Three Anti-Forensics Techniques that pose the Greatest Risks to Digital Forensic Investigations

Nicholas Nicolaou
Lancaster University

Nicholas Nicolaou

Three Anti-Forensic Techniques that provide the Greatest Risks to Digital Forensic Investigations.

1.0 Introduction

Many digital forensics investigations use straightforward acquisition and analysis techniques which can enable evidence to be found with ease by the investigator. Even so, cases are gradually becoming more complex as suspected adversaries are using sophisticated anti-forensics techniques to halt investigations. When used by sophisticated adversaries, anti-forensics techniques can allow them to successfully conduct cyber-crime activities whilst retaining anonymity and privacy; such techniques are becoming a prevalent issue for investigators as they can be deployed with ease, for example, full disk encryption.

Digital forensics tools allow investigators to gain knowledge about the user of a particular device, tools can allow investigators to recover deleted files, investigate for adversaries, and assemble users' activities. Anti-forensics tools can damage the integrity of the investigation by deleting or modifying information, obfuscating network information, or by planting fake information to implicate a third-party.

This essay categorises traditional and modern anti-forensic techniques, then showcases the three chosen anti-forensic techniques that provide the greatest risks to digital forensic investigations. It discusses approaches for conducting anti-forensic activities; this includes, using polymorphic code for obfuscation of malware, utilising a global network of relays for browser anonymity, and hiding information with encryption. The essay then gauges the effectiveness of these techniques for anti-forensics, presents possible methods of detection and countermeasures, provides additional advice to tackle the current threat, and gives insight to the upcoming threats based on the current threat landscape.

2.0 Background

Digital forensics is a field that utilises scientific practices to collect, analyse, and present evidence to courts. Digital forensics tools support forensic examiners by gathering key data from devices; data capturing tools create a forensically sound bit-by-bit copy of systems to be processed lawfully, this is also to later analyse information that may not be initially noticeable. Digital forensics tools are classified based on its method of acquisition:

- Persistent data tools analyse stored data, and this data remains when a device is turned off. An example of a persistent data tool is "Sleuth Kit" (Brian Carrier, 2020).
- Volatile data tools analyse data that is transitory, this data does not remain after a device is turned off; this can include a device's Random Access Memory (RAM) or the flow of network packets between a network. An example of a volatile data tool is "Volatility" (Volatility Foundation, 2018).

Anti-forensics is an evolving set of tools and techniques that disturb forensic investigations. Liu and Brown (2006) have identified primary and secondary uses for anti-forensics:

Primary

- Avoiding detection of a particular event.
- Interfering with the collection of information.
- Wasting the time of the examiner.
- Increasing uncertainty to a forensic report or testimony.

Secondary

- Making a forensic tool be known to the adversary.
- Subverting a forensic tool to use against a system.
- Attacking the forensic examiner directly, forcing them to disconnect from the system.
- Erasing evidence of malicious activity on a system.

Due to the growing interest in anti-forensics tools and techniques, researchers have created and published tools online (Liu and Brown, 2006). It is argued that the published anti-forensics tools validate the restrictions of digital forensics tools (Buskirk and Liu. 2006). This challenges the notion that digital forensics tools are reliable for acquiring evidence lawfully. However, it is argued by Liu and Brown (2006) that the anti-forensics techniques published by researchers will help to establish improvements in the existing tools and processes; this is because it increases the pressure to make improvements by identifying vulnerabilities, not creating them. Yet it is agreeable that the vulnerabilities need to be published by researchers, there is an element of due care that needs to be considered as attackers may take advantage of the information by developing advanced anti-forensics tools before the current forensics tools are patched. Vulnerabilities should be published to the relevant organisations/communities before they are made accessible to anyone on the internet.

To further argue, current techniques have shifted a change between the primary and secondary uses of anti-forensics. For example, there is a growing increase in anti-forensic techniques being incorporated within cyber-attacks and the source code of malware. A cyber-criminal group named “Lazarus Group” successfully infiltrated a Bangladeshi Bank and gained access to the SWIFT network to transfer $850 million; after the attack, the team utilised a secure delete function to overwrite files with data from the heap memory. This anti-forensic technique is used to securely delete traces of malicious activity beyond recovery (Shields, 2018). In another case, the SamSam ransomware automates the anti-forensic process by securely erasing its malicious files and payloads to ensure the investigation of the attack is more complex (MITRE ATT&CK, 2016). Even though the anti-forensic technique of overwriting data is traditional, it has gained popularity due to its use in malware and network breaches.

As adversaries are commonly removing files throughout an intrusion to hinder forensic investigations, this shows that the threat landscape has changed since Liu and Brown’s study in 2006; therefore, the erasure of malicious activity should be changed to a primary use of anti-forensics, rather than a secondary one. Furthermore, some of the uses such as “Interfering with the collection of information” and “Avoiding detection of a particular event” is very broad and does not provide many characteristic traits to classify the main uses of anti-forensics. To improve, the main characteristics of anti-forensic activities need to be mapped, then sorted based on their prevalence in attacks. MITRE ATT&CK (2020) has begun documenting the characteristics of cyber-attacks to identify threat actors, but the organisation does not differentiate this with anti-forensic activities, nor do they indicate its prevalence of use. Therefore, statistical research needs to be conducted between knowledge bases to truly elicit the main characteristics of anti-forensics for the current threat landscape.

3.0 Traditional Anti Forensic Techniques

Traditional anti-forensics tools and techniques are still used today in many cyber-attacks (Garfinkel, 2007; Breitinger et al., 2016); however, the traditional techniques have advanced to be more effective (Hausknecht and Gruičić, 2017; InfoSec Institute, 2019). This section showcases anti-forensic techniques that have been prevalent since the early 1990s, this demonstrates the evolution of traditional techniques of anti-forensics, into the greatest risks to digital forensic investigations.

2.1 Overwriting Data and Metadata

There are many tools available that allow users to overwrite data and metadata to ensure that it is impossible to restore. To securely remove the data, programs typically use three settings:

1. Overwrite the entire storage device.
2. Overwrite selected files.
3. Overwrite 'deleted' files.

Tools will overwrite data a specified number of times to ensure that it has been deleted securely. For example, Apple's Disk Utility specifies 7-35 passes of NULL bytes, whereas Microsoft's cipher.exe uses 3 passes; a pass with zeros, a pass with FFs, and a pass with random data, this is compliant with the United States Department of Defence (DoD) standard (Department of Defense, 2006). However, Gutmann (1996) proclaimed it is possible to recover data that is not overwritten with 35+ passes. As time went by, this was further investigated by security researchers and it was found that data only needs 1-3 passes to be securely deleted (Gargean, 2019).

Determining which data to overwrite is challenging for users who do not wish to overwrite their entire drive. Defining which data to overwrite can be difficult as it is highly dependant on the activities that were conducted that the user is trying to obfuscate; therefore, it requires computer forensic skills to be confident in the secure deletion of data and metadata. To reinforce, Geiger (2005) assessed secure deletion programs and discovered that most of them did not successfully remove the required data, programs kept evidence such as prefetch data on computer systems exposing user activity.

Be that as is may, the concept of overwriting data and metadata to remove evidence has been successful for cyber-criminals when correctly implemented in their attack mechanisms. Therefore, it is far more effective to overwrite data when the process is manually implemented within cyber-attacks, rather than using automated computer programs.

"TimeStomp" is an example of a tool used to overwrite metadata (Offensive Security, 2019). Timestomp edits the timestamps of files by editing the "Created", "Last Accessed", and "Last Modified" timestamps of files. This disrupts the investigation by eluding forensic analysis; it is a common procedure for investigators to sort timestamps in chronological order to determine the flow of events that lead to an attack. However, by using TimeStomp it disrupts the flow of events. TimeStomp must be used meticulously to hoax the investigator; if the timestamps appear to be false, this indicates to the investigator that an attacker has technical skills, thereby creating an attack profile.

2.2 Least-Significant-Bit (LSB) Steganography

Steganography is the process of hiding data, the process can utilise security measures such as authentication; more specifically, steganography embeds data into computer images, these are referred to as "cover images" that usually do not cause attention to unsuspecting users. The process of hiding data with steganography relies on a large embedding capacity and high-quality images, the embedding of data reduces the quality of the image; steganography is conventionally adopted using least-significant-bit substitution (LSB) of an image's pixels. Sarreshtedari and Ghaemmaghami (2010) have found that many researchers have focussed on solutions for high embedding capacity whilst retaining a high-quality image (Moghadam et al., 2010; Rayappan et al., 2011; Hossain et al., 2014); however, this is a not an issue today as technology has developed to create supreme image quality, such image quality can be found on many mobile devices (Chen et al., 2019; Feng et al., 2019).

The ability to retain image quality has empowered many cyber-criminals as it allows them to easily hide data without arousing suspicion from victims. Regardless, qualified digital forensics investigators will be able to identify steganographic images as part of the investigation process; this reinforces the argument that LSB steganography, at least by itself, is not a great risk to digital forensic investigations. To argue, steganography can be coupled with encryption to provide enhanced privacy, but that aspect would only make steganography redundant as encryption can be used in plain sight as strong algorithms are used to cypher the data, encrypted data can only be accessed using weaknesses in its implementation or with a private key.

2.2 Attacks against Computer Forensic Tools

Attacks against Computer Forensic Tools (CFTs) aim to invalidate data collected by investigators which makes evidence inadmissible in court. There are six phases in the digital forensic investigation process; that is, identification, preservation, collection, examination, analysis, and presentation. Attacks against CFTs target the analysis phase, this is the most crucial part of the investigation process (Garfinkel, 2007). This is because CFTs depend on the analysis phase, as well as the professional skill of the investigator. The analysis phase utilises CFTs to examine the evidence for court proceedings; ergo, CFTs that are verified to use for forensic investigations in court are targeted.

Examples of attacks that invalidate data include the use of buffer overflows and arbitrary code which causes the CFT to be dysfunctional. Upon further analysis, it is found that this is particularly useful when used against network CFTs; tools such as tcpdump, snort, and ethereal are affected as they are vulnerable to an unlimited amount of data input (iDefense, 2005; Infoworld, 2003). Furthermore, Denial of Service (DoS) attacks may also be utilised to target specific components used by CFTs; in particular, attacks can exploit the input function of a CFT. For example, 'Compression Bombs' are used to hoax the investigator into opening a compressed file of a very large size. Folders are compressed numerous times to obfuscate the true size of the compressed file; after an investigator decompresses the folder, the true size is revealed and it causes the CFT to consume an extensive amount of disk space, thereby crippling the memory space and damaging the integrity of the investigation. CFTs often recognise file extensions and opens them automatically if interest is shown by the investigator; EnCase automatically opens .zip files after they are loaded onto the tool.

Regular expressions are used to match patterns of data to validate an input Jan Goyaverts (2019). 'ReDoS' (Regular Expression Denial of Service) is another type of DoS attack that is used to bypass CFTs that try and detect suspicious data using Regular expressions OWASP (2020). ReDoS intentionally provides a poor input to increase processing times exponentially; an example of ReDoS is Evil Regex, in which inputs are created to repeat the creation of groups in order to cause the process to run for a very long time (*(a+)+*).

Analysing this, the likelihood of occurrence of DoS can be avoided if the forensic investigators were trained to carefully configure the input for the CFTs in-line with the type of evidence they are trying to pursue; however, DoS attacks cannot be completely avoided as the specific information an investigator needs is sometimes unknown, or hidden as another data type. Furthermore, attackers who exploit the vulnerabilities found in common CFTs are at an advantage due to their prior knowledge of the tools used to detect their malicious activity. Moreover, attackers have access to a wealth of information relating to forensic tools and practise; thus, vulnerabilities can be elicited by gaining access to the tools or by gaining external knowledge about the tool before formulating an attack. Additionally, attackers are aware of the procedures that state the standards for reliability of evidence, found in the ACPO (Association of Chief Police Officers) guidelines. With prior knowledge of the procedures, attacks can be formulated to damage the integrity of evidence, causing it to be inadmissible in court, this means that adversaries are further at an advantage during the investigation process.

Despite this, not all digital forensics investigations are directly conducted from the perpetrator's computer. Some attacks will require an investigator to analyse the victim first, in order to find evidence that leads to the perpetrator. Even though the same attacks can be conducted on the victim's device, the victim will commonly inform the investigator of this prior to the investigation; consequently, not all investigations can be thwarted by utilising attacks on CFTs. For instance, the famous attack on Sony Pictures© by the Lazarus Group involved infiltrating victims' computers using the Bramble Malware, the victims' computers were used to launch attacks on Sony Pictures© in order to gain access to their systems whilst obfuscating their North Korean IP addresses (Shields, 2018). Investigators then chased leads by analysing the victims' devices; prior to this, the investigators were informed by the organisation's security team of the presence of techniques to attack CFTs. This strengthens my previous argument that not all attempts to attack CFTs can ruin the digital forensics investigation process; to that end, this is not one of the greatest threats to digital forensic investigations.

4.0 Supreme Anti Forensic Techniques

There are numerous anti-forensic tools and techniques available to obfuscate digital activities for users. Traditional techniques are often perceived as basic and can be mitigated by investigators (Garfinkel, 2007), there have been modern advancements for anti-forensics; some of which require thorough technical knowledge to conduct. (Chen et al., 2019; Feng et al., 2019).

In contrast to the traditional techniques, modern anti-forensic techniques focus on minimising fingerprinting and bypassing detection systems. The following section exhibits 3 anti-forensic techniques that pose the greatest risk to digital forensic investigations.

4.1 Cryptography

Cryptographic file systems can be utilised to encrypt data as it is written to the disk, this ensures the data is incomprehensible to anyone without the decryption key. Such file systems are available on Windows, Linux and Mac OS and are secured with a password for authentication. Also, cryptography can be utilised at the application level to encrypt specific documents instead of the entire file system, this method of cryptography is less intensive for performance (Hoffman, 2014).

To encrypt data transmitted within a network, cryptographic network protocols can be utilised to hide information from forensic investigators. Protocols such as 'Secure Socket Layer' (SSL) and 'Secure Shell' (SSH) are used to encrypt the content of network traffic. However, this does not protect investigators from traffic analysis as the communication between different networks via HTTP methods can still be elicited. In some cases, encryption is not used by suspects as the use of cryptographic protocols to hide data can trigger alerts in Intrusion Detection Systems (IDS), this disallows cyber-criminals from breaching networks. Nevertheless, the evolution of cyber-crime has caused advanced methods to bypass IDSs such as FakeTLS (Shields, 2018); furthermore, in particular criminals cases such as terrorism and child sexual abuse, trivial methods for encrypting content such as Full Disk Encryption and Virtual Private Networks (VPN) can be successfully utilised to thwart criminal investigations as it disables investigators from finding evidence that is admissible in court.

Although encryption is not a modern technique, it is arguably the greatest hindrance to digital forensic investigations. This is due to strong cryptographic algorithms that are near impossible to break. Most cryptographic algorithms use large random prime numbers to encrypt data; as prime numbers perform randomly, it is impossible to determine the n^{th} prime number for decryption, this is formerly known as number theory in mathematics (Nicolaou, 2019).

Having said that, even though cryptography is very valuable at hiding information, encrypted data itself is easy to detect. This is due to the high entropy that encrypted data harnesses; encrypted data also embeds flags, signatures, and headers that can be used to automate the process of finding the data. Furthermore, if cryptographic protocols are not implemented correctly, the private key can be determined which can be used to decrypt the data (Casey, 2002). Forensic investigators use tools such as the Password Recovery Toolkit to employ password dictionaries and rainbow tables to decrypt data. By finding encrypted data, it indicates that the suspect may be hiding data that implicate them to a criminal offence; to add to this, many suspects have been convicted without cooperating with law enforcement to decrypt the data due to the Investigatory Powers Act 2016. The Investigatory Powers Act 2016 states that if a suspected offender does not disclose passwords or decryption keys the offender is breaking the law (Legislation, 2016).

However, the judicial system still requires credible evidence to suggest that the encrypted data implicates the suspect of committing a criminal offence; additionally, evidence that suggests the offender is actively refusing to reveal passwords and keys needs to be apparent (Legislation, 2016). Such evidence includes pretending to forget the password, the attempt to destroy a device, and the production of witness statements. Also, suspects are often left uncharged for suspected crimes due to this lack of evidence, this is particularly the case for cyber-criminals as computer devices are the primary vector of cyber-crime, therefore all of the evidence will be located on the encrypted device. Smyth (2016) states that 60% of encryption cases are not processed due to the lack of evidence, this is because it is unlikely the case will lead to a conviction. The Open Rights Group provides backing to this as they state from 2012-2013, they encountered 19 encryption cases where there was a refusal to disclose encryption keys, with only 3 of the cases leading to a conviction (Smyth, 2016). Moreover, cyber-criminals' techniques have advanced to bypass the conviction of the Investigatory Powers Act. A separate encrypted partition can be created that reveals only a small amount of evidence once the password or key is disclosed, whilst a second partition is unknowingly apparent with further encrypted data. This allows a suspect to disclose the password or keys, thus, the Regulation of the Investigatory Powers Act 2000 is not broken.

To tackle this, advanced techniques need to be studied and implemented in forensic investigations, such techniques need to go beyond the standard digital forensic investigations process to keep up with the ever-evolving nature of the cyber-crime. For instance, investigators need to conduct thorough checks of all partitions of a disk to determine if there is any further encrypted content. Advanced research also needs to be conducted to detect the use of malicious protocols such as FakeTLS, training must then be provided to investigators before this is incorporated into the digital forensics process for advanced investigations.

4.2 Onion Routing

The Tor project aims to utilise onion routing to protect users' privacy and anonymity whilst browsing online. Anonymity ensures that the browser does not reveal any identifiable information such as names, IP addresses, or locations; whereas privacy ensures that organisations do not collect any information relating to the browser, account details, and any other information without users' knowledge (Tor Project, 2019).

The Tor Project originated in 1995 by the US Naval Research Laboratories, the main objective of the project was to create an anonymous network communication channel for military communication. The project was later disclosed which triggered vigorous security research. Today, Tor is used by multiple actors such as governments, journalists, researchers, and cyber-criminals; it has over 2.5 million users with 6000+ nodes that interlace users' traffic, rendering it extremely difficult to determine a user's online activity (Tor Project 2019).

In each session, a new virtual circuit is created that is composed of three random relays across the network; information transferred between each relay is encrypted using the Diffie-Hellman key exchange protocol. The information sent to the nodes is encrypted multiple times and decrypted between nodes to determine the next hop point.

Upon further analysis, this carries the risk that law enforcement agents can be the suppliers of exit nodes which have access to the decrypted content (Zorabedian, 2016); however, this is highly unlikely as there is a vast majority of nodes, furthermore, this can be easily overcome by using a VPN in combination with the Tor browser (Proton, 2018). As well as this, the Tor browser changes its destination path every 10 minutes, leaving law enforcement agents a short time frame to collect potentially useless information for investigations. The acute level of privacy and anonymity provided by Tor clearly showcases how it poses to be the greatest risk to digital forensic investigations.

To counter this statement, research has shown that forensic artefacts can be recovered from suspects' devices that use Tor (Dayalamurthy, 2016). The objective of the research was to collect information from the device's registry, memory, and storage. The investigation used the Volatility Framework to recover artefacts such as social media profiles, email addresses, and node information. Hex workshop was then used to find information relating to browser history, email text, IP addresses, ports, and bandwidth information; all of which are highly valuable artefacts for forensic investigations.

On the other hand, to allow forensic investigators to examine a user's device, users must first be subject to a warrant, meaning that they have to already be a suspect. Since Tor provides acute anonymity for online activity, it is highly unlikely that the use of the browser is the cause for law enforcement's suspicions. This means that the evidence found relies on garnering previous evidence, this is outside the scope of for determining if Tor is the greatest risk to digital forensic investigations as Tor would not be the cause of the investigation. Additionally, with FDE, investigators will not be able to recover any of the artefacts showcased in the previous analysis without the data being decrypted.

Going forward, it is difficult to determine steps to remediate the issue of anonymity in Tor network forensics, this is because of the high calibre of technology used to provide privacy and anonymity to users. In some countries, Tor is illegal to use; these countries are Iran and China, France also expressed interest in banning Tor as well as free WiFi networks after the Paris terrorist attacks (Cook, 2015). However, it is commonly perceived that a ban on Tor would be an infringement on the individuals' human rights, as it is a human right to preserve one's privacy (Human Rights Watch, 2015). Further, since Tor is not primarily used by criminals, it is even harder to ban the network for digital investigatory purposes.

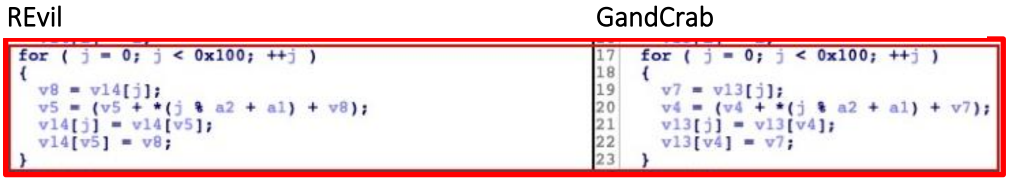
4.3 Malware Obfuscation

Malware can infect devices using various methods, attack vectors include the use of spear-phishing campaigns, botnets, and malicious web servers (Norton, 2020). The detection of such malware relies on digital forensics to identify the malware and to block its access to the network or system. Anti-malware tools commonly use two methods of detection, static and behavioural analysis; static analysis relies on the detection of the malware's file signature, this is generated from the source code of the malware. Behavioural analysis detects malware by analysing its behaviour when run, the malware can be deployed in a secure environment known as a sandbox to determine if the suspected files are malware or not (Sowells, 2019).

Malware obfuscation relies on pre-configured libraries within the source code of the malware, the libraries automatically change the variable names and the structure of the code to avoid detection by static analysis forensics tools, this is formerly known as polymorphic malware. Since the source code of the malware utilises polymorphic code, the file signature of the malware will change after each iteration, causing it to bypass static analysis used in anti-virus and malware tools (Sowells, 2019).

On the other hand, polymorphic malware can be detected by using behavioural analysis, this requires the behaviour of the malware to be previously learnt; to do this, the source code of the polymorphic malware must be analysed to identify parts of the code that remain the same after an iteration. This is then saved and provided a name to formally identify the malware for future attacks.

An example of this was demonstrated during the identification of the REvil malware, figure 1 shows identical decompiled pseudocode for the string decoding function in both malware types. This indicates that the REvil malware derived from the GandCrab malware; moreover, this portion of the code can be saved to detect the malware in future attacks (Secure Works, 2019).



```
for ( j = 0; j < 0x100; ++j )
{
  v8 = v14[j];
  v5 = (v5 + *(j % a2 + a1) + v8);
  v14[j] = v14[v5];
  v14[v5] = v8;
}
```

```
for ( j = 0; j < 0x100; ++j )
{
  v7 = v13[j];
  v4 = (v4 + *(j % a2 + a1) + v7);
  v13[j] = v13[v4];
  v13[v4] = v7;
}
```

Figure 1 - Decompiled pseudocode for string decoder function in both malware types.

To argue this point, behavioural analysis does not protect attacks from relatively new malware, this is because the malware would not have gained enough notoriety to gain the attention of malware analysis professionals. The behaviour of the malware must be specifically learnt and saved as malicous activity before it can be identified using behavioural analysis tools. As such, new malware developed for a specific attack on a victim cannot be detected using behavioural analysis.

To tackle this threat, more attention needs to be paid on patching specific vulnerabilities that malware exploit; further to his, proactive threat protection needs to be more accessible to individual users and small organisations to ensure protection against 0-day malware attacks.

5 Conclusion

This paper has identified many tools and techniques that can be used for anti-forensics purposes and has stated the three greatest risks to digital forensic investigations. Further research is required to classify the techniques into different categories; such as ease of use, the likelihood of use, detectability, and difficulty to overcome.

As anti-forensics evolves, necessary changes must follow in the digital forensic investigation process based on the type of investigation. Investigation types can be classified by the sophistication of the attack, the tools and techniques used, or the motive of the attack. By further classifying the investigation process, it allows investigators to take the necessary precautions to combat the use of anti-forensics tools and processes. For example, if an investigator has prior knowledge that the suspect has astute technical skills, an investigation process can be followed to identify traps such as compression bombs and ReDoS attacks. In respect of this, technological advancements have previously led changes in the investigation process; suspects who utilised encryption taught investigators to conduct a live investigation to ensure evidence is available later in the investigation. Previous changes to the investigation process have been linear; instead, it is proposed to create many investigation processes, to which investigators determine which process to follow based on the previously-stated characteristics of the investigation. This will ensure the latest policies and procedures are followed to combat the latest technological advancements in anti-forensics.

Based on the research conducted in this analysis, the desire for anonymity is clearly apparent in modern anti-forensics techniques. The advancements in anonymity will continue to progress, Tor can be developed to ensure that ISPs and websites cannot detect the user's connection to the Tor network, thereby bypassing additional authentication checks, CAPTCHA mechanisms, and intrusion detection systems. Malware can be further developed to not only avoid statistical analysis but to also avoid behavioural analysis, this is known as metamorphic malware and is rarely seen in new attacks.

Going forward, it is feasible for digital forensics to counter the latest threats and to keep up with the advancements of anti-forensics; however, procedural changes must be implemented. Further human intelligence and time conducted on investigations need to be invested in order to develop a universal investigation processes. Further to this, judicial systems need to be encouraged to consider reasonable doubt in forensic investigations, thus, evidence exposed to anti-forensics will instead be actionable in court.

6 Bibliography

1. Brian Carrier, 2020. *The Sleuth Kit®*. Open Source Digital Forensics, Available from: https://www.sleuthkit.org/sleuthkit/ [Accessed 5 May 2020].

2. Volatility Foundation, 2018. *Volatility Foundation*. Available from: www.volatilityfoundation.org [Accessed 5 May 2020].

3. Liu and Brown, 2006. "Bleeding-Edge Anti-Forensics,"Infosec World Conference & Expo, MIS Training Institute. Available from: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.5063&rep=rep1&type=pdf [Accessed 5 May 2020].

4. Eric Van Buskirk; Vincent T. Liu, 2006. Digital Evidence: Challenging the Presumption of Reliability. *Journal of Digital Forensic Practice*, Taylor & Francis Group, Available from: bishopfox.com/files/articles/2006/Journal_of_Digital_Forensic_Practice%E2%80%93Challenging_the_Presumption_of_Reliability%E2%80%93Mar2006.pdf [Accessed 5 May 2020].

5. Nathan P. Shields, 2018. *CRIMINAL COMPLAINT*. Central District of California: UNITED STATES DISTRICT COURT. Available from: justice.gov/opa/press-release/file/1092091/download [Accessed 5 May 2020].

6. MITRE ATT&CK, 2016. *SamSam*. Available from: attack.mitre.org/software/S0370/ [Accessed 5 May 2020].

7. MITRE ATT&CK, 2016. *Tactics*. Available from: attack.mitre.org/tactics/ [Accessed 5 May 2020].

8. Simson L. Garfinkel, 2007. *Anti-forensics: Techniques, detection and countermeasures*. Monterey, CA, USA: ResearchGate. Available from: researchgate.net/publication/228339244_Anti-forensics_Techniques_detection_and_countermeasures [Accessed 5 May 2020].

9. Kevin Conlan; Ibrahim Baggili; Frank Breitinger, 2016. Digital Investigation. *roceedings of the 16th Annual USA Digital Forensics Research Conference*, 7 August 2016, Pages S66-S75. Elsevier, Available from: doi.org/10.1016/j.diin.2016.04.006 [Accessed 5 May 2020].

10. K. Hausknecht; S Gruičić, 2017. Anti-computer forensics. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 22-26 May 2017. IEEE, Available from: resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/anti-forensic-tools-techniques/ [Accessed 5 May 2020].

11. InfoSec Institute, 2019. Computer Forensics: Anti-Forensic Tools & Techniques. Available from: resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/anti-forensic-tools-techniques/ [Accessed 5 May 2020].

12. Department of Defense, 2006. *Operating Manual*. Washington, USA: National Industrial Security Program. Available from: www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf [Accessed 5 May 2020].

13. Peter Gutmann, 1996. Secure Deletion of Data from Magnetic and Solid-State Memory. *Sixth USENIX Security Symposium Proceedings*, San Jose, California, July 22-25, 1996. USENIX, Available from: www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html [Accessed 5 May 2020].

14. Bernard Le Gargean, 2019. *How Many Times Must You Overwrite a Hard Disk for Complete Data Erasure*. blancco: Available from: blancco.com/blog-many-overwriting-rounds-required-erase-hard-disk/ [Accessed 5 May 2020].

15. Matthew Geiger, 2005. Counter-Forensic Tools: Analysis and Data Recovery. PDT Forensics Team: Available from: https://www.first.org/conference/2006/papers/geiger-matthew-papers.pdf [Accessed 5 May 2020].

16. Offensive Security, 2019. *TimeStomp*. Available from: https://www.offensive-security.com/metasploit-unleashed/timestomp/ [Accessed 5 May 2020].

17. Saeed Sarreshtedari; Shahrokh Ghaemmaghami, 2010. High Capacity Image Steganography in Wavelet Domain. *2010 7th IEEE Consumer Communications and Networking Conference*, 9-12 Jan. 2010, Las Vegas, NV, USA. IEEE, Available from: https://ieeexplore.ieee.org/abstract/document/5421800 [Accessed 5 May 2020].

18. Neda Raftari; Amir Masoud Eftekhari Moghadam, 2012 "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", *Computational Intelligence Communication Systems and Networks (CICSyN) 2012 Fourth International Conference on*, pp. 295-300, 2012. Available from: https://ieeexplore.ieee.org/document/6274358 [Accessed 5 May 2020].

19. V Thanikaiselvan; P Arulmozhivarman; Rengarajan Amirtharajan, John Bosco Balaguru Rayappan, 2011, "Wave (let) decide choosy pixel embedding for stego", *Computer Communication and Electrical Technology (ICCCET) 2011 International Conference on*, pp. 157-162, 2011. Available from: https://ieeexplore.ieee.org/document/5762459 [Accessed 5 May 2020].

20. Md. Rashedul Islam; Ayasha Siddiqa; Md. Palash Uddin; Ashis Kumar Mandal; Md. Delowar Hossain, 2014, "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", *Informatics Electronics & Vision (ICIEV) 2014 International Conference on*, pp. 1-6, 2014. Available from: https://ieeexplore.ieee.org/document/6850714 [Accessed 5 May 2020].

21. Jennifer Newman; Yong Guan; Li Lin; Stephanie Reinder; Wenhao Chen, 2019. StegoAppDB and how prevalent mobile steganography is. *CSAFE Presentations and Proceedings: Center for Statistics and Applications in Forensic Evidence*, 2-21-2019, Iowa USA. ISU, Available from: https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1044&context=csafe_conf [Accessed 5 May 2020].

22. Liyun Liu; Zichi Wang; Zhenxing Qian; Xinpeng Zhang; Guorui Feng, 2019. Steganography in beautified images. *Mathematical Biosciences and Engineering*, 21-2019, Iowa USA. Available from: https://www.aimspress.com/fileOther/PDF/MBE/mbe-16-04-116.pdf [Accessed 5 May 2020].

23. iDefense, 2005, “Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability,” Available from: http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=349 [Accessed 5 May 2020].

24. Infoworld, 2003, “ISS reports Snort vulnerability,” March 4

25. Jan Goyvaerts, 2019. *Regular Expressions*. Available from: https://www.regular-expressions.info/ [Accessed 5 May 2020].

26. OWASP, 2020. Regular expression Denial of Service (ReDoS). Available from: https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS [Accessed 5 May 2020].

27. Chris Hoffman, 2014. *How to Easily Encrypt Files on Windows, Linux, and Mac OS X*. How To Geek: Available from: https://www.howtogeek.com/195124/how-to-easily-encrypt-files-on-windows-linux-and-mac-os-x/ [Accessed 5 May 2020].

28. Nicholas Nicolaou, 2019. Current Challenges in Data Analysis. *Machine Learning*, January 2019, Bournemouth. ResearchGate: Available from: https://www.researchgate.net/publication/335758167_Current_Challenges_in_Data_Analysis [Accessed 5 May 2020].

29. Eoghan Casey, 2002. Practical Approaches to Recovering Encrypted Digital Evidence. International Journal of Digital Evidence, Knowledge Solutions: Available from: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf [Accessed 5 May 2020].

30. UK Legislation, 2016. Investigatory Powers Act. Available from: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted [Accessed 5 May 2020].

31. Padhraic Smyth, 2016. Research Area Overview – Digital Forensics. *Centre for Statistics and Applications in Forensic Evidence*, Available from: https://forensicstats.org/wp-content/uploads/sites/4/2019/05/PSmyth_DigitalForensics_Summary-final-compressed.pdf [Accessed 5 May 2020].

32. John Zorabedian, 2016. *Couple hosting Tor exit node raided by cops investigating child abuse*. Sophos. Available from: https://nakedsecurity.sophos.com/2016/04/07/couple-hosting-tor-exit-node-raided-by-cops-investigating-child-abuse/ [Accessed 5 May 2020].

33. ProtonVPN, 2018. *Why use Tor over VPN*. Proton. Available from: https://protonvpn.com/blog/tor-vpn/ [Accessed 5 May 2020].

34. Divya Dayalamurthy, 2016. Forensic Memory Dump Analysis And Recovery Of The Artefacts Of Using Tor Bundle Browser – The Need. Australian Digital Forensics Conference, Available from: https://ro.ecu.edu.au/adf/122/ [Accessed 5 May 2020].

35. James Cook, 2015. France could try to outlaw the gateway to the dark web to fight terrorism. *Business Insider*, 7 November 2015, Available from: https://www.businessinsider.com/france-is-considering-a-ban-on-tor-and-public-wifi-2015-12?r=US&IR=T [Accessed 5 May 2020].

36. Human Rights Watch, 2015. On the Use of Encryption and Anonymity in Digital Communications. *HWR*, 1 February 2015, Available from: https://www.hrw.org/sites/default/files/related_material/EncryptionandAnonymity_Feb1015.pdf [Accessed 5 May 2020].

37. Norton, 2020. *https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-simple-attacks.html*. Available from: https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-simple-attacks.html [Accessed 5 May 2020].

38. Julia Sowells, 2019. *Static Malware Analysis Vs Dynamic Malware Analysis*. Hacker Combat, Available from: https://hackercombat.com/static-malware-analysis-vs-dynamic-malware-analysis/ [Accessed 5 May 2020].