Anti-computer forensics

K. Hausknecht[1]
S. Gruičić[1]
[1]INsig2 d.o.o., Zagreb, Croatia
Kresimir.Hausknecht@insig2.eu
Savina.Gruicic@insig2.eu

***Abstract* - Generally speaking, anti-computer forensics is a set of techniques used as countermeasures to digital forensic analysis. When put into information and data perspective, it is a practice of making it hard to understand or find. Typical example being when programming code is often encoded to protect intellectual property and prevent an attacker from reverse engineering a proprietary software program.**

Through this paper the focus will be on anti-forensics methods which in sense is how information obfuscation is affecting digital forensic investigation. The paper will describe some of the many anti-forensics methods used under the broad classifications of data hiding, artefact wiping, trail obfuscation and finally attacks on the forensic tools themselves.

With any modern-day investigation relying more and more on digital forensics, investigators are required to deal with anti-forensics methods on a daily basis. This paper will explore the challenges investigators and forensic practitioners are facing when conducting investigations. The methods used will be separated into low-tech and high-tech techniques, how they are being used, how they are affecting digital forensic investigation and what the mitigation possibilities are. Focus will be on high-tech techniques that will not stop the investigation but rather prolong or make the process extremely time consuming and therefore not possible to complete in a timely manner or be cost effective.

***Index Terms* - information, obfuscation, artefacts, anti-forensics, digital forensics**

I. DIGITAL FORENSICS

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer or mobile device crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early 1980s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Forensics may also feature in the private sector; such as during internal corporate investigations or intrusion investigation (a specialist probe into the nature and extent of an unauthorized network intrusion) [1].

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis, mobile device forensics and new emerging cloud/internet or cyber forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report of collected evidence. Later it will be shown how obfuscation directly affects each of these steps.

As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents. Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions) often involving complex time-lines or hypotheses. To make this harder or impossible to do, information obfuscation is used.

Obfuscation is method used for obscuring intended meaning in communication, making the message or content confusing, wilfully ambiguous, or harder to understand. It may be intentional or unintentional (although the former is usually connoted) and may result from circumlocution (yielding wordiness) or from use of jargon or even argot (yielding economy of words but excluding outsiders from the communicative value). Unintended obfuscation in expository writing is usually a natural trait of early drafts in the writing process, when the composition is not yet advanced, and it can be improved with critical thinking and revising, either by the writer or by another person with sufficient reading comprehension and editing skills. Conventionally, obfuscation is commonly tied to encryption since it is the main way of making any type of information unreadable unless the cypher is known. Nevertheless, information can be obscured in many other ways that will be described later on [1][2][3].

The combination of information obfuscation methods and digital forensics form anti-forensics techniques.

II. ANTI-FORENSICS

Anti-forensics was first defined by Ryan Harris in 2006 in his paper “Arriving at an Anti-forensics Consensus: Examining How to Define and Control the Anti-forensics Problem” as “Attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct”. He was also one of the first to produce classification of common anti-forensics methods as described in the table below [4]:

Classification of common anti-forensic methods				
Name	**Destroying**	**Hiding**	**Eliminating source**	**Counterfeiting**
MACE alterations	Erasing MACE information or overwriting with useless data			Overwriting with data which provides misleading information to investigators
Removing/wiping files	Overwriting contents with useless data	Deleting file (overwriting pointer to content)		
Data encapsulation		Hiding by placing files inside other files		
Account hijacking				Evidence is created to make it appear as if another person did the ‘‘bad act”
Archive/image bombs				Evidence is created to attempt to compromise the analysis of an image
Disabling logs			Information about activities is never recorded	

TABLE 1 Classification of common anti-forensics methods

In his paper Ryan reflected only on several methods but in today’s world many new have emerged and the ways how data is being hidden or obfuscated has changed. This paper will go much further than this. Still, the goal of anti-forensics remains the same, avoid detection of the true meaning of data, disrupting information collection, increasing time needed to conduct the investigation, trail obfuscation, information modification, data hiding, data saturation and general casting doubt on the forensics report or testimony.

Anti-forensic techniques aimed towards digital forensics tools are especially of interest, since they exploit shortcoming of tools that are the main means of giving broader meaning to data. It is important to mention that in the period when this paper was written an average storage capacity of a computer is about 1TB of data and personal computers hold about 8GB or Random Accesses Memory (RAM). On the other hand, mobile devices have at least 16GB of data while the top capacity phones now stretch up to 256GB of data. The amount of data that must be examined is truly vast and the only way of putting any meaning to it, in a reasonable amount of time, is to use digital forensic tools that accelerate the process. Manually going through such high capacity storages would be too time consuming for police officers and the back log (number of cases waiting to be processed) would be vast, while in the perspective of corporate investigations, it would be financially unprofitable.

As mentioned earlier, there are many ways of making information hard or impossible to interpret. To build on previously mentioned classification, means of obfuscation will be separated into two main classes, low tech and high tech. As their names suggest, low tech requires basic knowledge of computing and electronics while high tech requires excellent conversance of computing/programming and electronics.

III. LOW TECH ANTI-FORENSICS TECHNIQUES

A. *Physical data destruction*

The simplest method of them all that doesn’t require any special knowledge is complete physical data destruction. Typically, this means taking data holding media such as computer hard drive or USB thumb drive and smashing it with a hammer. In some cases, this procedure can be used as an official procedure for media destruction when certain hardware becomes obsolete or is due for replacement/upgrade. Besides using a hammer, criminals will do some of the following:

- Use a power drill and bore through the hard drive plates or through memory chips
- Throw the media in water – nearby pond, toilet, pour water over electronic parts
- Use power press to completely crush the media
- Use strong magnets to demagnetize the media
- Pour acid over the media

In today’s modern world, these very primitive methods are not used very often since if applied, the media will become unusable and what is even more troublesome is the fact that data will be destroyed even for the criminals to use again. Today even the media can be somewhat expensive to replace but the data can be irreplaceable. Because of these facts, criminals will tend to use other techniques that will allow them to access the data after it was investigated by the legal authorities.

B. *Hard drive scrubbing*

Besides physical data destruction, next low tech method that is commonly used is Hard Drive (HDD) scrubbing or wiping. This is easy to implement since modern HDD’s and file system will do this automatically when data is being deleted from a digital source. Basically, a user will delete everything he doesn’t want others to find. This can be a full HDD wiping – writing zeros to the whole HDD or just deleting important files. Since this is also a destructive method on a logical form where data is being completely destroyed, persons usually go for less destructive method where they can still retrieve the data for the same reason described in the section above. The most common and fastest

method is quick formatting. By doing a quick format, only index that contains information where the data is located is deleted, but data still resides on the media. If untrained investigator performs a preview of the media he will not see any data and disregard it when in reality, everything is still there but "hidden" from the operating system.

Data deletion is commonly used by low level criminals but even an average investigator will know that soft deleted data can be retrieved by all digital forensic tools and how to do it. What is also important to state is that data deletion often implies guilt and intention to destroy evidence. Furthermore, often absence of information can be evidence itself. To explain on an example, it would be very strange to see a mobile phone that doesn't have any pictures on it since everybody takes pictures and it would be anticipated to find at least some. Another example would be to find an older computer that has no user files on it while there are traces of past user activities. Same would be if someone is buying a 5 year old car that has very low mileage – for experienced buyer a definitive sign of mileage count manipulation.

C. *Artefact wiping*

Continuing with the previous section, besides actual information deletion or partial deletion which is very destructive mechanism persons can delete artefacts that make digital forensics analysis more difficult. This can be considered as removing metadata – information that describes other information. To accomplish this, users can utilize various free programs used for fixing or clearing up space on computers as CCleaner, Clean Master, BC Wipe or Eraser. These programs are advertised as PC optimization tools, speeding up systems, clearing up space, safe browsing, privacy protection etc [5]. In reality what they do is remove browsing history, delete cache files, delete operation system files, wipe slack and unallocated space and "clean" registry files. All this information is used to create a better picture of what the person was doing on the system, what was their intention and if they were trying to hide their true goal. For example, by wiping artefacts investigators can find an incriminating picture but they don't have the information on who was the original author, to whom was it sent to or how did it get on the system.

Mitigating this method is relatively easy. No tool is perfect and therefore "anti-forensic" tools are not perfect and will leave something behind that could be used during the investigation. As before, the mere presence of the tool will raise suspicion with the investigator and make him dig deeper into analysis.

D. *Steganography*

A bit of history… Roots in hiding data/information begin with steganography - the practice of concealing messages or information within other non-secret text or data [5]. When put into digital information perspective, steganography can be used on computers and networks through steganography applications that allow for someone to hide any type of binary file in any other binary file, where image and audio files are today's most common carriers. To put it simple, hide pictures in MS Office PowerPoint or word document or hide a message in a spam email. Persons can go even one step further by covering picture, table or text block under a white block so if the document is quickly reviewed it would be hard to spot. Most modern digital forensic tools will detect most of these anti-forensics methods since they unpack and index documents with their metadata [6][7]. Of course, this can also be a high-tech technique if data is being embedded in an audio file or inside the picture, null cyphers can be used to select a pre-determined pattern of letters from a sequence of words or similar. These methods are rarely used since they are hard to implement, take time to do and also require lot of time to decode. Steganography is especially hard do implement on data that is accessed often.

E. *Cryptography*

Cryptography is a very easy and commonly used technique to hide data. Sometimes it is also described as an ultimate anti-forensic tool since if properly implemented, will put the digital forensic investigation to a complete halt. It is very easy to implement since there are variety of tools, both paid and free that have excellent encryption algorithms and are simple to install and use. Most commonly known programs widely used all over the globe are Truecrypt, Veracrypt and Bitlocker for Windows and Linux machines while Apple devices use proprietary encryption FileVault. They can be implemented in two ways – full disk encryption or file/container encryption.

If full disk encryption is used, whole media (hard drive, memory card, USB thumb drive) will be fully encrypted, first to last byte and without a password no data is accessible or retrievable. If less known product is used for encryption, even with knows password it can be troublesome to retrieve the data.

Other type is file or container encryption. This method will create an encrypted file or encrypted container that can store other files and acts as a vault. Everything stored in this container will be fully encrypted but rest of the files on a system or media will be readable. Digital forensics tools will often detect encryption but don't have any means of decrypting the data without the proper password. There are tools that will attempt to break the encryption by trying to guess the password, but this method of decryption is a very time consuming process and with no guarantee of success. The table below represents the number of combinations per number of letters in a password.

Number of Letters	Possible Combinations
1	94
2	8836
3	830584
4	78074896
5	7339040224
6	689869781056
7	6.4847759e+13
8	6.0956894e+15

TABLE 2 Password combinations

This table is only for English dictionary and does consider capital letters, numbers or special characters which make up total of 94 different characters:

- numbers (10 different ones: 0-9)
- letters (52 different ones: A-Z and a-z)
- special characters (32 different ones)

Usual password length today is 6-8 characters with requirement for at least 1 small and 1 capital, and 1 number. As seen from the table, even with today's powerful computers that can compute 100.000 passwords per second, for 6 character password it would take several years to guess the password [8][9].

Encryption can be implemented not only on stored data but also to hide data/information that is being transmitted over the network. This can be implement through various ways such as PGP, encrypted VPN, TOR networks and similar. Again, if an investigator is collecting network traffic, all data will be fully encrypted and not possible to interpret.

Similarly to data deletion, encryption in respect to the circumstances, can be interpreted as intention to hide data and raise suspicion which for suspects is an undesirable effect since it will cause investigators to dig deeper into the case. On the other hand, encryption it widely used as a necessity, corporate or government rule or is turned on by the manufacturer by default. Usage of encryption can be debated but it not the subject of this paper.

IV. HIGH TECH ANTI-FORENSICS TECHNIQUES

Most of low tech methods can be utilized with various free tools and do not require any special interaction from the user except running the tool and making few selections. The main issue they have in common is that they raise suspicion from the investigator side, since they leave noticeable traces and it's very easy to spot something is wrong, missing or hidden. On the other hand, high tech methods are not destructive and are focused more on hiding data, breaking digital forensics tools and process, or causing prolongation of the whole investigation. These methods will try to confuse the automated process of evidence discovery and basically make the whole investigation last longer and therefore making it not financially profitable. To better understand how this is achievable, the regular forensic process must be defined. These are common steps that are part of any digital forensic investigation:

1. Collection – gathering all relevant evidence from the crime scene
2. Preservation – respecting the chain of custody. Marking and transporting the digital evidence from the scene to the lab
3. Identification – reviewing and identifying gathered evidence and determining what and how it should be processed
4. Analysis - preforming digital forensic analysis of collected evidence
5. Presentation – creating a report on the findings

Each of this basic steps will be challenged with the goal not to prevent the forensics from happening but rather just slowing down the examination process down until the data loses its value or intelligence or cost.

There are many high tech anti-forensics methods and this paper will mention just some of them since they are very technical and as mentioned before, require a lot of advance knowledge of computing.

A. *Data saturation*

To start simple, it is very easy to create problems in collection phase of investigation - own a lot of media. Simply, persons will never throw out old hard drives, USB drives, memory cards, phones, laptops or any storage media. When investigators come to the scene, they will find all this media that they cannot neglect and must either review on the scene, image or take with them to the laboratory. This will prolong the time needed to image all storage media before it can be processed and examined.

To mitigate this, investigators must parallelize the acquisition process – utilize multiple duplicators and machines. Also, investigators can use the suspects hardware against them to preview the evidence prior to imaging.

In the later investigation phase, data saturation can also be applied by creating or owning a lot of false data or senseless data. This method will again prolong the investigation since the investigator must divide false from real data and later on come to some concrete conclusion. The same is often used when one is trying to conceal its public information by creating vast number of false information.

Mitigation technique involves having as much as possible data about the case so that through analysis investigator can easily pinpoint desired information. Never the less, there will always be cases where data crosscheck will be required.

B. *Hiding data*

Similar to steganography where binary data is hidden in other binary data, the same effect can be accomplished in numerous ways. This section will address only few that are very common and appear in many digital forensics investigations.

Most common would be hiding data in virtual machines. In computing, a virtual machine (VM) is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a full physical computer. Their implementations may involve specialized hardware, software or a combination [10]. Even an average personal computer today is capable of running virtual machines and software for creating them is very easy to use. Persons that want to hide their activity create VM's and use them for malicious or secret work while the host machine is used for everyday work. These machines can also be fully encrypted or password protected for strengthen security.

Next possibility of hiding data can be accomplished by storing data in other user disk spaces, closed sessions on compact discs and public or shared servers. By storing data away from the original machine where it is actually being used, if not all data storage spaces are inspected it can easily be omitted. Furthermore, analysis of such data can be tedious work since it can be difficult to determine the owner of the information. This poses a serious problem for digital forensic

investigator since data today can very easily be transferred and received over the network to and from a remote location. In cases where data is being stored on remote servers outside the person's country, police officers usually don't have any jurisdiction over that kind of data and is often inaccessible.

To mitigate this, investigators must perform live machine analysis and dawn raids where persons of interest don't have time to delete, disconnect or close their sessions to remote data. When data is stored in such way, there is always some data leftovers that will provide clues to investigators on what was going on and how the user was operating.

C. *Hiding data in slack and unallocated space*

Over 80% of computers today are running Windows OS which implies that the most used file system is Windows New Technology File System (NTFS) [11]. When formatting a hard drive to NTFS users have a choice of how many partitions they want to create, e.g. if they want to format the whole drive or create several partitions. After partition is created, certain portion of hard drive space will be reserved for file system files and there will be partitions that will remain unused by the file and operating systems. Some of these protected and unused areas are Master Boot Record (MBR), Host Protected Area (HPA), Device Configuration Overlay (DCO), unallocated hard drive space. These areas are never used by regular user and are by default inaccessible, but for skilled user they can be used for storing sensitive data or for data exchange between users. If storage media is not properly examined, it is very easy to omit these areas.

Main stream digital forensic tools will always examine most of these areas for data but some, such as HPA and DCO, must be explicitly reviewed if any trace of hidden data exists. If investigator is performing a manual analysis, it is very easy to overlook.

D. *Nonstandard RAID configurations*

RAID or redundant array of independent disks provide a way of storing the same data in different places (thus, redundantly) on multiple hard disks (though not all RAID levels provide redundancy). By placing data on multiple disks, input/output (I/O) operations can overlap in a balanced way, improving performance. Since multiple disks increase the mean time between failures (MTBF), storing data redundantly also increases fault tolerance [12]. In order to create a RAID array, users must define share stripe patterns, block sizes and various other parameters. By using nonstandard parameters, if investigators image or confiscate the drives, before they start the analysis they must rebuild the RAID array. If parameters are not known this is not possible. RAID arrays commonly need not only proper parameters to function but also dedicated hardware. If nonstandard hardware is used, this will also cause issues during investigation.

To mitigate, investigators can de-RAID volumes on suspects machines, create images on suspect machine or preview the data. It would be recommended to image volumes rather than physical drives and therefore worry only about copying data to destination drive. Recording configuration of the suspects machines is a necessity.

E. *File signature masking*

All digital forensic tools work with file signature rather than file extensions. This basically means that all files will be analysed and handled by their binary header and/or footer (signature) rather than the file name extension which is easily changed just by renaming the file with a single click. In the past, this method was widely used to hide data on the system, but today it would be detected automatically by forensic tools. To make it harder, users can "hollow out" a file and store wanted data inside it. To go even one step further, data that is pasted in the middle of the other file can be encrypted. This method is sometimes also called transmogrify since the original file is being significantly changed. Other method would be to change the file header/footer rather than the file extension to confuse the digital forensic tool. For an example, all *.jpg picture files have header FF D8 in hexadecimal representation and by changing it to e.g. 00 00 00 14 66 74 79 70 would mask it as Quick Time movie file. If somebody tried to open such modified file, they would get an error.

Mitigating file signature masking can be accomplished with usage of fuzzy hashing. In order to understand this, general file hashing must be explained. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. Put simple, hash function is a mathematical formula that takes any value as an input and returns a fixed size result. If the input changes even by one digit or one byte, the resulting output will be a completely different number. In forensics, most common hash functions used are MD5 which returns 128-bit value and SHA-1 which returns 160-bit value. Hashing in computing is mostly used to find and/or compare data. This will be discussed later. Going back to fuzzy hashing, it is a concept which involves the ability to compare two distinctly different items and determine a fundamental level of similarity (expressed as a percentage) between the two. Chances are that the person or suspect chose a file from his own system and copied it or hollowed it out. By analysing recent files investigators can easily spot suspicious activity such as opening system file as rundll.dll with Excel. Also during analysis when fuzzy hashing produces results that specific file is very similar to notepad.exe. One other mean of mitigation is to use National Software Reference Library (NSRL) which is a large database of known files with their hash values. NSRL database contains large physical collection of commercial software packages (e.g., operating systems, off-the-shelf application software as MS Office, Adobe etc.), detailed information, or metadata, about each file that makes up each of those software packages and smaller public dataset containing the most widely used metadata for each file in the collection that is published and updated quarterly [13] Investigators use NSRL libraries to filter out "typical" files from the evidence so that only unknow remains. This process is sometime called De-NISTing.

F. *NSRL Scrubbing*

In previous section NSRL database was introduced. As investigators use NSRL on regular basis to reduce the amount of data needed to be analysed, suspect will try to disable the usage of this database by modifying system, program and other files in general. As mentioned before, if only a fraction of input data is changed, the resulting hash value will be completely different and therefore it will not match the record in the database. This is accomplished by modifying strings or insignificant part of files. Furthermore, by turning off Data Executing Prevention (DEP) which is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system, hashes will again be changed and no longer match with the NSRL databases.

There is no easy way of mitigation for this technique of masking files and therefore obfuscating information they hold. There are some guidelines investigators can follow not to omit important information. Instead of using blacklisting, whitelisting approach is preferable – approach that looks for things that match. Investigators are encouraged to identify useful files rather than eliminating them.

G. *Scrambled MACE Times*

Timing is everything. Same can be said for digital forensics investigations. It is of utmost importance to establish proper timeline of events. Investigators will also utilize dedicated tools for creating histograms in addition to timelines of events in order to create a better picture of what and when something happened. All files on computer store multiple timestamps:

- Modified - the last time file was modified or written to
- Accessed - the last time file was read
- Created - the file's creation date
- Entry - the last time the Master File Table (MFT) entry was updated

As it can be seen above, these four times form MACE acronym. By changing these times either manually or by randomizing them, investigators will have hard time in determining the proper timeline of events. Time changes can be also accomplished by changing BIOS time, turning off "Last Access" update in Windows or by changing time zone of the system.

Mitigation process involves ignoring MACE times and creating new timeline by determining proper ones. As an example, suspects will rarely go to such lengths of changing all possible times on the system and since majority of systems are connected to the internet, investigators only need to find times that are correct by comparing them to real time. Log files will usually be sequential and therefore anything that is off can be considered to be changed intentionally. Also, identifying small sets of similar times can prove to be helpful since investigator only needs to determine the time offset to the real time. All times that are completely scrambled can be ignored. Scrambled MACE times is one of the most difficult anti-forensic techniques to mitigate since it can be very hard to determine when something happened to the second, since that information can be crucial to any case.

H. *Restricted filenames*

Since this paper is addressing information that is stored in a digital form, in order for that to be possible a storage media is needed. Every storage media must be formatted to a specific file system to hold data. In computing, a file system or filesystem is used to control how data is stored and retrieved. Without a file system, information placed in a storage medium would be one large body of data with no way to tell where one piece of information stops and the next one begins. By separating the data into pieces and giving each piece a name, the information is easily isolated and identified [14]. A filename (or file name) is used to identify a storage location in the file system. Most file systems have restrictions on the length of filenames. In some file systems, filenames are not case sensitive (i.e., filenames such as FOO and foo refer to the same file); in others, filenames are case sensitive (i.e., the names FOO, Foo and foo refer to three separate files). Most modern file systems allow filenames to contain a wide range of characters from the Unicode character set. However, they may have restrictions on the use of certain special characters, disallowing them within filenames; those characters might be used to indicate a device, device type, directory prefix, file path separator, or file type (File system, 2016). As mentioned earlier, most widely spread file system is Windows NTFS. This file system has specific restricted file names such as:

- CON
- PRN
- AUX
- NUL
- COM1, COM2, COM3, COM#
- LPT1, LPT2, LPT#

Furthermore, file names cannot have nonstandard or hidden characters as 0xFF 'e, ~u or similar. If file has a restricted file name or file name contains nonstandard or hidden characters, it will not be accessible through the operating system and will confuse the digital forensic tools. Also, some functions in tools will not work properly such as exporting files. This again will not stop the investigation but will cause prolongation of the data analysis since live preview and live analysis will not be possible until the data is properly imaged and analysed in a forensic tool.

Mitigation is relatively easy since the only requirement is to process all acquired data in a digital forensic tool. Files with such modified file names must be exported with different files names or with file ID number as a name.

I. *Circular references*

As defined in the previous chapter, file system not only has file name restriction but also file location restrictions. Users can also exploit this restriction for hiding data. Folders have a limit of 255 characters for the full file path. If file is stored with a file path longer than 255 it will become inaccessible to the operating system and therefore to the investigator. File path can also contain "junctions" or "symbolic links" that change the actual file location. File can be represented to the operating system in way that the actual file location is in a completely different location than reported. Users can also use circular references in a way that the file is being stored in

file path as: C:\Parent\Child\Parent\Child etc. to confuse the investigator or they can be stored in multiple nested folders to cause the tool to run into an infinite loop or throw errors during acquisition or analysis [15].

As in previous case with restricted filename, mitigation is relatively easy. Just knowing about this method will help investigator circumvent it. Investigators should always work from digital forensic images and be mindful about this anti-forensic method when dealing with a live system.

J. *Broken log files*

In addition to file MACE times, logs can also be vital evidence. Logs will show important information such as when a user logged in to the system, when did he log out, what programs were used, when did the system restart, how application was used and in general will lay out an audit trail. To hide their activity and make the information hard to retrieve, users will make changes to log files as described in artefact wiping, file signature masking or restricted filenames sections of the paper. This will confuse certain data parsers and make them throw errors [16].

To mitigate broken log file method, investigators first must ask themselves whether they actually need the log file. Usually there should be sufficient data to gather all necessary information from evidence files – try to prove a point without logs. If there is a necessity for examination of the log file, they can potentially be parsed in portions (parts that are needed), create custom small scripts that will perform automatic parsing or zero in on the specific records that are of interest rather than parsing the whole log.

K. *Portable systems and programs*

With the introduction of restricted user profiles that don't have administrator privileges and no possibility to modify the system (eg. install new programs or change settings), many portable software's have emerged ranging from simple programs as file browser to full portable operating systems. These applications and systems can be simply copied to a portable USB thumb drive and used on whatever system is available. Most common usage would be in public internet shops or libraries. Person just plugs the USB thumb drive into computer and boots into his own operating system, usually Linux. There he has a full control over all hardware that is available. After he is done, he simple takes his USB and boots back to the original operating system leaving almost no trace on the host machine. Similar can be done with programs. Portable version of internet browser can be run directly from the USB. In this way majority of data will be stored on USB drive itself and therefore very little will be left on the machine hard drive for investigators to go through.

Mitigation method requires thorough preparation before going to field. On the scene, machines must be imaged live, computer memory must be captured and all media storages must be confiscated. This procedure will ensure that investigators have all possible data sources that will enable them to perform full analysis.

L. *Non standard program usage*

The last method that this paper will address is based on usage of nonstandard tools. As mentioned multiple times throughout this paper, what was addressed were the most common operating systems, file systems, programs etc. Digital forensic tools parse best "common" data that is coming from common programs or sources. To lay out an example, there is excellent support for parsing artefacts coming from Microsoft Office but few coming from LibreOffice. All Microsoft Windows operating system versions are supported but not all Linux operation systems are supported. The same can be said for smaller types of software such as internet browser, encryption programs, communication programs etc. It is easy to spot an emerging pattern that is exploited by users. By using non-popular programs, it is very easy to hide activity, information or intentions since tools will not parse data coming from non-popular/standard sources.

Mitigation of this method can only be achieved by constant education and by following current trends. Investigators should train themselves to spot suspicious applications and educate on how they work. Unfortunately, investigation of such data should be performed manually and will definitely prolong the overall investigation time.

V. CONCLUSION

In today's modern world where almost all information is exchanged in a digital from, digital forensics plays a big role. Conceiving true form of information, person's intention, information destination or source are just some of the ways data and therefore information is being manipulated and therefore making discovery and data analysis hard or impossible to perform. In digital forensics, anti-forensics methods are trying to confuse investigators and their tools in accomplishing their task. Over the years, goal of anti-forensics changed from trying to completely deny access to information, to just making it too hard to obtain or being cost effective. The main reason for this change is that the lack of evidence is evidence itself and intentional (obvious) hiding of information, raises unwanted suspicion. It is also necessary to mention that complete data destruction is not an option since in today's world, information is money.

Taking all methods that were explained throughout this paper into account and considering that there are many more available, it can be concluded that it is very easy to disrupt digital forensic investigation. There are also other factors that make investigation hard to perform, one of them being data stored in the cloud that takes it out of current investigators jurisdiction and making it hard to obtain and investigate. The future with everyday development of hardware and encryption possibilities will bring even more obstacles in conducting investigations. The only method that can help investigators to come on top of this never-ending battle is education. Knowing about these and other methods and their mitigation is to only way investigators will be successful in their jobs.

REFERENCES

[1]. K. Conlan, I. Baggili, F. Breitinger, Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy, Digital Investigation, Volume 18, Supplement, 7 August 2016, Pages S66–S75

[2]. Obfuscation. (2016, December 12). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Obfuscation

[3]. Strickland, J. (2016). How Computer Forensics Works. Retrieved 2016, from How Stuff Works Tech: http://computer.howstuffworks.com/computer-forensic3.htm

[4]. Harris, R. (2006). Arriving at an Anti-forensics Consensus: Examining How to Define and Control the Anti-forensics Problem. DIGITAL FORENSIC RESEARCH CONFERENCE.

[5]. Piriform. (2016, December). Piriform. Retrieved from CCleaner: https://www.piriform.com/ccleaner

[6]. Steganography. (2016, December 14). Retrieved from Wikipedia : https://en.wikipedia.org/wiki/Steganography

[7]. Kessler, G. C. (2015, February). Gary Kessler Associates. Retrieved from An Overview of Steganography for: http://www.garykessler.net/library/fsc_stego.html

[8]. Brute forcing passwords (2012), Retrieved from Extreme Tech: https://www.extremetech.com/computing/133110-are-fpgas-the-future-of-password-cracking-and-supercomputing

[9]. Password combinations (2016), Retrieved form AceBit: https://www.password-depot.com/know-how/brute-force-attacks.htm

[10]. Virtual machine. (2016, December). Retrieved from Virtual machine: https://en.wikipedia.org/wiki/Virtual_machine

[11]. Net market share. (2016, December 14). Retrieved from Desktop Operating System Market Share: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpob=ColumnName

[12]. TechTarget. (2015, April). Retrieved from RAID (redundant array of independent disks): http://searchstorage.techtarget.com/definition/RAID

[13]. National Software Reference Library. (2016, February). Retrieved from National Institute of Standards and Technology : http://www.nsrl.nist.gov/

[14]. File system. (2016). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/File_system

[15]. Chhabra, G. S. (2014). Anti-Forensic Techniques: An Anlytical Review. Thepar University.

[16]. Palmer, C., Newsham, T., Stamos, A., & Ridder, C. (2007). Breaking Forensics Software: Weaknesses in Critical Evidence Collection. Retrieved 2016, from Black Hat USA 2007: http://www.blackhat.com/html/bh-usa-07/bh-usa-07-speakers.html#Palme