(Il)Legal Aspects of Digital Antiforensic

Jasmin Ćosić
IT Section of Police Administration
Ministry of Interior of Una-sana canton
502.V.bbr br.2, Bihać, B&H
jascosic@bih.net.ba

Zoran Ćosić
"STATHEROS" d.o.o
Kaštel Stari, Split, Croatia
zoran.cosic@statheros.hr

Miroslav Bača
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
miroslav.baca@foi.hr

Abstract. *This paper defines digital antiforensic. It is a relative new technology used by cyber criminals, to destroy digital evidence in purpose to obstruct digital investigation, and by legal users to keep their privacy. This paper introduces some methods and tools that are used in digital antiforensic, that should be comprehensible for participants of digital investigation, after reading this study. Ontological model is presented.*

Keywords. digital antiforensic, steganography, privacy, encryption

1 Introduction

Locard exchange principle implies that anyone or anything that was at „crime scene", took part of scene or left traces. The triangle victim-suspect-crime scene is always current. Same model is usable for solving cyber criminal cases.[1]
In these cases cyber criminal investigators use scientific methods and tools to find crime evidences (digital evidence). So they use digital forensic (science of collecting, storing, testing, analyzing and presenting relevant digital evidence for use in court processing) [2]. Criminals use antiforensic methods to cover traces, and to obstruct investigations. We can say that digital antiforensic can be used against digital forensic.
There is a lack of papers on this subjects because antiforensic is still undefined. Some papers treated this area, and some analysis and experiments were made. Digital forensic is science – scientific area, and is accepted as well in scientific circles. As digital antiforensic is primary used by criminals, it is perceived as technique or method. Some of that methods are more and more used in legal purposes. That mainly considers user that want to be anonymous for some reason, or they want to keep their privacy in cyber space, or they want to save their personal data.
In following text the authors will list the types of antiforensic, and provide the review of tool that are used for this purpose.

2 Digital antiforensic definition

There is no precise definition of digital antiforensic. Some authors deal with this problem in past few years, and defined antiforensic from aspect and definition of digital forensic. So according to [6] digital antiforensic is method used for preventing scientific methods that are used u public and criminal law, and are implemented by police agencies in legal system.[6]

Some authors define antiforensic as „simple tool for breaking or avoiding detection [7]. Peron and Legarty [8] define it as process of limitation of identification, collecting, comparing and checking of validity of electronic data, in purpose to obstruct criminal investigation. Digital antiforensic can be called as set of tactics and measures taken by person that wants to prevent a process of digital investigation (10)

If we look at digital antiforensic in terms of primary purpose and respecting a fact that it is technology, according authors digital antiforensic is:
Set of methods and techniques whose primary purpose is compromising the process of digital forensics, system manipulation, and violation of the integrity of digital evidence. If we look at it in aspect of using for legal purposes, in order to protect and preserve the integrity, we can conclude that the methods of digital

antiforensic are increasingly used in order for free expression of will and protection when using a global network - the Internet.

In Figure No. 1 shows an ontological approach to defining digital antiforensic.

The model consists of several layers that are arranged in a hierarchical structure.

On top of these hierarchies are Methods, Professions, Types, Purpose and Terminology.

Methods and Professions have been further developed at lower levels.

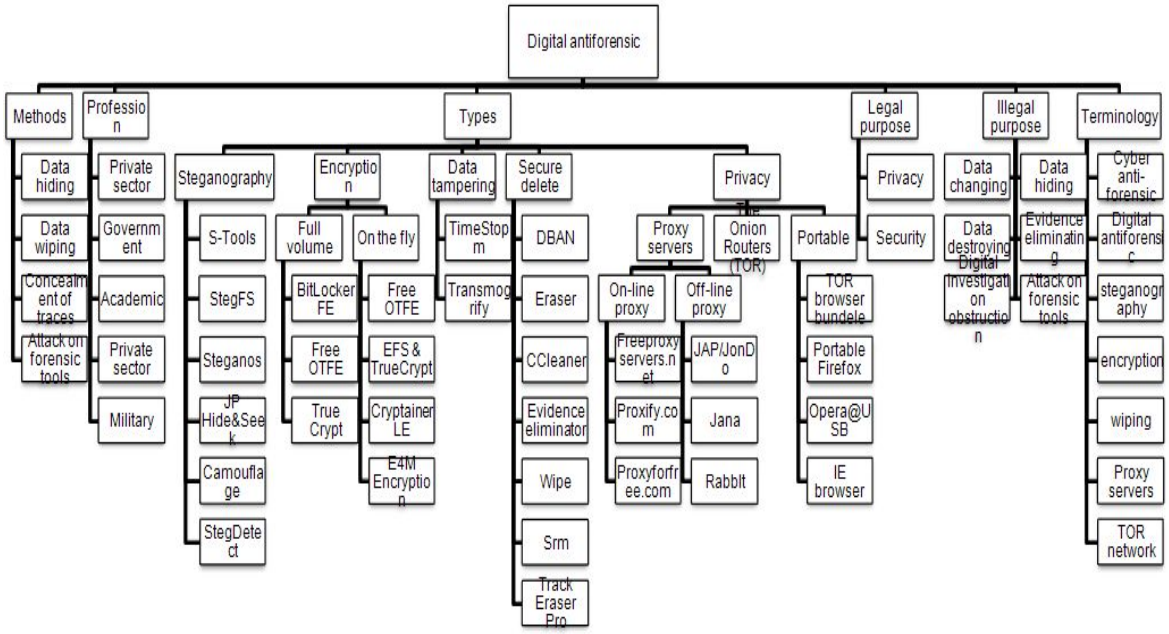

Figure 1 An ontological approach to study a digital anti-forensic

Methods can be Data hiding, Data wiping, Concealment of traces and Attack on forensic tools. Profession can be Private sector, Government, Academic, Private sector and Military. Types are further broken at lower levels, where we went to the software tools and methods.

The purpose are broken down into Legal and Illegal purpose. Reason for legal purpose is Privacy and Security and for Illegal purpose is Data hiding, Data changing, Data destroying, Evidence eliminating, Investigation obstruction and Attack on forensic tools. Terminology define a set of vocabulary which describe this methods and tools.

The original intent of digital antiforensic was hiding, change, protection and destruction of data (potential digital evidence), and obstruct of process of digital forensics by attacking forensic tools.

Looking from this aspect, methods and types can be divided into:

1. *Steganography*
2. *Encryption*
3. *Secure delete*
4. *Data tampering*
5. *Privacy and proxy servers hiding [5]*

2.1 Steganography

The creation and first use of steganography goes back many years at the time of the ancient Greeks. Very notion of a coin the word Steganos (Greek disguised) and graphein (written in Greek), which in translation means "hidden writing".

At that time, when they wanted to send a hidden message, the Greeks would shave messengers head, tattooed a message on it, and then waited for hair to grow and then send it as a secret message.
During World War II the"invisible" ink made from fruit juice, urine, milk or wine vinegar has been used to wrote messages that were supposed to be invisible.
When the paper on which message was written was heated, the ink would be obscured and the message would be readable.[3]
Steganographic process takes place so that the hidden message is inserted into a transport agent, called a carrier. Hidden message is expanded in the holder and stenographic mediator is formed. After that steganographic key is added so file could be encrypted. [3]
Added, TCP / IP protocol has certain weaknesses that can be used for so-called "Covert communication“ by private or public networks.
These omissions in the protocol are used by malicious users who transmit secret messages, and not wanting to be discovered.
Antiforensic tools use various methods and hiding mechanisms.
Some are hiding information in the so-called "slack" and "unallocated" space on the hard disk, while others use encrypted or hidden partition, or even emulate the so-called "bad sectors" to hide data.
Today dozens of tools for steganography are available, a for every operating system. The most popular are:
S-tools, StegFS,Steganos, JPHide&Seek.

2.2 Encryption

Unlike steganography, cryptography is used for further encryption and not hiding.
The data are visible but without the use of special keys unreadable and unusable.
For cryptography in forensic practice is considered as real nightmare for forensic investigators.
Today many applications, have certain tools to encrypt files, but most 2 types of tools are: tools for encryption on the fly and tools for full encryption.
The main difference is that tools for encryption on the fly are much simpler and faster for real time use.
File access is possible immediately after entering the key, while the full encryption encrypts the entire disk bit by bit, which sometimes can be very slow and takes a lot of valuable time.
Most used tools for encryption on the fly are: FreeOTFE, TrueCrypt, EFS, Cryptainer LE, while so called. FVE („Full Volume Encryption“) tools: TrueCrypt, BitLocker FVE, FreeOTFE.
Encrypted web-based communication can do traffic analysis and content that these channels are transmitting almost impossible and therefore malicious users use it very often [2].

2.3 Secure delete and data wiping

Tools and methods to permanently erase data exist for a years, since the times of DOS and UNIX.
The essence of all actions is based on one of many algorithms which on the located area (or former area) of data, overwrites a random series of 1 and 0 and for 1-35 passages.
There are many safety standards imposed by the United States, Canada, Germany, and Russia and other developed countries, and certainly the most famous are: *Bruce Schneier's algorithm, Canadian OPS-II, DoD 5220.22 M, Gutmann's algorithm, German VSITR, Russian GOST p50739-95, US Army AR380-19 S Air Force 5020.*
All today's programs that are available on the Internet are using some of the listed algorithms.
According to some claims one passage across the disk with the software is enough for irretrievable lost of data.
Most of the algorithms supported transcription 3-7 times until Gutman algorithm supports 35-fold random copying of content (0 and 1) over the disk space where they were deleted data. Gutman algorithm is perhaps the most advanced because it consists of up to 35 passages and provides full protection from restoring deleted files, but the price to be paid here is the time required for this operation.
Some of popular software are: *Acvite@KillDisk, Secure Erase, Eraser, Data Wiper Advanced File Shredder , DBAN (Darik s boot and nuke).* Programs can be used to erase the whole hard disk, parts of hard disk space, even free, space where currently are no data (as there was before) [4].

2.4 Attacking forensic tools

This method involves attacks and cheating tools used in digital forensic investigations, so as to hide the activity, changes of some system value on the computer, etc.
One way is to use the tools that delete all traces of user activity on computer, application programs, and on the Internet.
Software as *Evidence eliminator, TrackEraser, Window Washer* completely remove all traces of user activity – browsing history, cash memory, slack and unallocated disk space. This prevents the finding of these activities by the investigator in charge for digital investigations. Often the case in practice, are use of tools to change the system date and time of creation, modification, access and files update on the NTFS system.
In this purpose is used, a very dangerous tool TimeStomp "that easily can fool the most popular tools for digital forensics and made digital evidence unacceptable by the court.
Program "Transmogrify" allows the user to modify the header files as it places the header of .jpg image in

.doc file, or inversely, in order to mislead EnCase, FTK, or other forensic programs.
Another way to prevent the work of forensic tools is to hide data in the so-called "Slack" space on the hard disk. In this purpose we use tool *"Slacker"*.

2.5 Proxy servers and anonymity

In digital investigations beside computer forensics, it is often case that the information are requested from Internet Service Providers - ISPs. Most often it is necessary to know the IP address of computer which is suspected to be used for illegal purposes. In order to hide the actual IP address that is assigned to them by local ISPs, malicious users often use proxy servers. Instead of direct accessing to the server which keeps requested resource on the Internet, this method eliminates the proxy server's IP address, while the actual address of the user remains protected (only proxy is known). In order of better protection a series of proxy servers can be used. A common case is to use online proxy servers, of which the most famous are proxify.com, freeproxyservers.net etc. but the servers that are installed locally on your computer (Jana, FreeProxyServer, Rabbit, etc.)

2.6 TOR, Portable browsers and operating systems

One of the ways that can be used in anti forensic purposes as well as in legitimate purposes in order to keep privacy and anonymity when surfing the Internet is a TOR. (*The Onion Router*). TOR is a network of virtual tunnels - open and free network that helps in the battle against the so-called "traffic analysis". [11]. The idea of the TOR network is to use routes that are hard to follow and to delete "fingerprints" after a certain time. Each time you create a new route between users of TOR and that prevents packet interception and analysis of such traffic. TOR today has a dual function, it issued by cyber criminals and legitimate users (journalists, bloggers, military, government agencies and institutions) with the aim of conservation of consistency and protection to IP addresses, and privacy.

Today is a very common case the use of so-called mini or portable browsers that can be run from a USB memory sticks, or MMC / SD memory cards. This allows launching of browser and complete software is in working memory (RAM). This means, as soon as you complete activities on the internet and USB memory separates from the computer, then any traces disappear.

There are dozens of these browsers : *TOR browser bundle, Portable Firefox, Portable IE, Opera@USB* etc. They al insure so calles „silent mode„ or „private browsing" [11].
In purpose of additional protection special so called „LIVE" versions of operational systems are used. Functioning of such operational systems is that the same are not installed locally on your computer (hard drive the computer), but is run directly from CD / DVD or other portable media (USB stick, MMC, SD or other portable storage). Then they are performed in RAM memory. Shutting down of the computer erases all traces of any activities and it is almost impossible to find any evidence. The most common are versions of different Linux distributions. (*Knoppix, BackTrack, Ubuntu, Fedora,SuSe,Windows PE, Anonym.OS* i sl) . [12]

4 Conclusion and recommendation

Most authors of scientific and professional articles dealing with issues of digital anti-forensic, agree on the fact that digital anti-forensic is term connected to hackers and cyber criminals, and that the original purpose was hampering the process of digital investigations.
Yet we should not ignore the fact that these methods and techniques are used today by journalists, publicists, writers of different ("prohibited") columns and blogs, as well as experts from various spheres of social life that appear on the Internet while at the same time wish to remain anonymous and protected.
In some (many) countries in the world, even in Europe there is a review online and internet service providers exercise a strict control of traffic with the aim of censoring content that circulates over internet. Digital anti-forensic is recognized as a good method for on-line privacy protection is a method that provides a relatively safe activity.

5 Acknowledgments

The presented research and results came out form the research supported by the Centre for biometrics - Faculty of Organization and Information Science Varaždin, University of Zagreb.

References

[1] Bača,M. Introduction in computer securtity (on Croatian), Narodne novine, Zagreb, 2004.
[2] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (2nd ed.). London: Elsevier Academic Press,2004.
[3] Ćosić, J, Bača, M. Steganography and its implication on forensic investigation, INFOTEH Jahorina, B&H, 2010.
[4] Ćosić J. Secure data wiping (on Croatian), INFO 141, p.24-25, Sarajevo, 2009.
[5] Ćosić, J, Ćosić, Z. Digital Antiforensic - manipulation with digital investigation process

(on Croatian) , TELFOR, Beograd,2010, pp. 1204-1207

[6] Harris, R. Arriving at an anti-forensic consensus: Examination how to define and control the anti-forensic problem, Digital investigation 3S, ELSEVIER, p.44-49 , 2006.

[7] Fosters, LC, Liu,V. Catch me if you can...In:Blackhat briefings 2005, www.blackhatcom/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf (accessed 12.03.2008).

[8] Peron, CSJ, Legarty,M. Digital antiforensic:emerging trends in data transformation techniques, www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf.

[9] Pollit, M, Whiteledge, A. Exploring big Haystacks, Data Mining and Knowledge Management, Advances in Digital Forensic II.IFIP, 2006.

[10] Kessler, G.C. Anti-Forensics and the Digital Investigators, Proceeding of the 5th Australian Digital Forensic Conference, 2007.

[11] TOR: Anonimity on line: http://www.torproject.org/index.html.en , (accessed 01.09.2010.)

[12] The Live CD list: http://www.livecdlist.com/ (accessed 01.09.2010)