BOOK CHAPTER | Closed Doors

Inaccessibility of Services as a Threat to Forensic Analysis

Maxwell Amparbeng
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: amparbengMaxwell@gmail.com
Phone: +233545444248

ABSTRACT

Computer and Internet-based crimes are widespread problems that affect a vast number of individuals. Combating such criminals has become a difficult task for competent authorities, as it has enabled a new wave of criminal activity. This phenomenon has drew the attention of security and justice systems all over the world, and these institutions must now deal with the task of reforming and redefining the laws and methodologies used to investigate computer-related criminal activity (Garfinkel, 2010). On the other hand cybercriminals are also making use of existing technologies or systems and new means or techniques to make cybercrime detection, investigation and prevention very difficult. The paper will look at anti-forensics strategies such as data concealment, artefact erasure, trail obfuscation, and attacks on the forensic instruments themselves. Investigators must deal with anti-forensics approaches on a regular basis as digital forensics becomes more significant in current investigations. This article will explore the challenges that investigators and forensic practitioners face when conducting investigations.

Keywords: Digital Forensics, Cloud Computing, Cloud Service Provider, Full Disk Encryption

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Maxwell Amparbeng (2022). Inaccessibility of Services as a Threat to Forensic Analysis
. SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 29-34. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P5

1. INTRODUCTION

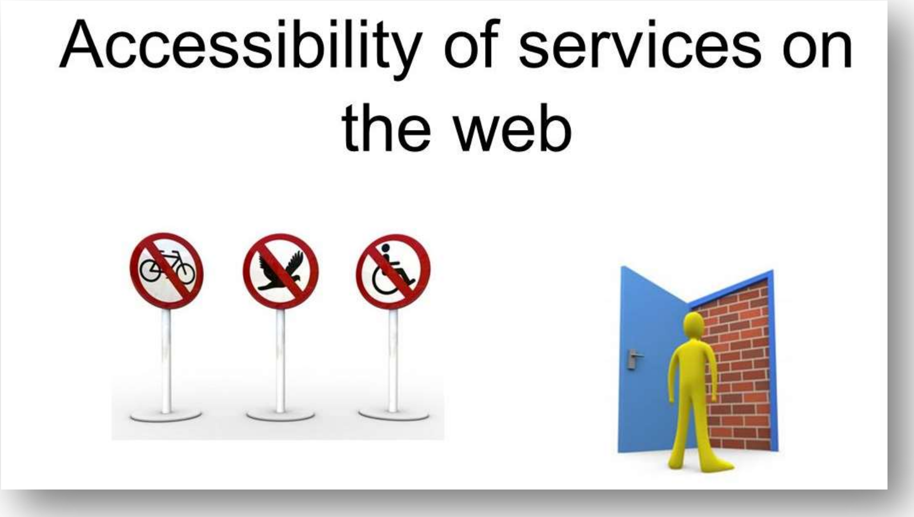
After a computer-aided crime, digital forensics is the process of producing acceptable digital evidence that can be presented to the court. The digital forensics procedure entails locating and gathering data relevant to the crime scene, analyzing the data, recreating the crime scene, and presenting the findings to the courts. Computer forensics, smartphone forensics, network data forensics, and Internet and cloud forensics are the four key sources studied to uncover the evidence. Anti-computer forensics is the application of a collection of techniques as a defense against forensic investigation. Digital forensic investigation is not similar to traditional forensic investigation procedures. It requires specialized training tools which are used on various digital devices. Computerized forensics like other scientific fields moreover requires consistency and guidelines.

Computer forensics has played a significant role in discovering and avoiding frauds as well as prospective business losses that can damage a company's reputation.

The following procedures form the foundation of computer forensics:

- Identifying,
- Preserving,
- Recovering,
- Analysis,
- Presenting.

The above-mentioned collection of processes is concerned with computer forensics for the detection and prevention of fraud and cybercrime; nevertheless, our primary concern now is the efficient application of these processes in accomplishing the desired objectives of fraud and cybercrime detection and prevention.



Accessibility of services on the web

Imagery for Accessibility of Services on the Web
Source: https://slideplayer.com/slide/10687688/

Computer forensics is used in the civil and criminal judicial systems to ensure the integrity of digital evidence presented in court cases. Digital evidence — and the forensic method used to collect, preserve, and investigate it — has grown more crucial in solving crimes and other legal concerns as computers and other data-gathering devices are utilized more often in every part of life. Much of the data collected by modern devices is never seen by the average individual.

For example, cars computers continuously collect data on whether a driver brakes, switches, or changes speed without the driver’s knowledge. However, this information might be crucial in resolving a legal matter or crime, and computer forensics is frequently used to locate and preserve it. Data theft, network breaches, and illicit internet transactions are all crimes that can be solved with digital proof. It's also utilized to solve physical crimes like burglary, assault, hit-and-run accidents, and murder in the real world.

2. RELATED LITERATURE

According to Damshenas et al (2012), Due to limited access to physical devices at the CSP site, the first step in computer forensics is to seize them at the scene. If this is not done, crucial evidence that could be beneficial in computer forensics may be lost. Physical device seizure is difficult in cloud forensics since data is not always available at a single location and may exist in numerous geographical locations. A cloud forensic team can acquire access to physical equipment if the deployment model is private cloud; support and access are provided by the CSP; however, if the deployment model is public cloud, access may not be granted as per the investigation team's requirements. You don't know where your data is stored as a cloud computing customer because it could be hosted in multiple places.

It's possible that CSP is merely pretending to store data in a jurisdiction where laws don't apply in order to acquire access to physical equipment, but this isn't the case, raising serious problems during cloud forensics operations. For example, if a client is from Pakistan and the data is actually stored in Israel, access to the data becomes more difficult due to the nations' diplomatic relations. Traditional software tools Computer forensics are inadequate in cloud computing forensics due to inaccessibility of the physical devices. They become inadequate during cloud digital investigation and not feasible for gathering of digital evidences, so they are not viable for cloud computing forensics. Over the last five years, surveys have showed that enterprises have been increasingly using cryptographic solutions for various data security platforms (K. Getgen, 2009).

According to the poll results, non-users expect to use partial or holistic cryptographic solutions in the near future. This means that cryptographic techniques will soon be in charge of protecting information in the computer world. Investigators can outmaneuver the use of encryption as a provocation to digital forensics operations in a number of ways. These tactics include getting legal 'search and seizure' authorizations or strategically arranging to catch the offender off guard and so gain access to live – operating and unencrypted – systems (E. Casey, G. Fellows, M. Geiger, and G. Stellatos, 2011).However, only a handful of encryption incidents encountered by investigators have been solved using those methods. The greater lot is rarely prosecuted, not because the evidence was overlooked, but because there was nothing that could be done to obtain it.

There are numerous data encryption solutions for disk drives. Each solution addresses data protection and privacy requirements using different methods. Some encryption solutions are compatible with particular operating systems, unlike others who are portable. They protect data at different levels and employ different key management and authentication methods. According to an article published in E-security Planet, (2012), the majority of encryption systems are deployed as software, however some businesses choose hardware-based solutions. A list of popular disk drive encryption solutions is provided below.

Microsoft's BitLocker, Symantec's PGP, Apple's FileVault, WinMagic's SecureDoc ,IronKey's D200, RSA Data Security's RSA SecurPC, and McAfee's Endpoint.

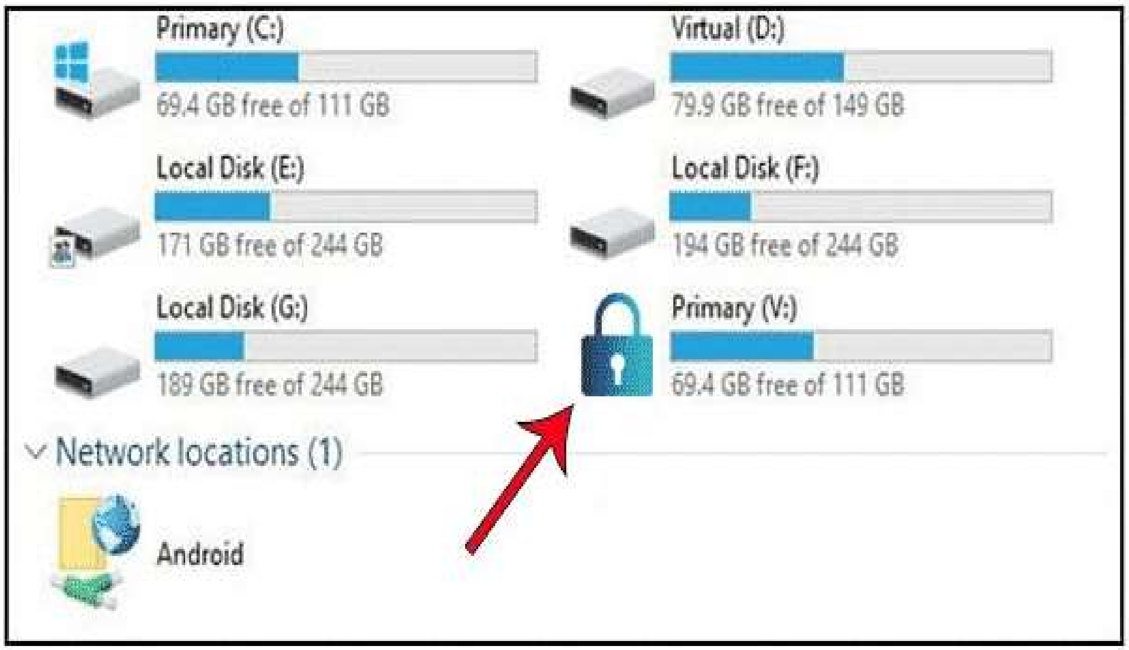


Figure 1: Showing an Encrypted Hard Disk Drive with Microsoft BitLocker

Although data encryption does not completely disable investigators, according to E. Casey and G. Stellatos (2008), the legal system can occasionally assist in gaining access to evidence. Perpetrators used to use file-system encryption because they were only interested in material that was incriminating in their eyes. The other unencrypted regions usually have enough evidence to prosecute them. A whole disk encryption solution, on the other hand, poses a greater threat to digital forensics. However, as the phrase says, "no machine is perfect," and these encryption methods do have certain exploitable flaws.

From the time the symmetric key is accepted by the system until it is shut down, the encryption status ceases to hold for all data on the entire disk. When the system is turned on and off, data becomes accessible and inaccessible, accordingly. Investigators in digital forensics must conduct a legal and well-planned "search and seizure" with the goal of catching the culprit off guard while his system is running.

Another method of avoiding the threat is to conduct a traditional search for the encryption key. No matter how unlikely, the key to decrypt the disk drive could be scrawled on a notepad or saved on a USB drive somewhere at the scene.

3. RESEARCH GAPS/FINDINGS

Finally, research is needed to develop new techniques and technology for breaking or bypassing full disk encryption. Without these measures in place, FDE will increasingly hamper digital investigations.

4. CONCLUSION

The Inaccessibility of Service has far reaching implications in digital forensics.
It presents a significant barrier in the investigation of digital crimes. Investigators' real-world problems were emphasized, and recommendations were made to improve the dependability and accessibility of information systems. This will allow fraud and cybercrime to be tracked in real time, reducing the risk of corporate loss and data leakage.

5. RECOMMENDATION FOR POLICY AND PRACTICES

The following are the recommendation for policies and practices:

- The establishment of a centralized regularity body will be extremely helpful in improving the overall performance and efficacy of forensics teams, allowing them to solve issues that are still posing significant challenges.
- To improve the possibilities of recovering encrypted data from computer systems, digital forensic laboratories must update standard operating procedures to ensure that encrypted disks and volatile data are treated promptly and effectively.

6. DIRECTION FOR FUTURE WORKS

We concentrated on forensics issues related to the inaccessibility of service in this study. These should be better mitigated to improve the overall digital forensics procedure. The following may be the primary areas of future development:

- Research and development of software solutions to improve the evidence collection process in cloud computing.
- Breaking or bypassing entire disk encryption with new approaches and technologies. FDE will become increasingly difficult to conduct digital investigations without these safeguards in place.

REFERENCE

[1] Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology https://arxiv.org/abs/1312.3183

[2] Accessing the inaccessible: digital forensics at the Dalhousie University Archives https://dalspace.library.dal.ca/bitstream/handle/10222/72921/CNSA_2017_Digital Forensics.pdf?sequence=2&isAllowed=y

[3] The Impact of Full Disk Encryption on Digital Forensics https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=8E304358CAA98993223 5B3C46E9CBC4B?doi=10.1.1.178.3917&rep=rep1&type=pdf

[4] Digital forensics vs. Anti-digital forensics: techniques, limitations and recommendations. https://arxiv.org/pdf/2103.17028.pdf

[5] A framework and demo for preventing anti-computer forensics https://pdfs.semanticscholar.org/ec9e/2ba332e370bf225df9c91699b3f60e9d0bd1 .pdf

[6] Taxonomy of Anti-Computer Forensics Threats https://dl.gi.de/bitstream/handle/20.500.12116/22388/GI-Proceedings-114-103.pdf

[7] Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments https://link.springer.com/chapter/10.1007/978-3-030-56223-6_9

[8] K. Getgen, (2009). Encryption and Key Management Industry Benchmark Report. http://beepdf.com/doc/153430/2009_encryption_and_key_management_industry_b enchmark_report.html. Retrieved 19th February, 2013

[9] E. Casey, G. Fellows, M. Geiger and G. Stellatos, (2011). The growing impact of full disk encryption on digital forensics. Digital Forensics. Vol. 8. pp. 129–134.

[10] Forensics Issues in Cloud Computing https://www.scirp.org/journal/paperinformation.aspx?paperid=69913

[11] E. Casey and G. Stellatos, (2008).The impact of full disk encryption on digital forensics. Digital Forensics. ACM SIGOPS Operating Systems Review. 42(3). pp. 93–98.

[12] E-security Planet, (2012). Buyer's Guide to Full Disk Encryption. Available at http://www.esecurityplanet.com/mobile-security/buyers-guide-to-full-disk-encryption.html Retrieved 18th January, 2013.