The Anti-Forensics Challenge

Kamal Dahbur
kdahbur@nyit.edu

Bassil Mohammad
bassil.mohammad@jo.ey.com

School of Engineering and Computing Sciences
New York Institute of Technology
Amman, Jordan

ABSTRACT
Computer and Network Forensics has emerged as a new field in IT that is aimed at acquiring and analyzing digital evidence for the purpose of solving cases that involve the use, or more accurately misuse, of computer systems. Many scientific techniques, procedures, and technological tools have been evolved and effectively applied in this field. On the opposite side, Anti-Forensics has recently surfaced as a field that aims at circumventing the efforts and objectives of the field of computer and network forensics. The purpose of this paper is to highlight the challenges introduced by Anti-Forensics, explore the various Anti-Forensics mechanisms, tools and techniques, provide a coherent classification for them, and discuss thoroughly their effectiveness. Moreover, this paper will highlight the challenges seen in implementing effective countermeasures against these techniques. Finally, a set of recommendations are presented with further seen research opportunities.

Categories and Subject Descriptors
K.6.1 [**Management of Computing and Information Systems**]: Projects and People Management – *System Analysis and Design, System Development.*

General Terms
Management, Security, Standardization.

Keywords
Computer Forensics (CF), Computer Anti-Forensics (CAF), Digital Evidence, Data Hiding.

1. INTRODUCTION

The use of technology is increasingly spreading covering various aspects of our daily lives. An equal increase, if not even more, is realized in the methods and techniques created with the intention to misuse the technologies serving varying objectives being political, personal or anything else. This has clearly been reflected in our terminology as well, where new terms like cyber warfare, cyber security, and cyber crime, amongst others, were introduced. It is also noticeable that such attacks are getting increasingly more sophisticated, and are utilizing novel methodologies and techniques. Fortunately, these attacks leave traces on the victim systems that, if successfully recovered and analyzed, might help identify the offenders and consequently resolve the case(s) justly and in accordance with applicable laws. For this purpose, new areas of research emerged addressing Network Forensics and Computer Forensics in order to define the foundation, practices and acceptable frameworks for scientifically acquiring and analyzing digital evidence in to be presented in support of filed cases. In response to Forensics efforts, Anti-Forensics tools and techniques were created with the main objective of frustrating forensics efforts, and taunting its credibility and reliability.

This paper attempts to provide a clear definition for Computer Anti-Forensics and consolidates various aspects of the topic. It also presents a clear listing of seen challenges and possible countermeasures that can be used. The lack of clear and comprehensive classification for existing techniques and technologies is highlighted and a consolidation of all current classifications is presented.

Please note that the scope of this paper is limited to Computer-Forensics. Even though it is a related field, Network-Forensics is not discussed in this paper and can be tackled in future work. Also, this paper is not intended to cover specific Anti-Forensics tools; however, several tools were mentioned to clarify the concepts.

After this brief introduction, the remainder of this paper is organized as follows: section 2 provides a description of the problem space, introduces computer forensics and computer anti-forensics, and provides an overview of the current issues concerning this field; section 3 provides an overview of related work with emphasis on Anti-Forensics goals and classifications; section 4 provides detailed discussion of Anti-Forensics challenges and recommendations; section 5 provides our conclusion, and suggested future work.

2. THE PROBLEM SPACE

Rapid changes and advances in technology are impacting every aspect of our lives because of our increased dependence on such systems to perform many of our daily tasks. The achievements in the area of computers technology in terms of increased capabilities of machines, high speeds communication channels, and reduced costs resulted in making it attainable by the public. The popularity of the Internet, and consequently the technology associated with it, has skyrocketed in the last decade (see Table 1 and Figure 1). Internet usage statistics for 2010 clearly show the huge increase in Internet users who may not necessary be computer experts or even technology savvy [1].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
ISWSA'11, April 18–20, 2011, Amman, Jordan.

Copyright 2011 ACM 978-1-4503-0474-0/04/2011…$10.00.

WORLD INTERNET USAGE AND POPULATION STATISTICS				
World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Growth 2000-2010
Africa	1,013,779,050	4,514,400	**110,931,700**	2357%
Asia	3,834,792,852	114,304,000	**825,094,396**	622%
Europe	813,319,511	105,096,093	**475,069,448**	352%
Middle East	212,336,924	3,284,800	**63,240,946**	1825%
North America	344,124,450	108,096,800	**266,224,500**	146%
Latin America/ Caribbean	592,556,972	18,068,919	**204,689,836**	1033%
Oceania/Australia	34,700,201	7,620,480	**21,263,990**	179%
WORLD TOTAL	**6,845,609,960**	**360,985,492**	**1,966,514,816**	**445%**

Table 1. World Internet Usage – 2010 *(Reproduced from [1]).*

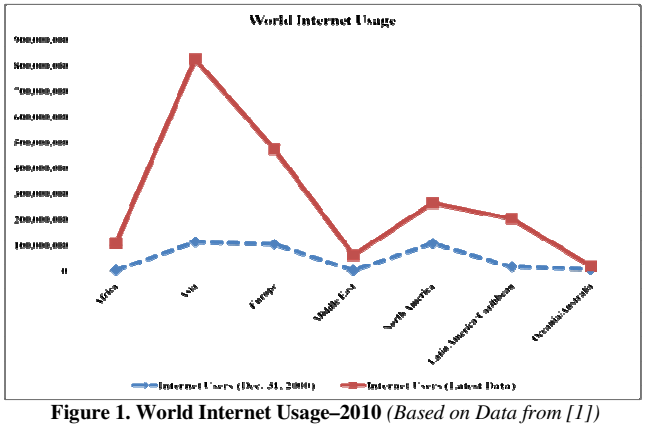

Figure 1. World Internet Usage–2010 *(Based on Data from [1])*

Unfortunately, some of the technology users will not use it in a legitimate manner; instead, some users may deliberately misuse it. Such misuse can result in many harmful consequences including, but not limited to, major damage to others systems or prevention of service for legitimate users. Regardless of the objectives that such "bad guys" might be aiming for from such misuse (e.g. personal, financial, political or religious purposes), one common goal for such users is the need to avoid detection (i.e. source determination). Therefore, these offenders will exert thought and effort to cover their tracks to avoid any liabilities or accountability for their damaging actions. Illegal actions (or crimes) that involve a computing system, either as a mean to carry out the attack or as a target, are referred to as Cybercrimes [2]. Computer crime or Cybercrime are two terms that are being used interchangeably to refer to the same thing. A Distributed Denial of Service attack (DDoS) is a good example for a computer crime where the computing system is used as a mean as well as a target. Fortunately, cybercrimes leave fingerprints that investigators can collect, correlate and analyze to understand what, why, when and how a crime was committed; and consequently, and most importantly, build a good case that can bring the criminals to justice. In this sense, computers can be seen as great source of evidence. For this purpose Computer Forensics (CF) emerged as a major area of interest, research and development driven by the legislative needs of having scientific reliable framework, practices, guidelines, and techniques for forensics activities starting from evidence acquisition, preservation, analysis, and finally presentation. Computer Forensics can be defined as the process of scientifically obtaining, examining and analyzing digital information so that it can be used as evidence in civil, criminal or administrative cases [2]. A more formal definition of Computer Forensics is "the discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law" [3].

To hinder the efforts of Computer Forensics, criminals work doggedly to instigate, develop and promote counter techniques and methodologies, or what is commonly referred to as Anti-Forensics. If we adopt the definition of Computer Forensics (CF) as scientifically obtaining, examining, and analysing digital information to be used as evidence in a court of law, then Anti-Forensics can be defined similarly but in the opposite direction. In Computer Anti-Forensics (CAF) scientific methods are used to simply frustrate Forensics efforts at all forensics stages. This includes preventing, impeding, and/or corrupting the acquiring of the needed evidence, its examination, its analysis, or its credibility. In other words, whatever necessary to ensure that computer evidence cannot get to, or will not be admissible in, a court of law.

The use of Computer Anti-Forensics tools and techniques is evident and far away from being an illusion. So, criminals' reliance on technology to cover their tracks is not a claim, as clearly reflected in recent researches conducted on reported and investigated incidents. Based on 2009-2010 Data Breach Investigations Reports [4][5], investigators found signs of anti-forensics usage in over one third of cases in 2009 and 2010 with the most common forms being the same for both years. The results show that the overall use of anti-forensics remained relatively flat with slight movement among the techniques themselves. Figure [2] below shows the types of anti-Forensic techniques used (data wiping, data hiding and data corruption) by percentage of breaches. As shown in Figure [2] below, data wiping is still the most common, because it is supported by many commercial off-the-shelf products that are available even as freeware that are easy to install, learn and use; while data hiding and data corruption remain a distant behind.

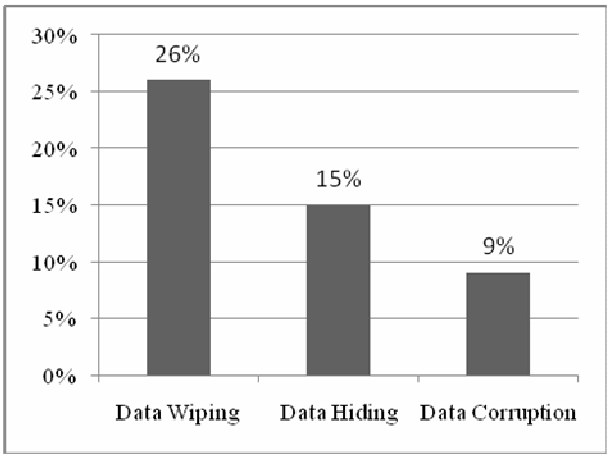

Figure 2 Types of Anti-Forensics – 2010 *(Reproduced from [5])*

It is important to note that the lack of understanding on what CAF is and what it is capable of may lead to underestimating or probably overlooking CAF impact on the legitimate efforts of CF. Therefore, when dealing with computer forensics, it is important that we address the following questions, among others, that are related to CAF: Do we really have everything? Are the collected evidences really what were left behind or they are only just those intentionally left for us to find? How to know if the CF tool used was not misleading us due to certain weaknesses in the tool itself? Are these CF tools developed according to proper secure software engineering methodologies? Are these CF tools immune against attacks? What are the recent CAF methods and techniques? This paper attempts to provide some answers to such questions that can assist in developing the proper understanding for the issue.

3. RELATED WORK, CAF GOALS AND CLASSIFICATIONS

Even though computer forensics and computer ant-forensics are tightly related, as if they are two faces of the same coin, the amount of research they received was not the same. CF received more focus over the past ten years or so because of its relation with other areas like data recovery, incident management and information systems risk assessment. CF is a little bit older, and therefore more mature than CAF. It has consistent definition, well defined systematic approach and complete set of leading best practices and technology.

CAF on the other side, is still a new field, and is expected to get mature overtime and become closer to CF. In this effort, recent research papers attempted to introduce several definitions, various classifications and suggest some solutions and countermeasures. Some researchers have concentrated more on the technical aspects of CF and CAF software in terms of vulnerabilities and coding techniques, while others have focused primarily on understanding file systems, hardware capabilities, and operating systems. A few other researchers chose to address the issue from an ethical or social angle, such as privacy concerns. Despite the criticality of CAF, it is hard to find a comprehensive research that addresses the subject in a holistic manner by providing a consistent definition, structured taxonomies, and an inclusive view of CAF.

3.1. CAF Goals

As stated in the previous section, CAF is a collection of tools and techniques that are intended to frustrate CF tools and CF's investigators efforts. This field is growingly receiving more interest and attention as it continues to expose the limitations of currently available computer forensics techniques as well as challenge the presumed reliability of common CF tools. We believe, along with other researchers, that the advancements in the CAF field will eventually put the necessary pressure on CF developers and vendors to be more proactive in identifying possible vulnerabilities or weaknesses in their products, which consequently should lead to enhanced and more reliable tools.

CAF can have a broad range of goals including: avoiding detection of event(s), disrupting the collection of information, increasing the time an examiner needs to spend on a case, casting doubt on a forensic report or testimony. In addition, these goals may also include: forcing the forensic tool to reveal its presence, using the forensic tool to attack the organization in which it is running, and leaving no evidence that an anti-forensic tool has been run [6].

3.2. CAF Classifications

Several classifications for CAF have been introduced in the literature. These various taxonomies differ in the criteria used to do the classification. The following are the most common approaches used:

1. **Categories Based on the Attacked Target**
   - Attacking Data: The acquisition of evidentiary data in the forensics process is a primary goal. In this category CAFs seek to complicate this step by wiping, hiding or corrupting evidentiary data.
   - Attacking CF Tools: The major focus of this category is the examination step of the forensics process. The objective of this category is to make the examination results questionable, not trustworthy, and/or misleading by manipulating essential information like hashes and timestamps.
   - Attacking the Investigator: This category is aimed at exhausting the investigator's time and resources, leading eventually to the termination of the investigation.
2. **CAF Techniques vs. Tactics**

   This categorization makes a clear distinction between the terms anti-forensics and counter-forensics [7], even though the two terms have been used interchangeably by many others as the emphasis is usually on technology rather than on tactics.
   - Counter-Forensics: This category includes all techniques that target the forensics tools directly to cause them to crash, erase collected evidence, and/or break completely (thus disallowing the investigator from using it). Compression bombs are good example on this category.
   - Anti-Forensics: This category includes all technology related techniques including encryption, steganography, and alternate data streams (ADMs).
3. **Traditional vs. Non-Traditional**
   - Traditional Techniques: This category includes techniques involving overwriting data, Cryptography, Steganography, and other data hiding approaches beside generic data hiding techniques.
   - Non-Traditional Techniques: As opposed to traditional techniques, these techniques are more creative and impose more risk as they are harder to detect. These include:
     - *Memory injections*, where all malicious activities are done on the volatile memory area.
     - *Anonymous storage*, utilizes available web-based storage to hide data to avoid being found on local machines.
     - *Exploitation of CF software bugs*, including Denial of Service (DoS) and Crashers, amongst others.
4. **Categories Based on Functionality**

This categorization includes data hiding, data wiping and obfuscation. Attacks against CF processes and tools is considered a separate category based on this scheme

4. CAF CHALLENGES

Because Computer Anti-Forensics (CAF) is a relatively new discipline, the field faces many challenges that need considered and addressed. In this section, we have attempted to identify the most pressing challenges surrounding this area, highlight the research needed to address such challenges, and attempt to provide perceptive answers to some the concerns.

4.1. Ambiguity

Aside from having no industry-accepted definition for CAF, studies in this area view anti-forensics differently; this leads to not having a clear set of standards or frameworks for this critical area. Consequently, misunderstanding may be an unavoidable end result that could lead to improperly addressing the associated concerns. The current classification schemes, stated above, which mostly reflect the author's viewpoint and probably background, confirm as well as contribute to the ambiguity in this field. A classification can only be beneficial if it must has clear criteria that can assist not only in categorizing the current known techniques and methodologies but will also enable proper understanding and categorization of new ones. The attempt to distinguish between the two terms, anti-forensics and counter-forensics based on technology and tactics is a good initiative but yet requires more elaboration to avoid any unnecessary confusions.

To address the definition issue, we suggest to adopt a definition for CAF that is built from our clear understanding of CF. The classification issue can be addressed by narrowing the gaps amongst the different viewpoints in the current classifications and excluding the odd ones.

4.2. Investigation Constraints

A CF investigation has three main constraints/challenges, namely: time, cost and resources. Every CF investigation case should be approached as separate project that requires proper planning, scoping, budgeting and resources. If these elements are not properly accounted for, the investigation will eventually fail, with most efforts up to the point of failure being wasted. In this regard, CAF techniques and methodologies attempt to attack the time, cost and resources constraints of an investigation project. An investigator may not able to afford the additional costs or allocate the additional necessary resources. Most importantly, the time factor might play a critical role in the investigation as evidentiary data might lose value with time, and/or allow the suspect(s) the opportunity to cover their tracks or escape. Most, if not all, CAF techniques and methodologies (including data wiping, data hiding, and data corruption) attempt to exploit this weakness. Therefore, it proper project management is imperative before and during every CF investigation.

4.3. Integration of Anti-Forensics into Other Attacks

Recent researches show an increased adoption of CAF techniques into other typical attacks. The primary purposes of integrating CAF into other attacks are undetectability and deletion of evidence. Two major areas for this threatening integration are Malware and Botnets [8][9]. Malwares and Botnets when armed with these techniques will make the investigative efforts labour and time intensive which can lead to overlooking critical evidence, if not abandoning the entire investigation.

4.4. Breaking the Forensics Software

CF tools are, of course, created by humans, just like other software systems. Rushing to release their products to the market before their competition, companies tend to, unintentionally, introduce vulnerabilities into their products. In such cases, software development best practices, which are intended to ensure the quality of the product, might be overlooked leading to the end product being exposed to many known vulnerabilities, such as buffer overflow and code injection. Because CF software is ultimately used to present evidence in courts, the existence of such weaknesses is not tolerable. Hence, all CF software, before being used, must be subjected to thorough security testing that focuses on robustness against data hiding and accurate reproduction of evidence.

The Common Vulnerabilities and Exposures (CVE) database is a great source for getting updates on vulnerabilities in existing products [10]. Some studies have reported several weaknesses that may result in crashes during runtime leaving no chance for interpreting the evidence [11]. Regardless of the fact that some of these weaknesses are still being disputed [12], it is important to be aware that these CF tools are not immune to vulnerabilities, and that CAF tools would most likely take advantage of such weaknesses. A good example of a common technique that can cause a CF to fail or crash is the "Compression Bomb"; where files are compressed hundreds of times such that when a CF tool tries to decompress, it will use up so many resources causing the computer or the tool to hang or crash.

4.5. Privacy Concerns

Increasingly, users are becoming more aware of the fact that just deleting a file does not make it really disappear from the computer and that it can be retrieved by several means. This awareness is driving the market for software solutions that provide safe and secure means for files deletion. Such tools are marketed as "privacy protection" software and claim to have the ability to completely remove all traces of information concerning user's activity on a system, websites, images and downloaded files. Some of these tools do not only provide protection through secure deletion; but also offer encryption and compression. Moreover, these tools are easy use, and some can even be downloaded for free. WinZip is a popular tool that offers encryption, password protection, and compression. Such tools will most definitely complicate the search for and acquiring of evidence in any CF investigation because they make the whole process more time and resources consuming.

Privacy issues in relation to CF have been the subject of detailed research in an attempt to define appropriate policies and

procedures that would maintain users' privacy when excessive data is acquired for forensics purposes [13].

4.6. Nature of Digital Evidence

CF investigations rely on two main assumptions to be successful: (1) the data can be acquired and used as evidence, and (2) the results of the CF tools are authentic, reliable, and believable. The first assumption highlights the importance of digital evidence as the basis for any CF investigation; while the second assumption highlights the critical role of the trustworthiness of the CF tools in order for the results to stand solid in courts.

Digital evidence is more challenging than physical evidence because of its more susceptible to being altered, hidden, removed, or simply made unreadable. Several techniques can be utilized to achieve such undesirable objectives that can complicate the acquisition process of evidentiary digital data, and thus compromise the first assumption.

CF tools rely on many techniques that can attest to their trustworthiness, including but limited to: hashing; timestamps; and signatures during examination, analyses and inspection of source files. CAF tools can in turn utilize new advances in technology to break such authentication measures, and thus comprise the second assumption..

The following is a brief explanation of some of the techniques that are used to compromise these two assumptions:

- ***Encryption*** is used to make the data unreadable. This is one of the most challenging techniques, as advances in encryption algorithms and tools empowered it to be applied on entire hard drive, selected partitions, or specific directories and files. In all cases, an encryption key is usually needed to reverse the process and decrypt the desired data, which is usually unknown to an investigator, in most cases. To complicate matters, decryption using brute-force techniques becomes infeasible when long keys are used. More success in this regard might be achieved with keyloggers or volatile memory content acquisition.
- ***Steganography*** aims at hiding the data, by embedding it into another digital form, such as images or videos. Commercial Steganalysis tools, that can detect hidden data, exist and can be utilized to counter Steganography. Encryption and Steganography can be combined to obscure data and make it also unreadable, which can extremely complicate a CF investigation.
- ***Secure-Deletion*** removes the target data completely from the source system, by overwriting it with random data, and thus rendering the target data unrecoverable. Fortunately, most of the available commercial secure-deletion tools tend to underperform and thus miss some data [14]. More research is needed in this area to understand the weaknesses and identify the signatures of such tools. Such information is needed to detect the operations and minimize the impact of these tools.
- ***Hashing*** is used by CF tools to validate the integrity of data. A hashing algorithm accepts a variable-size input, such as a file, and generates a unique fixed-size value that corresponds to the given input. The generated output is unique and can be used as a fingerprint for the input file. Any change in the original file, no matter how minor, will result in considerable change in the hash value produced by the hashing algorithm. A key feature in hashing algorithms is "Irreversibility" where having the hash value in hand will not allow the recovery of the original input. Another key feature is "Uniqueness" which basically means that the hash values of two files will be equal if and only if the files are absolutely identical. Many hashing algorithms have developed, and some have been already infiltrated or cracked. Other algorithms like MD5, MD6, Secure Hashing Algorithms (SHA), SHA-1, SHA-2, amongst others, are harder to break. However, all are vulnerable to being infiltrated as technology and research advance [15]. Research is also necessary in the other direction to enhance the capabilities of CF tools in this regard and maintain their credibility.
- ***Timestamps*** are associated with files and are critical for the task of establishing the chain of events during a CF investigation. The time line for the events is contingent on the accuracy of timestamps. CAF tools have provided the capability to modify timestamps of files or logs, which can mislead an investigation and consequently coerce the conclusion. Many tools currently exist on the market, some are even freely available, that make it easy to manipulate the timestamps, such as Timestamp Modifier and SKTimeStamp [16].
- ***File Signatures***, also known as Magic Numbers, are constant known values that exist at the beginning of each file to identify the file type (e.g. image file, word document, etc.). Hexadecimal editors, such as WinHex, can be used to view and inspect these values. Forensics investigators rely on these values to search for evidence of certain type. When a file extension is changed, the actual type file is not changed, and thus the file signature remains unchanged. ACF tools intentionally change the file signatures in their attempt to mislead the investigations as some evidence files are overlooked or dismissed. Complete listing of file signatures or magic numbers can be found on the web in [17].
- ***CF Detection*** is simply the capability of ACF tools to detect the presences of CF software and their activities or functionalities. Self-Monitoring, Analysis and Reporting Technology (SMART) built into most hard drives reports the total number of power cycles (Power_Cycle_Count), the total time that a hard drive has been in use (Power_On_Hours or Power_On_Minutes), a log of high temperatures that the drive has reached, and other manufacturer-determined attributes. These counters can be reliably read by user programs and cannot be reset. Although the SMART specification implements a DISABLE command (SMART 96), experimentation indicates that the few drives that actually implement the DISABLE command continue to keep track of the time-in-use and power cycle count and make this information available after the next power cycle. CAF tools can read SMART counters to detect attempts at forensic analysis and alter their behavior accordingly. For example, a dramatic

increase in Power_On_Minutes might indicate that the computer's hard drive has been imaged [18].

- ***Business Needs: Cloud Computing*** (CC) is a business model typically suited for small and medium enterprises (SME) that do not have enough resources to invest in building their own IT infrastructure. Hence, they tend to outsource this to third parties who will in turn lease their infrastructure and probably applications as services. This new model introduces more challenges to CF investigations due to mainly the fact that the data is on the cloud (i.e. hosted somewhere in the Internet space), being transferred across countries with different regulations, and most importantly might reside on a machine that hosts other data instances of other enterprises. In some instances, the data for the same enterprise might even be stored across multiple data centres [19][20]. These issues complicate the CF's primary functions (i.e. data acquisition, examination, and analyses) needed to build a good case extremely hard.

4.7 Recommendations

Based on our findings, we see room for improvement in the field of ACF that can address some of the issues surrounding this field. We believe that such recommendations, when adopted and/or implemented properly, can add value and consolidate the efforts for advancing this field. Below is a list and brief explanation of the recommendations:

a) Spend More Efforts to Understand ACF

More efforts should be spent in order to reach an agreed upon comprehensive definition for ACF that would assist in getting better understanding of the concepts in the field. These efforts should also extend to develop acceptable best practices, procedures and processes that constitute the proper framework, or standard, that professionals can use and build onto. ACF classifications also need to be integrated, clarified, and formulated on well-defined criteria. Such fundamental foundational efforts would eventually assist researchers and experts in addressing the issues and mitigating the associated risks.

Awareness of AFC techniques and their capabilities will prevent, or at least reduce, their success and consequently their impact on CF investigations. Knowledge in this area should encompass both techniques and tactics. Continued education and research are necessary to stay atop of latest developments in the field, and be ready with appropriate countermeasures when and as necessary.

b) Define Laws that Prohibit Unjustified Use of ACF

Existence of strict and clear laws that detail the obligations and consequences of violations can play a key deterrent role for the use of these tools in a destructive manner. When someone knows in advance that having certain ACF tools on one's machine might be questioned and possibly pose some liabilities, one would probably have second thoughts about installing such tools.

Commercial non-specialized ACF tools, which are more commonly used, always leave easily detectable fingerprints and signatures. They sometimes also fail to fulfil their developers' promises of deleting all traces of data. This can later be used as evidence against a suspected criminal and can lead to an indictment. The proven unjustified use of ACF tools can be used as supporting incriminatory evidence in courts in some countries [21].

To address the privacy concerns, such as users needs to protect personal data like family pictures or videos, an approved list of authorized software can be compiled with known fingerprints, signatures and special recovery keys. Such information, especially recovery keys, would then be safe-guarded in possession of the proper authorities. It would strictly be used to reverse the process of AFC tools, through the appropriate judicial processes.

c) Utilize Weaknesses of ACF Software

In some cases, digital evidence can still be recovered if a data wiping tool is poorly used or is functioning improperly. Hence, each AFC software must be carefully examined and continuously analyzed in order to fully understand its exact behaviour and determine its weaknesses and vulnerabilities [14][22]. This can help to develop the appropriate course of actions given the different possible scenarios and circumstances. This could prove to be valuable in saving time and resources during an investigation.

d) Harden CF Software

CAF and CF thrive on the weaknesses of each other. To ensure justice CF must always strive to be more advanced than its counterpart. This can be achieved by conducting security and penetration tests to verify the software is immune to external attacks. Also, it is imperative not to submit to market pressure and demand for tools by rapidly releasing products without proper validation. The best practices of software development must not be overlooked at any rate. When vulnerabilities are identified, proper fixes and patches must be tested, verified and deployed promptly in order to avoid zero-day attacks.

5. CONCLUSION AND FUTURE WORK

5.1. Conclusion

Computer Anti-Forensics (CAF) is an important developing area of technology. Because CAF success means that digital evidence will not be admissible in courts, Computer Forensics (CF) must evaluate its techniques and tactics very carefully. Also, CF efforts must be integrated and expedited to narrow the current exiting gap with CAF. It is important to agree on an acceptable definition and classification for CAF which will assist in implementing proper countermeasures. Current definitions and classifications all seem to concentrate on specific aspects of CAF without truly providing the needed holistic view.

It is very important to realize that CAF is not only about tools that are used to delete, corrupt, or hide evidence. CAF is a blend of techniques and tactics that utilize technological advancements in areas like encryption and data overwriting amongst other techniques to obstruct investigators' efforts.

Many challenges exist and need to be carefully analyzed and addressed. In this paper we attempted to identify some of these

challenges and suggested some recommendations that might, if applied properly, mitigate the risks.

5.2. Future Work

This paper provides solid foundation for future work that can further elaborate on the various highlighted areas. It suggests a definition for CAF that is closely aligned with CF and presents several classifications that we deem acceptable. It also discusses several challenges that can be further addressed in future research. CAF technologies, techniques, and tactics need to receive more attention in research, especially in the areas that present debates on hashes, timestamps, and file signatures.

Research opportunities in Computer Forensics, Network Forensics, and Anti-Forensics can use the work presented in this paper as a base. Privacy concerns and other issues related to the forensics field introduce a raw domain that requires serious consideration and analysis. Cloud computing, virtualization, and related laws and regulations concerns are topics that can be considered in future research.

6. REFERENCES

[1] Corey Thuen, University of Idaho: "*Understanding Counter-Forensics to Ensure a Successful Investigation*". DOI=http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.138.2196

[2] Internet Usage Statistics, "*The Internet Big Picture, World Internet Users and Population Stats*". DOI= http://www.internetworldstats.com/stats.htm

[3] Bill Nelson, Amelia Phillips, and Steuart, "*Guide to Computer Forensics and Investigations*", pp 2-3, 4th Edition.

[4] US-Computer Emergency Readiness Team, CERT, a government organization, "*Computer Forensics*", 2008.

[5] Verizon Business, "*2009 Data Breach Investigations Report*". A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service. DOI=http://www.verizonbusiness.com/about/news/podcasts/1008a1a3-111=129947--Verizon+Business+2009+Data+Breach+Investigations+Report.xml

[6] Verizon Business, "*2010 Data Breach Investigations Report*". A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service. DOI=http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf?&src=/worldwide/resources/index.xml&id=

[7] Simson Garfinkel, "*Anti-Forensics: Techniques, Detection and Countermeasures*", 2nd International Conference in i-Warefare and Security, pp 77, 2007

[8] W.Matthew Hartley, "*Current and Future Threats to Digital Forensics*", ISSA Journal, August 2007

[9] Murray Brand, (2007), "*Forensics Analysis Avoidance Techniques of Malware*", Edith Cowan University, Australia.

[10] "*Security 101: Botnets*". DOI= http://www.secureworks.com/research/newsletter/2008/05/

[11] *Common Vulnerabilities and Exposures (CVE) database*, http://cve.mitre.org/

[12] Tim Newsham, Chris Palmer, Alex Stamos, "*Breaking Forensics Software: Weaknesses in Critical Evidence Collection*", iSEC Partners http://www.isecpartners.com, 2007

[13] Guidance Software: Computer Forensics Solutions and Digital Investigations (http://www.guidancesoftware.com/)

[14] S. Srinivasan, "*Security and Privacy vs. Computer Forensics Capabilities*", ISACA Online Journal, 2007

[15] Matthew Geiger, Carnegie Mellon University, "*Evaluating Commercial Counter-Forensic Tools*", Digital Forensic Research Workshop (DFRWS), 2005

[16] Xiaoyun Wang and Hongbo Yu, Shandong University, China, "*How to Break MD5 and Other Hash Functions*", EUROCRYPT 2005, pp.19-35, May, 2005

[17] *How to Change TimeStamp of a File in Windows*. DOI= http://www.trickyways.com/2009/08/how-to-change-timestamp-of-a-file-in-windows-file-created-modified-and-accessed/.

[18] *File Signature Table*. DOI= http://www.garykessler.net/library/file_sigs.html,

[19] McLeod S, "*SMART Anti-Forensics*", DOI= http://www.forensicfocus.com/smart-anti-forensics, .

[20] Stephen Biggs and Stilianos, "*Cloud Computing Storms*", International Journal of Intelligent Computing Research (IJICR), Volume 1, Issue 1, MAR, 2010

[21] U Gurav, R Shaikh, "*Virtualization – A key feature of cloud computing*", International Conference and Workshop on Emerging Trends in technology (ICWET 2010), Mumbai, India

[22] *U.S .v .Robert Johnson - Child Pornography Indictment*. DOI=http://news.findlaw.com/hdocs/docs/chldprn/usjhsn62805ind.pdf

[23] *United States of America v. H. Marc Watzman*. DOI= http://www.justice.gov/usao/iln/.../2003/watzman.pdf

[24] Mark Whitteker, "*Anti-Forensics: Breaking the Forensics Process*", ISSA Journal, November, 2008

[25] Gary C. Kessler,"*Anti-Forensics and the Digital Investigator*", Champlain College, USA

[26] Ryan Harris, "*Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem*", DOI= www.elsevier.com/locate/dinn.

Appendix A: Anti-Forensics Tools

The following is a list of some commercial CAF software packages available on the market. The tools listed below are intended as examples; none of these tools were purchased or tested as part of this paper work.

Category	Tool Name
Privacy and Secure Deletion	Privacy Expert; SecureClean; PrivacyProtection; Evidence Eliminator; Internet Cleaner
File and Disk Encryption	TruCrypt, PointSec; Winzip 14
Time stamp Modifiers	SKTimeStamp; Timestamp Modifier; Timestomp
Others	The Defiler's Toolkit – Necrofile and Klimafile; Metasploit Anti-Forensic Investigation Arsenal (known affectionately as MAFIA)