A Survey On Anti-Forensics Techniques

Murat Gül, Emin Kugu
Computer Science
Hezarfen Aeronautics and Space Technologies Institute, National Defense University
Yeşilyurt, İstanbul, Turkey
muratgul2003@gmail.com; e.kugu@hho.edu.tr

***Abstract*—Digital forensics methodologies and tools have become a crucial part for investigation of cybercrimes and collecting digital evidences in a case. Digital forensics experts usually follow a common workflow and use known methodologies and tools while investigating a case. Attackers and cybercriminals also know which methodologies are used in an investigation and how digital forensics tools work. As a consequence, they started to find and implement a new methodology which is called anti-forensics for deceiving investigator or having a case lasts longer than expected. Anti-forensics has been acknowledged as a legitimate field of study recently, therefore it can be considered as an emerging area of interest and there is a lack of knowledge about anti-forensics techniques. This paper aims to make mention of the anti-forensics techniques such as Data Pooling; Non-Standart RAID'ed Disks; Manipulating File Signatures; Restricted Filenames; Manipulating MACE (file Modified, Accessed, Created and Entry) Times; Loop References; Hash Collisions; Dummy HDDs and proposals for mitigating these techniques.**

Keywords— digital forensics;counter forensics; anti forensics; anti anti-forensics.

I. INTRODUCTION

Information technology (IT), has significantly changed human lifestyle. Especially 21st century has been a rising period in the history. IT and digital communications have improved our living standards to a higher level [1]. However, digital communications have provided criminals a newer way to commit crime called as digital crime (cyber-crime) which is the combination of wide range of crimes, such as identity theft, online piracy, hacking, and terrorism.

Digital crimes are not new. With the crimes shifted to cyber space, it was required to establish a new discipline, called computer forensics (CF), for collecting electronic evidences scientifically and technically, investigating and presenting findings to law enforcement agencies (LAE) to prove the crime. LAEs have been dealing with crimes involving electronic devices and communications since the 1970s [1]. The number continues increasing exponentially [2]. Counter-digital-crime techniques have been increasing as well [3]. They are called anti-forensics and they mean efforts to weaken the availability or integrity of evidence before or during the digital-forensics process [2].

Users and cyber criminals can make use of anti-forensic tools and methods to remove digital evidence much like how criminals could take away evidences from crime scenes. Investigators of the physical area have robust and well-established techniques to detect a removal or a tampering of evidence at a physical crime scene. However, this is not true for digital crimes. Although there is a well-established taxonomy of anti-forensic techniques, anti-forensic tools have not been analyzed in detailed yet [2].

This paper aims to review anti-forensics techniques (AFTs) and mitigation proposals against them. The goal of this paper is to cover newer techniques but classical anti-forensics techniques. Section 2 provides related works in the scope of anti-forensics techniques. Section 3 covers new and most used methods such as data pooling; non-standart RAID'ed disks; manipulating file signatures; restricted filenames; manipulating MACE times; loop references; hash collisions; dummy HDDs and mitigation proposals against these anti-forensics techniques. Eventually conclusion notes presented in section 4.

II. RELATED WORKS

Shirani defined anti-forensics as "Hiding intrusion attempts to a computer system" in 2002 as pointed out in [5]. Peron and Legary in [6] provided a definition as "Attempt to limit the identification, collection, collation and validation of electronic data" and divides anti-forensics into four categorization: destruction of data, hiding of data, data creation prevention and emerging techniques such as transformation methods utilized by rootkits or rogue shared libraries which could exploit system calls or run time linkages to alter data while creation process.

Entire software packages designed for anti-forensics purposes were evaluated by Geiger in [7]. It provided a detailed survey on six anti-forensics tools: Window Washer, SecureClean, CyberScrub, Professional, Evidence Eliminator, and Acronis Privacy Expert. All tools were run on Windows XP operating system. The paper consists examination of tools' capabilities by analysing the disk images with Forensics Tool Kit (FTK). FTK showed notable shortfalls of each anti-forensics tool such as insufficient wiping of unallocated space which could cause the recovery of evidential data. Furthermore it showed that each tool had fingerprints which is a sign of anti-forensics application used. Harris attempted to reach a standardized method of addressing anti-forensics by defining the term, classifying the anti-forensics techniques and indicating general principles to preserve forensic integrity in [8]. In this work, human elements, dependence on tools and physical/logical limitations were taken into consideration as an exploited items in the perspective of anti-forensics purposes.

According to Grugq, anti-forensics has three strategies which are data hiding, data destruction and data contraception

978-1-5386-1880-6/17/$31.00 ©2017 IEEE

[9]. In this paper data contraception has been identified as the effort to limit the quantity and quality of forensic evidence by keeping evidentially valuable / useful, data away from the disk. From this perspective, data contraception could fall under evidence source elimination category in [8].

A newly approach for categorization of anti-forensics techniques was proposed by Rogers in [10]. The taxonomy which is widely adopted in digital forensics research has four categories "data hiding, artefact wiping, trail obfuscation and attacks against both the forensic process and forensic tools". Another useful paper was presented by Garfinkel [4]. The paper presents a research about present-time anti-forensics tools such as Transmogrify, Timestomp etc. It also gives information about anti-forensics techniques which minimize footprint and exploit computer forensics tools' bugs. In addition, it provides examples of anti-forensics techniques that detect computer forensics tools running and change its behaviour like not decrypting its payload if it realized that it is running on a disk which has been imaged. Eventually countermeasures for detecting anti-forensics techniques were outlined.

Smith put forth in [11] that disk-avoiding anti-forensics tools are growing in use. Therefore it is required that disk-avoiding tools need to be described and classified in order to have forensics investigator to be informed of and so be able to diagnose the tools and gather information produced by them. Memory resident compiler/assemblers, syscall proxying, remote library injection, LiveDistros, and direct kernel object manipulation (DKOM) are described as disk-avoiding tools in Smith's paper.

Different perspective to persevering a rootkit and the related anti-forensics tactics that can be involved to frustrate an investigator who's performing an autopsy of a disk image were examined in [12]. The anti-forensics tools and techniques, mainly rootkits, were described in the form of steps followed by a forensics investigator.

Dahbur and Mohammad covered challenges of anti-forensics in [13]. This paper presented a categorization of anti-forensics procedures, techniques, and tools and assess their success.

III. Modern Anti-forensics Techniques and Mitigation Proposals

Digital crimes or cyber-crimes have risen in frequencies, and their degrees of complexity have also advanced [14]. Therefore, digital forensics (DF) plays significant role to get the digital evidence.

A. Anti-forensics

Electronic devices and IT are massively and prevalently used by users, but they are used by criminals and attackers as well for malicious purposes [15]. The lack of knowledge of anti-forensic techniques limits the focus of digital forensics analysis, so digital evidence cannot prove the guilt or innocence of the suspect. Similarly, without knowing the details of individual anti-forensics tools, forensics investigators cannot provide valid digital evidence to criminal investigators.

Anti-forensics has been defined as "Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct" by Dr. Marcus Rogers in [16]. As understood from definition, the aim of anti-forensics is to frustrate and mislead forensics tools and investigators, make it hard for them to find attacker who evades getting caught or add man-hour ($) and make case cost a lot more money. According to Garfinkel, anti-forensics is a growing collection of tools and techniques that frustrate forensic tools, investigations and investigators in [4]. As creators of anti-forensics tools and methods it is stated that anti-forensics is the application of the scientific techniques to digital media in order to invalidate factual information for judicial investigation [17].

The general categories for anti-forensics techniques presented in [18]:

- Hiding, Obfuscation and Data Encryption,
- Deletion or Data Destruction,
- Data Falsification,
- Analysis Prevention,
- Obstruction of Traces Collection,
- Tools Subversion.

This paper does not intend to cover the classical anti-forensics techniques such as HDD and File Wiping, encryption, steganography and physical destruction but the modern anti-forensics techniques.

Modern anti-forensics techniques generally aim minimizing footprints, exploiting DF tools' bugs and they are used more often than classical anti-forensics techniques. The following techniques are needed to be taken into consideration by forensics examiners.

B. Data Pooling

This simple technique means having a lot of media by attackers. The attackers intend to keep every piece of digital media they have ever had such as every USB key, every burned CDs/DVDs, every cell phones, every laptop and every hard drive. If all of these media are used frequently then investigator will have to search all of them and look through everything because of being used within the last few months. This will add too much time and cost to the investigation. The question how long the investigation will take depends on the number of devices collected. This technique directly aims the phase of data collection in a DF event.

For mitigating this technique, two techniques can be used [19]. The first technique is that investigators can parallelize the data acquisition process. Parallelizing data acquisition process can be done by using more drive duplicators limited by the budget. The drive duplicators copy source drive of suspect to a blank drive byte for byte. The second one is using their hardware against them. If it is possible to use their laptop or desktop, a bootable write-blocking Linux Live CD can be used. After operating system booted, all data can be copied to an external hard drive. In addition, digital forensic triage techniques should be well implemented as proposed in [20].

The real challenge in data pooling is the fact that imaging large datacentre (such as amazon.com, ebay etc.) in the event of DF [21].

C. Non-Standart RAID'ed Disks

Redundant Array of Independent Disks (RAID) is a technology combining multiple physical drives into single logical unit for the purpose of data storage virtualization [22]. Common RAIDs like RAID 0, RAID 1and RAID 5 shares parameters such as stripe patterns, block size and some others. This simple anti-forensics technique consists of using uncommon settings like arbitrary disk order, stripe order, stripe size, block size and endianness. And also using uncommon RAID controllers which has different settings and parameters may force investigator not to combine RAID arrays back properly. For instance, for jpeg files which are improperly reassembled may look like a jigsaw of a photo. This technique also aims to hamper data collection phase as data saturation technique does.

In order to mitigate this technique, volumes can be de-RAID on suspects' own system using a boot disc which could use their RAID controller. Their hardware will reassemble data for the investigator [19]. The second one is to image volumes not the physical HDDs. Lastly, using specialized software that attempts to identify the RAID configuration and to recover data, such as R-Studio, is another mitigation proposal.

D. Manipulating File Signatures

File signature analysis done by forensics investigator is an effective way of deciding if a file tampered or not. Files are specified by their extensions (.exe, .pdf, .jpg and etc.) on Windows based systems. The Windows operating system uses these extensions to load the required software when the user calls a specific file to open. Although UNIX based systems shows the extension of a file, the operating system does not require extensions to load the correct software which will open the file. The UNIX based systems are able to look at the file signature to determine what software is needed to open the file. This is why UNIX based systems do not require file extensions [23].

The file signature is a small block of hexadecimal code used to determine the type of file. The file signatures of a file can be seen by a hexadecimal editing tool. The example of a file signature of a Windows executable file (Hex: 4D 5A; ASCII: MZ) is depicted as highlighted in Figure 1 which is an .exe file opened with HexEdit program.

A list of file signatures from [24] which belong to some well-known file extensions is presented in Table 1.

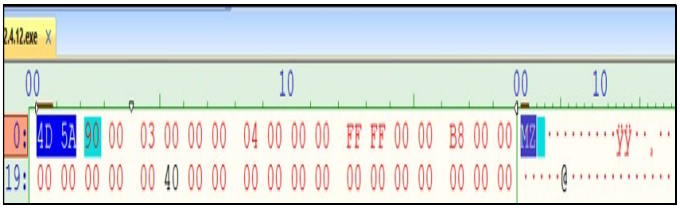

Figure 1. The File Signature of Windows Executable File.

TABLE I LIST OF FILE SIGNATURES OF MOST COMMON FILE TYPES

File Extension	File Signature (HexaDecimal)	File Signature (ASCII)
Adobe PDF	25 50 44 46	%PDF
Microsoft Office 2007 and Plus (DOCX)	50 4B 03 04 14 00 06 00	PK.....
Microsoft Office 97-2003 (DOC)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
JPEG Images	FF D8 FF E0	ÿØÿà
GIF Images	47 49 46 38 37 61	GIF87a

Transmogrify which is a Metasploit 2009 Project MAFIA tool had the capability of changing file header and extension for an attacker. And this made EnCase which is a forensics tool to analyse images of a hard drive recognize, for instance, a jpeg file as a Windows executable file. This tool is not accessible for now in Metasploit Database because of not being updated more than five years. But it is still possible to change file header and extension manually.

In example shown in Figure 3, a text file's (transmogrify.exe) header is modified as MZ (Windows .EXE Header) in HexEdit tool and extension changed as .exe manually. When filtered by Autopsy 4.1.1 which is an open source digital forensics tool, it is shown as executable file in spite of being a text file originally. Furthermore it can be seen in Figure 2, Autopsy shows indexed text at the bottom.

Another method is storing confidential data in another type of a file. Appending binary files (for example using copy/b in Windows command line) can also be used for masking signature of a file. This techniques aim at disrupting data analysis phase of a DF investigation and also could be counted as attack to DF tools by exploiting the tool's bug.

Using "Fuzzy Hashing", which is defined in [25], is one of the mitigation technique by identifying similarity between files. If attacker chose a file from his/her own system to copy confidential data, similarity could be found. The fuzzy hashing is supported by FTK DF tool. The second mitigation is to analyse "Recent" lists of applications to search suspicious activity like opening a .dll file with notepad [19].

E. Restricted Filenames

Windows systems has holdovers from DOS days such as restricted folder and file names. Folder and file names like "CON, PRN, AUX, NUL, COM1, COM2, COM#, LPT1, LPT2 and LPT# are restricted and cannot be given to any folder or file normally. These are MS-DOS reserved names for

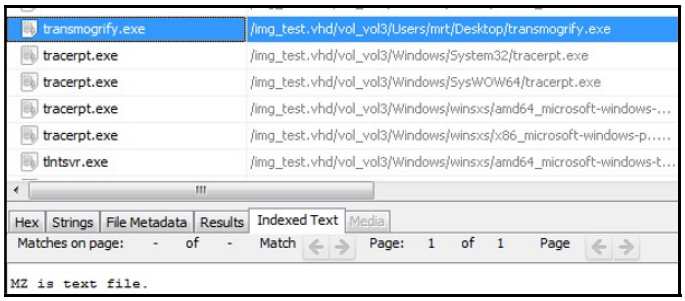

Figure 2. Manipulated File Signature Example filtered by Autopsy 4.1.1

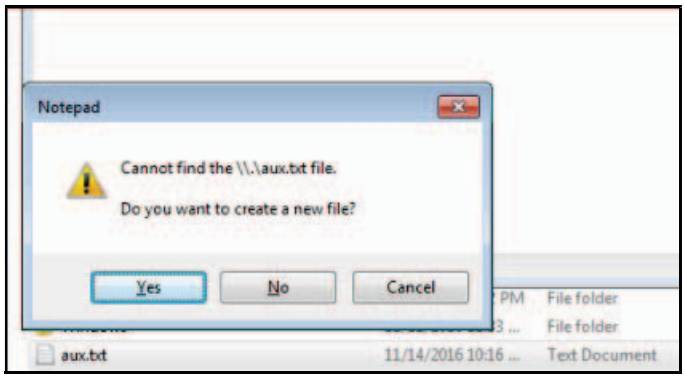

Figure 3. Restricted Filenames Error.

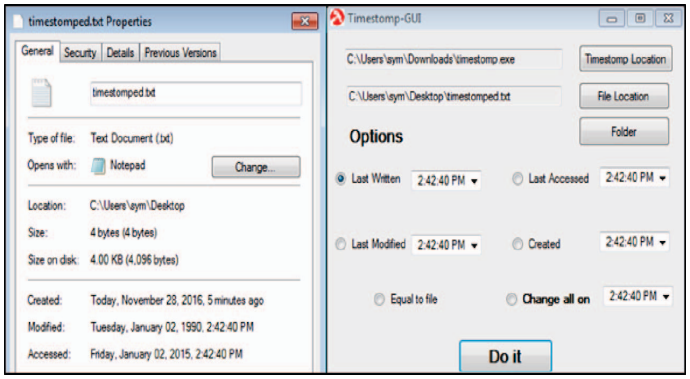

Figure 4. Manipulated MACE Times of a file.

system device drivers and ports for printers and serial communication. For example, when tried to create a folder or file named CON, it will give you an error message saying "The specified device name is invalid."

But there are ways providing use of these restricted folder and file names for attacker. Anyone can create or rename a folder or file with these names by opening a command prompt and typing "md \\.\c:\aux" which uses Universal Naming Convention (UNC) path (\\hostname\c$\folder). The second way is booting from a Linux supporting NTFS and move or rename the file or folder. A text file named secret.txt which has the evidence inside has been renamed as aux.txt using command line. When it is tried to open and see what file includes it will give an error message as shown in Figure 3.

This technique attempts to extend the time required for data analysis process. Forensics investigator can change the folder or file names and can see whether it is an evidence or not. It is not complicated but too many files or folders like that will take too much time to be analysed. So this will add man-hour to an investigation.

To mitigate against this technique, it is required not to export the files with their native file names. As an investigator always specify a different name for files exported. FTK 4 tool has a feature supporting this requirement like giving names 1.jpg, 2.jpg and etc. Exporting files with their File ID is another option.

F. Manipulating MACE Times

Masking or modifying forensics artefacts to mislead forensics investigator is one of the most used techniques in anti-forensics. Deletion or modification of MACE values can come under this technique. MACE attributes are the data included in a file that show the timestamps when a file is created, modified, accessed or an entry modified. In NTFS, timestamp information is kept under $STANDART_INFORMATION and $FILE_NAME attributes of a Master File Table entry. These timestamps could be very crucial to forensics investigator for providing evidence in terms of showing an activity occurred in a certain time. When considered in view of the amount of data obtained from a seized hardware, a forensics investigator can't examine every file in required detail. A common and very sensible analysis workflow is to narrow down the search to a particular timeframe-such as immediately before and after the data breach or other suspected incident occurred [26].

Timestomp is a utility co-authored by developers James C. Foster and Vincent Liu. The software's goal is to allow for the deletion or modification of timestamp-related information on files [27]. A file's modified or accessed times are usually equal or greater than created time but as seen in Figure 4, sometimes they are not. And using timestomp with a Graphical User Interface (GUI) does not require any expertise. Timestomp only changes the timestamps under $STANDART_INFORMATION attribute. It does not change the timestamps under $FILE_NAME attribute. If it is not known by user both attributes could be compared for the files suspected by using a tool like mftrcrd.exe in [28] for reading MFT entry data. The differences could be noticed easily between timestamps in Figure 5. But simply moving timestomped file to another location and running timestomp.exe again will make $STANDART_INFORMATION timestamps equal to $FILE_NAME timestamps. The Defiler's Toolkit can also overwrite inode (data structure in Unix file system) timestamps and deleted directory entries on many Unix systems; timestamps on allocated files could also be modified by using Unix touch command [9]. Moreover, SetMACE tool which has features like being advanced and hard to be detected in [29] could change timestamps under $STANDARD_INFORMATION, $FILE_NAME, $INDEX_ROOT and $INDEX_ALLOCATION attributes at once.

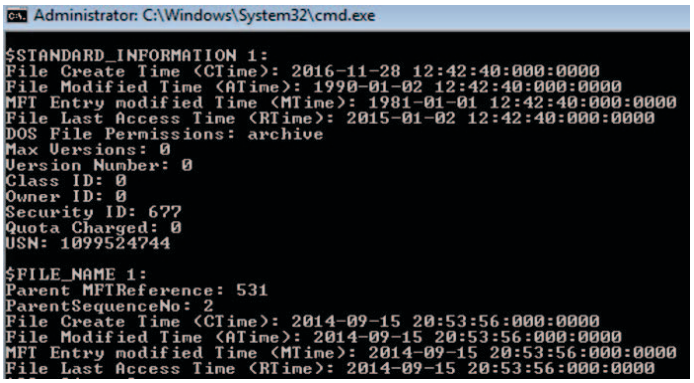

Figure 5. Comparing Timestamps Under Standard Info and File Name Attributes

The method of ignoring dates on metadata of files and looking the actual dates in files (if exist) instead is one of a mitigation step. If randomized BIOS time is the issue, looking log files of an application could give a hint about which event happened when, because logs are kept sequentially.

G. Loop References

There is a default file path length restriction because of Windows API which is 260 characters on NTFS. But there are ways of creating longer paths via using third party tools such as Long Path Tool [30]. The other way is using loop references with the help of using junctions or symbolic links which can point to a parent folder. This will create a recursive path like C:\Parent\Child\Parent\Child\Parent\Child…. and malicious users could store malicious data in those nested folders. When it is tried to open files or folder in this structure, it will give error message indicating that cannot resolve file name or file path is too long.

This attack aims at data analysis phase. DF tools can be affected by this attack and investigator could wait for a long time while exporting even small sized files. For mitigating this attack, examiner should work from an image and export file itself not the folders.

H. Hash Collisions

Hash functions are the algorithms used to create unique fixed string value to locate a file which can have any amount of data. On the contrary to encryption, hash algorithms are irreversible. In computer forensics it guarantees that digital evidence has not been changed during the investigation process [31]. [32] showed that same hash outputs could be created for two different input data. This probability can make digital evidence's credibility undermined. If a malicious executable file is only searched in black list which has hash values of known bad files, it is easy to change some characters in HexEdit which changes hash value of file. Thus it will not be detected as malicious. Adding dummy data to criminal files can change hash value which could match with one of a known good files. There are available tools for showing the weaknesses of some hash algorithms and probability of creating hash collisions like HashClash [33]. This technique aims at reporting findings phase.

In order to mitigate hash collisions, it is recommended to use hash algorithm which has fewer collisions such as Whirlpool, SHA 256 and not to search by hashes for locating files. If two files that have same hash value exist, hashing these two files sector by sector (for instance hashing per each 512 bytes) could show where difference occurs.

İ. Dummy HDDs

A personal computer's (PC) hard disk is not valuable in perspective of gathering evidence if it is not used for keeping data, information on it. Attackers could have a PC with a hard disk that is not used. A PC also could be used by booting from USB and hard disk could be ignored on daily based usage. This kind of usage intends to store data on cloud or a remote machine. In addition, attacker can use a service which automates random writes to hard disk to simulate that hard disk is being used regularly. As long as the hard disk has "Recent" entries, the investigator will think it's been used recently [19].

In order to mitigate this technique, an investigator is required to check seized hardware's USB slots to see if any USB drive connected or not. That USB drives are getting smaller could cause that an investigator could not notice them. Pagefile of the USB drive is needed to be checked carefully because this pagefile of USB drive could point to a network location. Eventually, if possible, before seizing hardware network traffic could be monitored to detect if any remote drive location exists [19].

The anti-forensics techniques and countermeasures described in this section are summarized and presented in Table 2.

IV. Conclusions

Throughout this study, what anti-forensics is and which techniques are included to extend the required time for a computer forensics investigation has been explained. While classical anti-forensics techniques intend to destroy data or making data impossible to be read, modern anti-forensics techniques intend to extend the time required for an investigation, obfuscate traces and complicate processes of a digital forensics. This kind of attacks could cause increase in cost of a forensics investigation or decrease in credibility of an evidence. As mentioned in modern anti-forensics techniques, in most of them, technical expertise is not required for using anti-forensics techniques. The advances in digital forensics and anti-forensic techniques will continue occurring.

The primary goal of this study is help to keep forensics experts' knowledge of AFTs current and "alive". The second goal is showing investigators and information security specialists where to check to see if any of these anti-forensics techniques used. Even the simplest and least complicated anti-forensics techniques can greatly complicate an investigation, therefore the investigators are required to have situational

TABLE II AFTS AND COUNTERMEASURES SUMMARY

AFTs	Countermeasures
Data Pooling	-parallelize the data acquisition, -use suspects' computers, -implement DF triage methods.
Non Standart RAID'ed Disks	-de-RAID on suspects' own system, - image volumes not the physical HDDs, -use RAID recovery tools.
Manipulating File Signatures	-using Fuzzy Hashing, -File Signature Analysis.
Restricted Filenames	-do not export files with native filenames, -Export files with File ID, etc.
Manipulating MACE Times	-Ignore dates, -Use actual dates in files (if exist).
Loop References	-work on image, -export files not folders.
Hash Collisions	-use secure hash algorithms, -do not search by hashes.
Dummy HDDs	-check USB slots, -monitor network traffic before seizuring hardware (if possible)

awareness about these techniques and be prepared to deal with them when they conduct a forensics investigation.

It is not easy to check every detail or possibility of anti-forensics usage in every investigation. The investigator will decide, if it is needed to search for anti-forensics or not, according to suspect's profile (technical or regular user etc.). Although anti-forensics techniques in the scope of this paper described one by one, a combinational use of these techniques would cause greater challenges in this field.

REFERENCES

[1] H. Jahankhani and E. Beqiri, Handbook of Electronic Security and Digital Forensics (Google eBook), vol. 2. 2010.

[2] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," Digit. Investig., vol. 18, no. December 2015, pp. S66–S75, 2016.

[3] I. Baggili, A. BaAbdallah, D. Al-Safi, and A. Marrington, "Research trends in digital forensic science: An empirical analysis of published research," Digit. Forensics Cyber Crime, pp. 144–157, 2012.

[4] S. Garfinkel, "Anti-Forensics : Techniques , Detection and Countermeasures," 2nd Int. Conf. Inf. Warf. Secur., pp. 77–84, 2007.

[5] B. Shirani, "Anti-forensics," High Technol. Crime Investig. Assoc., 2002.

[6] C. S. J. Peron and M. Legary, "Digital anti-forensics: emerging trends in data transformation techniques," Proc. 2005 E-Crime Comput. Evid. , 2005.

[7] M. Geiger, "Evaluating commercial counter-forensic tools," Proc. 5th Annu. Digit. Forensic …, pp. 1–12, 2005.

[8] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," Digit. Investig., vol. 3, no. SUPPL., pp. 44–49, 2006.

[9] Grugq, "The art of defiling: defeating forensic analysis.," Blackhat Brief., 2005.

[10] M.Rogers, "Anti-forensics: the coming wave in digital forensics.," 2006.

[11] A. Smith, "Describing and Categorizing Disk-Avoiding Anti-Forensics Tools," J. Digit. Forensic Pract., vol. 1, no. 4, pp. 309–313, 2007.

[12] B. Blunden, "Anti-Forensics : The Rootkit Connection," Commentary, pp. 1–44, 2009.

[13] D. K and M. B., "Toward understanding the challenges and countermeasures in computer anti-forensics.," Int. J. Cloud Appl. Comput., p. 14, 2011.

[14] A. Joshi and D. Bhilare, "Emerging trends and research in digital forensics," Oiirj.Org, no. I, pp. 293–304, 2014.

[15] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," Proc. 11th Annu. ADFSL Conf. Digit. Forensics, Secur. Law (CDFSL 2016), pp. 9–20, 2016.

[16] M. K. Rogers, "Anti-Forensics," in Presentation given to Lockheed Martin, 2005.

[17] V. Liu and F. Brown, "Bleeding-Edge Anti-Forensics," Present. InfoSec World, 2006.

[18] D. Franco, D. Fuschini, and T. Rodrigues, "How To Detect Anti-Forensic Techniques," eForensics, pp. 45–69, 2016.

[19] M. Perklin, "Anti-Forensics and Anti-Anti-Forensics," in DefCon, 2012.

[20] Moser, Andreas, and Michael I. Cohen. "Hunting in the enterprise: Forensic triage and incident response." Digital Investigation 10.2 (2013): 89-98.

[21] R. Kaur and A. Kaur, "Digital Forensics," Int. J. Comput. Appl. (0975 – 8887), vol. 50, no. 5, pp. 5–9, 2012.

[22] "RAID." [Online]. Available: https://en.wikipedia.org/wiki/RAID.

[23] R. Spishock, "Impact of Steganography on a Forensic Investigation," Stevenson Univ. Forensic J., pp. 30–35, 2013.

[24] G. Kessler, "File Signatures." [Online]. Available: http://www.garykessler.net/library/file_sigs.html.

[25] D. Hurlbut, "Fuzzy Hashing for Digital Forensic Investigators," no. January, pp. 1–9, 2009.

[26] "Identifying Anti-Forensics:Timestomping." [Online]. Available: https://www.nuix.com/2014/11/19/identifying-anti-forensics-timestomping.

[27] "Timestomp." [Online]. Available: http://www.forensicswiki.org/wiki/Timestomp.

[28] J. Schicht, "MFT Records Data." [Online]. Available: https://github.com/jschicht/MftRcrd.

[29] J. Schicht, "Set MACE." [Online]. Available: https://github.com/jschicht/SetMace.

[30] "Long Path Tool." [Online]. Available: http://longpathtool.com/.

[31] P. Pajek and E. Pimenidis, "Computer anti-forensics methods and their impact on computer forensic investigation," Commun. Comput. Inf. Sci., vol. 45, pp. 145–155, 2009.

[32] I. Mironov, "Hash functions : Theory, attacks, and applications Theory of hash functions," Microsoft Res. Silicon Val. Campus, pp. 1–22, 2005.

[33] M. Steven, "HashClash." [Online]. Available: https://marc-stevens.nl/p/hashclash/.