored in the SAM file.' In a computer system running Windows OS, the system key utility (program) is located at this logical address: C: /Windows/system32/config/system. The system key program also contains the key used to encrypt the passwords stored in SAM.

Usually access to SAM is restricted since it is a system file. Even if the user manages to copy SAM in a portable media device it will be difficult to unmask the hidden passwords since a key stored in the system utility is needed to decrypt SAM. The key must be extracted first from the system key utility. However with Backtrack, a user can extract quite easily user passwords stored in SAM, without creating digital evidence. By using Backtrack no digital evidence is left since all the operations are performed in RAM and at the same time no digital evidence will be left in the native Windows system since it is not running.

Backtrack can be also used to recover user account passwords of a remote computer system running Windows OS. In this case metasploit frame work might be used to achieve the goal. A metasploit 'exploit' called lsass_ms041_011 is used to connect remotely to vulnerable computer systems. Once a connection is established remotely an advanced metasploit package called 'meterpreter' is used to fully explore to the target system.

The meterpreter is a sophisticated software package shipped with metasploit that facilitates attack automation, by making it easy to interact with processes, networking, and the file system (Metasploit.com, 2007). Furthermore, another special module of meterpreter called Sam juicer can be used to copy password hashed from SAM. Sam juicer performs the task without accessing SAM file, the registry, or writing any files in the remote computer system hard disk. This is achieved through an advanced connection technique called direct memory injection; no digital evidence is created or left in the target computer system (Liu & Stach, 2007).

This technique undermines completely the investigation process because no digital evidence is created in the remote computer system since the communication between computers is

conducted in the temporary memory (RAM). Files are not accessed directly, new processes are not created or data added to the log (security monitoring) files. A computer forensic investigator will not be able to gather digital evidence from neither of the computer systems (the attacker's or the attacked system) simply because the evidence does not exist.

Modifying Timestamps

From a computer forensic investigation point of view file timestamps are very important because they provide the necessary evidence to prove if certain antiforensic activities occurred at a certain moment in time or whether a user was logged in a computer system. For this reason malicious users might attempt to modify timestamps in order to eliminate compromising evidence. A timestamp is the data appended to a file that shows when a file is created, accessed, modified, or entry modified. These file attributes are also known as modified-accessed-created-entry modified (MACE) attributes. Antiforensic tools attempt to modify these data parameters in order to mislead computer forensic investigators.

Backtrack again provides the perfect tool to modify timestamps. The tool is called timestomp and is included in the metasploit framework. Timestomp is a program developed by metasploit project which gives the user the opportunity to modify all NTFS timestamp parameters (Metasploit.com, 2007). NTFS is the proprietary file system of modern Windows operating systems including NT, 2000, 2003, XP, and Vista (NTFS, 2007).

Timestomp can be used also as a standalone program to modify timestamps; however its potential is fully explored when used within the metasploit framework. Meterpreter module (started from backtrack) permits a user to connect remotely to a target computer system. On the other hand from within this module timestomp can be executed to modify file timestamps. Since all the operations are conducted in temporary memory (RAM) no digital evidence is left in the systems to indicate traces of antiforensic activity. Certainly it will almost be impossible for a computer forensic investigator to notice timestamp modification since its parameters will look legitimate.

Hiding Data in Slack Space

Slack space is the preferred hard disk area used by a malicious user for storing illegal software, documents, or pictures because files stored in it are not seen or accessed by windows explorer; 'data is hidden in unallocated or unreachable locations that are ignored by the current generation of forensic tools' (Forensicwiki.org, 2007). The user is completely unaware of the existence of such files.

A variety of malicious programs might be used to hide data in the slack space; however 'slacker' is one the most proficient tools used to perform such activities. Slacker, which is named after the slack space, was developed by the metasploit team and was released as a module with metasploit framework (Metasploit.com, 2007). Slacker uses a sophisticated technique to hide programs, files, or any other type of data in the slack space. It takes the data, fragments them into thousands of pieces, and then distributes them across the slack space in the hard disk. This program mainly stores the data in stable file such as system files (windows/system32 files) which are not examined also buy computer forensic tools. Slacker's main features include file splitting and slack space hiding; these features make slacker very hard to trace.

If a computer forensic tool is used to analyse the data in the slack space, no evidence will be discovered since individual fragments of data will not help to construct the true nature of the hidden file; for the forensic tool data are so diffuse that they look like random noise (Berinato, 2007). Only Slacker can recompose the fragmented pieces of data to create the original file. Slacker has proven to be successful also against PGP desktop, a security tools that includes some tools claming to wipe out completely the slack space. Metasploit researcher Vinnie Liu has proven that data written in the slack space with slacker can not be wiped out even when PGP desktop tool is used (Metasploit.com, 2007).

Modifying File Extensions and Signatures

In a computer, system files are identified by two attributes: file extensions and file signatures. For each file format there is a unique file signature; for example executable files in Windows are identified by file signatures starting with the letters MZ (Liu & Stach, 2006). Therefore, to hide a file in a computer system suffices to change its extension and add the letters MZ at the beginning of that file. By using this technique files containing pornographic material for example can be masqueraded as system files and go undetected by computer forensic tools.

Memory-based antiforensic tools such as Backtrack can be used effectively to manipulate file extension and signatures. Metasploit project has developed and is about to release a tool called Transmogrify that allows a user to masquerade malicious files. Metasploit developers claim that this tool is able to alter file extension and header/signature without being detected by forensic tools like Encase (Metasploit.com, 2007).

Meterpreter loads remote processes (such as cmd.exe) in memory, therefore no digital evidence will be left in the system .To make things harder for computer forensic investigators, the MACE attributes of wufileuel.sys can be further altered to match the attributes of other system files. Forensic tools will not be able to identify the malicious file since file extension, signature, and timestamps look legitimate, and therefore no red flags will be raised.

CRITICAL DISCUSSION AND EVALUATION OF THE MEMORY-BASED ANTIFORENSIC TOOLS AND TECHNIQUES

Memory-based antiforensic tools and techniques interfere substantially with the investigation process by altering or hiding digital evidence. Because memory-based antiforensics techniques are deployed directly in temporary memory (RAM), the defence strategies must be focused at this memory area. Slack space must be scrutinised and analysed as well. These defensive strategies must be implemented to achieve some sort of success against memory-based antiforensic activities:

a. Slack space analysis: Statistical analysis of slack space must be conducted to discover strange or unusual samples of data (Liu & Stach, 2006). For example, Slacker splits and distributes file fragments usually across a vast range of system files. For this reason it would be wise to scrutinise carefully the slack space of these files in order to trace potential antiforensic activity, even though it will be difficult to reconstruct the original hidden data. According to Vinnie Liu, file fragments in slack space and file system information must be analysed together in order to discover elements of slack space antiforensics (Liu & Stach, 2006).
b. Capture data in memory: Memory-based live CDs load, operate, and store data in memory, unless specified otherwise by the user. For this reason the main area to look for digital evidence is the memory of the local or remote computer system used for antiforensic activities. Other data that should be captured are running processes, ports, and uploaded or downloaded files which will indicate if such activities occurred.

Memory-based antiforensics relies mainly on volatile memory, while traditional antiforensics is deployed in the secondary memory storage area (hard disk). For this reason memory-based live CD activities are hard to detect since volatile memory is unstable and easy to erase. Computer forensic investigators might be able to collect digital evidence only if the perpetrator's computer device is seized and is not shut down; however if the user has removed the live CD and turned off the system, the evidence is lost permanently since memory is volatile. Forensic tools such as Memparser (SourceForge, 2007) or Windows memory forensic toolkit (WFTK,

2007) might be used to collect valuable data in memory.

c. Improving Computer forensic tools: Some memory-based antiforensic tools (e.g., Timestomp, Transmogrify) tackle computer forensic packages. Timestomp provides a specific option to trick Encase; by using switch –b, timestamps are set to blank. Encase and forensic tool kit (FTK), two prestigious computer forensic tools, do not recognise Timestomp changes (Liu & Stach, 2006). This is a clear indication that these tools must be improved (or rewritten) in order to properly detect timestamp alterations, particularly because modified timestamps can compromise the success of a computer forensic case in the court of law. On the other hand Encase and FTK do not detect file extension or signature modification achieved with Transmogrify or Backtrack; even in this case these tools must be improved in order to detect traces of antiforensic activity. Computer forensic tool designers should examine carefully how memory-based live CDs interact with the system in order to improve their future released tools; the idea behind this is to use the same antiforensic tools to defeat them.
d. Improving signature analysis: Memory-based antiforensic tools manage to modify file extensions and signatures. In the meantime some of the most used computer forensic tools (i.e., Encase, FTK etc.) fail to detect such changes. Encase checks only the first two characters of a file signature which can be easily modified (e.g., MZ for executable files). Therefore, automated tools will not be able to detect file signature modifications achieved by using memory-based antiforensic tools. In this case manual investigation should be conducted provided that the investigator identifies the suspicious files. Forensic tools need to be redesigned to tackle file signature modification. A good way forward would be the redesign of the searching process so that files are checked from top to bottom for patterns of data. This method might produce good results since particular patterns of data might be associated with certain files; if these patterns are not present then further investigation can be conducted.
e. Invest in human and time resources: If digital evidence is well hidden there is a high probability that it will go undetected because of feasibility issues. This is true especially when there are thresholds to meet in terms of time and cost (e.g., pressure to complete a forensic investigation within a deadline). In the case of memory-based antiforensics, digital evidence is hard to recover because it is well hidden. Therefore more training and time must be provided to investigators so they can succeed. Financial resources must also be committed to develop efficient forensic tools in short periods of space in order to keep up to date with antiforensic tool development.

Another issue to consider seriously is the way computer forensic investigators process seized data. Computer forensic cases are usually based on evidence produced by automated tools such as Encase or FTP. Unfortunately these tools do not detect most of antiforensic activities deployed by live CDs. The solution to this problem is a combination of in depth manual investigation and automated tool searching since manual processing might be able to reveal some of the digital evidence traces.

CONCLUSIONS

Antiforensics is a reality that comes with every serious crime and involves tactics for 'safe hacking' and keeps the crime sophistication in a high level. Computer forensic investigators along with the forensic software developers should start paying more attention to antiforensics tools and approaches.

If we consider computer forensics as the actions of collection, preservation, identification, and presentation of evidence, antiforensics can affect the first three stages. Because these stages can be characterised as 'finish to start'

between them from a project management point of view, the failure of one of them could end up as a failure of the lot. Thus, there is a high impact of antiforensics to the forensics investigations.

Officially there is no such thing as antiforensic investigations because the antiforensic countermeasures are still part of the investigator's skills.

REFERENCES

Anonymous INET. (2006). *Fast proxy server list*. Retrieved February 28, 2007, from http://www.anonymousinet.com/

Ashroft, J. (2001). *Electronic crime scene investigation: A guide for first responders*. Retrieved June 22, 2007, from http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf

Berinato, S. (2007). *The rise of anti forensics*. Retrieved June 16, 2007, from http://www.whitehatsec.com/home/resources/trade/07tradenews/062607CSO.html

Brand, N. (2007). *Frozen tech: The LiveCD list*. Retrieved August 11, 2007, from http://www.livecdlist.com/

Census Bureau. (2003). *Computer use in 2003*. Retrieved June 21, 2007, from http://www.census.gov/population/pop-profile/dynamic/Computers.pdf

Forensicwiki.org. (2007). *Anti-forensic techniques.* Retrieved August 5, 2007, from http://www.forensicswiki.org/wiki/Anti-forensic_techniques

Free Proxy. (2006). Retrieved February 16, 2007, from http://www.freeproxy.ru/en/free_proxy/

Frozen Tech. (2006). *Live CD creation resources.* Retrieved February 16, 2007, from http://www.livecdlist.com/wiki/index.php/LiveCD_Creation_Resources

Gibson, S. (2006, December 14). *Gibson research corporation. Security now – transcript of episode 70 – achieving Internet anonymity*. Retrieved February 3, 2007, from http://www.grc.com/sn/SN-070.pdf

Gichioco, L. (2002). *Computer technology: From punch cards to clustered supercomputers*. Retrieved July 28, 2007, from http://tle.geoscienceworld.org

Greene T. C. (2003, August 21). *Net anonymity service backdoored*. Retrieved December 12, 2007, from http://www.theregister.co.uk/2003/08/21/net_anonymity_service_backdoored/

Harris, R. (2006). *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem.* Retrieved April 21, 2007, from http://www.dfrws.org/2006/proceedings/6-Harris.pdf

Insecure.org. (2006). *Top 100 network security tools.* Retrieved February 3, 2007, from http://www.insecure.org/tools.html

Jahankhani, H., Anastasios, B., & Revett, K. (2007). *ECIWS, digital anti forensics: Tools and approaches*. Retrieved June 21, 2007, from http://academic-conferences.org/pdfs/eciw07-booklet.pdf

Johansson, C. (2002). *Forensic and anti-forensic computing*. Retrieved June 24, 2007, from http://www.fukt.bth.se/~uncle/papers/forensics200212.pdf

Liu, V., & Stach, P. (2006). Defeating forensic analysis. *CEIC 2006: Technical lecture1*. Retrieved August 18, 2007, from http://stachliu.com/files/CEIC2006-Defeating_Forensic_Analysis.pdf

Metasploit.com. (2007). Retrieved June 12, 2007, from http://www.metasploit.com

Minix. (2007). Retrieved June 4, 2007, from http://www.minix3.org/

NTFS. (2007). Retrieved August 15, 2007, from http://www.ntfs.com

Oates J. (2006, September 11). *German police seize TOR servers*. Retrieved January 27, 2007, from http://www.theregister.co.uk/2006/09/11/anon_servers_seized/

Opensource.org. (2007). Retrieved July 21, 2007, from http://www.opensource.org/

Qlogic.com. (2007). *Persistent naming using udev in Linux environment*. Retrieved August 2, 2007, from http://www.qlogic.com/documents/datasheets/knowledge_data/whitepapers/SN0130979-00.pdf

Ruxcon. (2004). The art of defiling. *Grugq*. Retrieved February 16, 2007, from www.ruxcon.org.au/files/2004/13-grugq.ppt

Schneier, B. (2000). *Secrets and lies, digital security in a networked world*. John Wiley and Sons, Inc.

Securitydistro.com. (2007). Retrieved August 15, 2007, from http://www.securitydistro.com/index.php?option=com_weblinks&catid=11&Itemid=4

Shinder, D. (2002). Scene of the cybercrime. *Computer forensics handbook*. Syngress Publishing.

Siles, R. (2006, January 16). *Sebek 3: Tracking the attackers, part one*. Retrieved February 12, 2007, from http://www.securityfocus.com/infocus/1855

Siles, R. (2007, January 8). *Wireless forensics: Tapping the air-part two*. Retrieved February 16, 2007, from http://www.securityfocus.com/infocus/1885/2

SourceForge. (2007). *Memparser*. Retrieved August 11, 1007, from http://sourceforge.net/projects/memparser

Windows Memory Forensic Toolkit (WFTK). (2007). *Digital investigations*. Retrieved August 12, 2007, from http://forensic.seccure.net/

Wortley, R., & Smallbone, S. (2004). *Child pornography on the Internet*. Retrieved June 21, 2007, from http://www.cops.usdoj.gov/mime/open.pdf?Item=1729