IMPROVING COLLECTION AND PRESERVATION OF VOLATILE NETWORK EVIDENCE

Qo‘chqorov Jaloliddin Nurilla o‘g‘li

Tashkent State University of Law

Jalolqochqorov1997@gmail.com

Abstract

Digital evidence has become extremely relevant in criminal, civil, and cybercrime cases. In criminal proceedings, the scope of digital evidence is broader, it is not limited to network activities alone, it may also include traditional evidence captured in digital format in specific cases. There seem to be conflicting views among digital forensic analysts on whether digital evidence can be flawlessly manipulated. Many people get the impression that this can be true. Furthermore, state that digital evidence can be tampered with or corrupted based on the manipulator’s skills and expertise, and the manipulation can be unnoticeable despite the knowledge and competence as well as special equipment of digital forensic experts. Internet of Things forensics, Social Media Forensics, and Cloud Forensics are other domains where digital evidence can be acquired and used to solve cybercrime. Digital evidence has the following volatile features; is latent, fragile, easy to modify, can easily traverse jurisdictional borders, is time-sensitive and machine-dependent in many ways, and maintaining it comes with unique challenges. The main conclusion from this paper is the volatility of digital evidence, solutions to manage the challenges of handling digital evidence, and the principles applied in the handling of digital evidence as well as other methods and tools used to preserve the integrity of digital evidence.

Keywords: Volatile memory, Digital, Evidence, Forensics, Volatile, Preservation

I. Introduction. Any data or information processed by electronic media that strengthens or defends a theory regarding the state of digital artifacts or digital events of possible relevance and is admissible in court is classified as digital evidence, (Stoykova, 2021). Digital evidence has become extremely crucial in cybercrimes and criminal cases. Cybercrime has become more prevalent, and law enforcement officers are compelled to explore for precise digital evidence. Several digital forensic operations can be used to uncover crimes, (Sadiku et al., 2017). Any data assigned to a specific device or sent by information technology and telematics systems that have certain operational significance can be regarded as digital evidence, (Amato et al., 2019). Scientific evidence in digital format refers to any data provided to corroborate or reject a concept to specify how a crime transpired, as well as to demonstrate the intent or justification. Digital evidence according to ISO/IEC 270337:20126 is any type of information that may be retained or transported digitally, (Amato et al., 2019), and, digital evidence is any digital data containing credible facts that validate or disprove an incident. Due to the volatile and transient

nature of digital evidence, preserving it as evidence that is subsequently acceptable in court is fraught with challenges in both practice and law, (Camilleri, n.d.). She further states that it should be noted that digital evidence differs from other types of physical evidence in that it can be altered and modified relatively easily, and errors in the processing and maintaining of digital data could cause it to change therefore jeopardising its integrity and validity and compromising its legal worth. Therefore, the integrity of digital evidence is crucial during forensic investigations. This paper aims to discuss the description of digital evidence, principles that should be maintained when handling digital evidence so that it can be preserved for court admissibility, and the literature review on the volatile features of digital evidence as well as the challenges usually encountered when handling digital evidence. Furthermore, this paper discusses other domains of forensics such as Internet of Things(IoT) Forensics, Cloud Forensics, and Social Networks (Media) Forensics, and challenges with evidence acquisition and preservation. Tools that are used to search, collect and preserve digital evidence are also mentioned in this paper as well. The paper contributes to highlighting how the volatility of digital evidence affects its preservation and admissibility in court. The rest of this paper is structured as follows; related work on the volatility of digital evidence, cybercrime and other emerging technologies, description of digital evidence, and volatile features of digital evidence. Challenges of handling digital evidence, possible solutions to mitigate the challenges, tools used to search and preserve digital evidence, and conclusion.

II. Methodology The research methodology for this article adopted a mixed-methods approach. This approach combines both quantitative and qualitative data collection techniques to provide a comprehensive understanding of the research topic. The study began by conducting a systematic literature review of international legal frameworks related to the Cyber insurance. The article includes also scientific articles, research papers, reports, academic journals and conference proceedings, which provides information to understand the field of Volatile Network Evidence.

III. Results Some evidence is only present while a computer or server is in operation and is lost if the computer is shut down. Evidence that is only present while the computer is running is called volatile evidence and must be collected using live forensic methods. This includes evidence that is in the system's RAM (Random Access Memory), such as a program that only is present in the computer's memory. These programs are considered TSRs or Terminate and Stay Resident programs. Many types of malware such as Trojan horse programs, viruses, and worms are designed to be only memory-resident programs, present in the computer's memory when it is operating, and they disappear when the computer is turned off, in many cases leaving no traces. There are also many types of other volatile evidence that are only available while the computer is running, including certain temporary files, log files, cached files, and passwords. RAM is cleared when the computer is turned off and any data that is present is lost. This can be a critical step if there is suspicion that any kind of data encryption is enabled that prevents the hard drive or portions of the hard drive from being viewed. In many cases the only way to recover the password

needed to remove the encryption on a hard drive is to collect the "live memory" before the computer is turned off. Also, if the computer is running, the encrypted portion of the data storage would be accessible, but only until the computer is turned off, making it essential that the hard drive is copied while the computer is still turned on. There are tools available to make copies of RAM and hard drives on running computers and line-of-business servers that cannot be shut down, and still ensure that those copies are forensically sound.

IV. Discussion Cybercrime has become a serious threat to everyone at an alarming rate. Digital evidence is the most crucial part of every cybercrime scene as it serves in determining the accused person's guilt or innocence. The extensive use of digital devices and the rise of cybercrime has led to digital evidence becoming extremely relevant in criminal and civil cases. Pornography, phishing, financial crimes, prostitution, identity theft, and impersonation are all examples of cybercrimes with which digital evidence is associated, however, digital evidence is now employed to convict all types of crimes, (Riadi, 2018). In criminal proceedings, the scope of digital evidence is broader, it is not limited to network activities, and may include traditional evidence captured in digital forms in specific cases, (Wu & Zheng, 2020). To establish a connection between suspects or accused and the related crimes they are suspected of being involved in, cybercrime investigations predominantly depend on digital evidence, (Ali et al., 2022). The following principles must be observed and maintained when handling digital evidence, (Sommer, 2022). ; (i) Digital evidence must be collected in a lawful approach. (ii) Before handling digital evidence, professionals or personnel involved must undergo the required training program on how to handle and process digital evidence. (iii) Any activities or procedures applied to digital evidence should not alter its data. Whenever access to the original data or changes to the system settings are required, only authorised professionals/ personnel should be able to do so, and even those professionals should be able to defend their actions. (iv) Wherever possible, any operation or activity that necessitates accessing or modifying the original data should be documented and witnessed by another professional or personnel member. (v) All operations done while dealing with digital evidence should be recorded and kept on file so that they can be audited. The same operations should be repeatable by an impartial external third party and produce the same results. Digital evidence must be pertinent, substantial, and credible to be admitted in court, and its facts should vastly exceed prejudicial effect, (Krishnan, 2019). He, (Krishnan, 2019) furthermore states, that digital evidence is indeed not different in terms of validity and substance, even though it could be replicated with ease and edited frequently without raising suspicion or without leaving any proof and this can pose distinct competency challenges.

The following characteristics of digital evidence make it a continuous difficulty for forensic professionals who seek to uncover it and examine it in pursuit of truth, (Romero et al., 2019). ; • Unstable and volatile • Unattributed • It

is plausible to make a copy of it • It can be changed, manipulated, and corrupted • Vulnerable and prone to being deleted Digital evidence is latent in nature, because of this, it can only be seen, analysed, presented, and understood using tools. It is fragile and time-sensitive, sometimes it can exist for a short time, hence easier to mishandle, corrupt and destroy, (Alruwaili, 2021). It can be easily misinterpreted, therefore making it misleading and false, and it is easy to replicate and disseminate, which makes maintaining confidentiality difficult. Digital evidence is highly volatile and can be changed as compared to physical evidence, (Schneider et al., 2020). Furthermore, it can be altered unknowingly without leaving apparent traces that are obvious, (Warken, 2018). It is not visible to untrained personnel, and therefore can only be found in locations reachable by specific tools and specialists. Moreover, seized devices can be wiped clean, which means that evidence can be wiped clean remotely before the investigator has access to the evidence. Digital evidence can be perishable in its existence, for example, network logs, a user's browsing history on the internet, posts on social media, instant messaging, cached data, or data that has been erased can all be wiped if not preserved on time, (Considerations, 2021).

Digital evidence, in comparison to physical evidence, has several distinct qualities, including how easily it can be copied, modified, transported, and corrupted. It is often contested in court because of how it is gathered, inspected and reviewed, analysed, and displayed, with parties opposing how the digital device in question was obtained or alleging that it was examined and processed incompetently, (Anderson et al., 2021). The fact that digital evidence's physical attributes can be easily tampered with, as well as the gadgets retaining it, and the lack of necessary technical expertise makes it difficult for courts to authenticate its accuracy and integrity, (Wu & Zheng, 2020). Given its fragile and volatile structure, acquisition and managing of digital evidence is a major task, and because of these characteristics, any unforeseen modification can create irreversible damage and jeopardise its reliability, (Tsai, 2021). Moreover, it is crucial to note that small or insignificant alterations in the digital form either man-made or accidental or natural disasters are difficult to identify and commonly overlooked by forensic officers. Preventing data loss at the crime scene is one of the most serious threats in handling digital evidence. The investigator at the crime scene may be compelled to choose between preserving digital evidence that is more vulnerable to lose and other evidence that is less susceptible to destruction, (Camilleri, n.d.). Additionally, if a live system is restarted or shut down, or if the device is turned off or unplugged from the network, volatile data on Random Access Memory will be lost. Outdated procedures and techniques concerning documentation, collection, analysis, and preservation of digital evidence are also one of the challenges in handling digital evidence, (Mehta, 2018). Furthermore, technical challenges such as encryption, data hiding in storage space, operating in the cloud, and

steganography affect the handling of digital evidence, (Mugisha, 2019). It is also worth noting that a lack of training for forensic investigators can lead to errors when detecting, collecting, and storing digital evidence.

Digital evidence's credibility and reliability are crucial to its acceptance or admissibility in courts, (Wu & Zheng, 2020). According to, (Wu & Zheng, 2020), The authenticity of digital evidence is defined as the digital data or information collected from an electronic device as a true and factual, and exact depiction of initial or original data stored on the device. The integrity of digital evidence on the other hand refers to the electronic gadget and data to be presented as digital evidence is the same as the one that was first identified and taken into custody. Therefore, adequate and comprehensive digital evidence should be assured before and after its acquisition by forensic experts, and it should be protected by the relevant agencies throughout its custody. Below are some possible solutions that can mitigate the challenges of handling digital evidence and its volatility. - To protect the original evidence from accidental damage or malicious tampering, copies of the initial evidence should be made during the evidence-gathering stage, and any future investigations and analyses should be done on these duplicates. - To avoid manipulation and corruption of digital evidence remotely, Faraday shielding may be used. Faraday shielding uses wire mesh bags/Faraday bags to separate electronic gadgets and other cordless devices and hinder radio waves from accessing the captured gadget or leaving via the bag from the seized device. This prevents data from being corrupted or transformed remotely while it is in the possession of the investigators, (Camilleri, n.d.). - Hashing is another solution that can be used to maintain the integrity of digital evidence. - It is a method of testing and verifying whether collected and stored digital data has been manipulated. For the data collected, cryptographic hash values are generated, and the data should yield the exact same hash values when submitted to the same hashing algorithm at a later point in time, (Camilleri, n.d.). - Older or conventional methods used in the recording process in forensic laboratories, should be revised and improved by incorporating digitalised Chain of Custody blockchain technology to mitigate the threats of accidental modification and malicious manipulations, (Casey & Souvignet, 2020). - Digital evidence procedures at the basic training level should be incorporated into academy training for Law Enforcement agencies to assist first responders at a crime scene with basic skills and knowledge on how to handle digital evidence, (Cooper, 2015). In addition, investigators' training and equipment should be updated on a regular basis to assure that they are employing and utilising the most up-to-date technology. In addition to the above-mentioned solutions for mitigating the challenges of handling digital evidence, some principles can be applied, and other methods that can be used to preserve the integrity of digital evidence for court admissibility. The following principles must be observed and maintained when handling digital evidence, (Sommer, 2022). ; (i) Digital evidence must be collected

in a lawful approach. (ii) Before handling digital evidence, professionals or personnel involved must undergo the required training program on how to handle and process digital evidence. (iii) Any activities or procedures applied to digital evidence should not alter its data. Whenever access to the original data or changes to the system settings are required, only authorised professionals/ personnel should be able to do so, and even those professionals should be able to defend their actions. (iv) Wherever possible, any operation or activity that necessitates accessing or modifying the original data should be documented and witnessed by another professional or personnel member. (v) All operations done while dealing with digital evidence should be recorded and kept on file so that they can be audited. The same operations should be repeatable by an impartial external third party and produce the same results. Below are some of the methods that can be used to address the challenges of handling digital evidence; 7.1 Chain of custody The sequential paperwork or collection of documents that show the seizure, acquisition, possession, control, transfer, processing, and disposition of physical or digital evidence is referred to as the Chain of Custody, (Yankson & Davis, 2019). Chain of Custody is one of the methods used to preserve digital evidence. It provides assurance of the credibility and reliability of the evidence collected and presented, (Yunianto et al., 2019). During digital forensic investigations, how digital evidence is extracted, preserved, and documented is dependent upon the principles of the Chain of Custody and the volatility of the evidence. The Chain of Custody should uniquely identify the evidence. Computers, phones, and other storage media can be identified by recording the manufacturer's name, model number, and serial number. If no unique identifier exists, evidence can be tagged, labeled, or barcoded for that specific purpose, (Considerations, 2021). The Chain of Custody should at the very least include the (following, (Considerations, 2021). ; i. The individual who is in charge of gathering or accepting the evidence. ii. The source where the evidence came from iii. The date and time, as well as, where necessary the time zone details. iv. Unique identifiers for digital evidence. v. The tools and methods that were employed to gather the evidence. vi. Any further document that the entity requires 7.2 Blockchain technology Another solution to mitigate the above-mentioned challenges of handling digital evidence is to make use of Blockchain technology. Blockchain is defined as an open decentralised ledger that can efficiently and permanently record transactions or operations between two parties. Blockchains are digitally decentralised ledgers of cryptographically or signed transactions in sequential or chronological order that are grouped into blocks and are fully open to anyone in the blockchain retail, (Sathyaprakasan et al., 2021). Every blockchain includes a hash of a prior block, as well as a time frame that records when a file was created and modified, (Alruwaili, 2021). He, (Alruwaili, 2021), further states that the security on the blockchain is so high that no one, not even those who created the file or document will be able to alter it once it is captured into the system. Features of blockchain are decentralisation, authenticity, reliability, accountability, transparency, and

consistency that are needed by the traditional Chain of Custody, (Tsai, 2021). Some of the examples of Blockchain technology are; BlockDEF: A secure digital evidence framework using blockchain, (Tian et al., 2019). The Application of Blockchain of Custody In Criminal Investigation Process, (Tsai, 2021), CustodyBlock: A Distributed Chain of Custody Evidence Framework, (Alruwaili, 2021). 7.3 Tools used to search and collect digital evidence. Digital forensics uses a variety of tools for the processing, preservation, detection and discovery, analysis, and documenting of digital evidence, as well as legal procedures, submissions of verifiable or factual evidence discovered, and expert testimony,(Sachdeva et al., 2020). Digital forensic investigations necessitate specialised toolkits t gather, protect, preserve, and transport digital evidence, forensic investigations must be fully equipped with the necessary equipment. Depending on the device's operating system and the type of electronic device under investigation, the analyst will use different tools. 7.3.1 Write Blocker The use of write blockers enables read-only access to data storage systems without risking the integrity of the data. The digital forensic investigator duplicates or clon the drive by writing every component of the drive to a blank hard drive after a write blocker has been configured to prevent any data from being written to a suspect's hard drive. Write blockers can be found in both software and hardware,(www.uomustansiriyah.edu.iq, 2018). Write blockers function similarly whether they are software or hardware, they prevent attempts to write to the actual storage media. The primary distinction between software and hardware write blockers is that the software Write Blockers are installed on a forensic computer, whilst the hardware write blocker has the blocking software installed on a microchip on the physical blocker device,(www.uomustansiriyah.edu.iq, 2018). 7.3.2 Autopsy Autopsy is a digital forensic diagnostic tool that can examine original data, E01 disk image, internal drives in a device, and directories successively to identify probable origins of an incident,(Sachdeva et al., 2020). It is an application with a GUI that enables users to examine the hard drives of computers and smart mobile gadgets. The design of Autopsy permits the inclusion of new programs or customisation of some existing programs in python or Java, and functions as web server, and is accessible through an HTML browser,(Sachdeva et al., 2020). Features of Autopsy: - Timeline analysis -uses a visual displaying platform to showcase all incidents to pinpoint the activities that took place. - Search using keywords- it sets up a few modules to scan files containing particular phrases or words and look for frequent terms, and patterns used for the extraction of data. - Web application Artifacts- to distinguish user behaviour from web activities carried out by the user employing popular websites. - Registry analysis- use Register Ripper to uncover facts and retrieve documents. - LNK file analysis- to locate shorter ways for attaining admission to documents. There are benefits to using Autopsy - Fast- it uses a variety of components to execute all background functions simultaneously and delivers results immediately as they are completed. - User friendly- it is easy to set up and install with wizards provided to help through every step of the installation process.

Versatile and adaptable- can be designed with different modules that are also accessible to third parties, examples of these modules are hash filtering, data carving, web artifacts, etc. 7.3.3 Encase Encase is a forensic tool used for investigation in Law enforcement and private companies to collect, examine and report on evidence,(Shah & Paradise, 2014). It has the following features: - Encase uses E01 and L01 to store forensic evidence. - Can work on different operating systems like Windows, Linux, and Unix. - It can also be used to conduct investigations offsite. - Thorough forensic analysis- evidence that would go undetected with other tools can be uncovered by using Encase. It can now analyse EXT4 and HFSX file systems, encrypted drives, iOS physical images, etc, and in addition, an email investigation platform is also available. - Findings can be compiled- analysts can create templates for every case type, audience, and purpose using report features that clients can easily program. These among other many benefits are the features of Encase,(Opentext, 2019). 7.3.4 FTK Imager FTK imager is an open-source Windows-based product that has the ability to collect and analyse digital forensic evidence by making exact copies of the disk(disk imaging) of the original evidence without altering it,(Alwis, 2018). The source of evidence remains unchanged, allowing the analyst to copy data much more quickly and preserve the copied image for further investigation. 7.3.5 Oxygen Forensics Oxygen forensics is a digital forensic tool that enables the automatic collection and examination of data from mobile devices using iOS, Android, and other mobile operating systems,(Sachdeva et al., 2020). For a thorough and organised investigation of data evidence, it permits extraction and processing of social media platforms like Instagram, Facebook Meta, WhatsApp, Telegram, etc,(Sullivan, 2019). The program can be expanded to include additional capabilities for investigating connected gadgets like smartwatches and other latest technologies as well as encrypted data associated with any criminal conduct or illegal activity. The examples of tools mentioned above do not exhaust all the available tools used in digital forensics investigations and evidence collection, they only high lights some of the commonly used tools.

Conclusion

This paper discussed the description of digital evidence, and how it is becoming increasingly prominent in criminal and cybercrime investigations and prosecutions. Digital evidence is fragile, easy to tamper with, and corrupt and destroyed through inappropriate management and analysis. As a result, extra caution should be exercised when preserving digital evidence, neglecting to do so the evidence will be deemed useless and inadmissible in court and result in erroneous conclusions about a case. Other domains where digital evidence can be found include Internet of Things (IoT) forensics, Cloud forensics, and Social network (media) forensics; the same techniques for evidence preservation for court admissibility should be used in all of these cases. There are principles to be applied when handling digital evidence, possible solutions that can be used to mitigate the challenges of handling digital

evidence, and other methods that can be used to preserve the integrity of collected digital evidence. Write Blockers, Autopsy, Encase, Forensic ToolKit Imager, and Oxygen Forensics are some of the tools used to search, acquire and preserve digital evidence. Future research work will focus on the models used to preserve volatile digital evidence for admissibility in Namibian courts. The future work is intended to focus on the design of a model to preserve volatile digital evidence for admissibility in Namibian courts. According to Tredger,C.(2019), Namibia is vulnerable to cybercrimes, making it the most targeted country in Africa, therefore investigations need to be conducted to find solutions that will curb cybercrimes by ensuring that the evidence collected at a crime scene is admissible in court and the offender is prosecuted.

References

Ali, M., Ismail, A., Elgohary, H., Darwish, S., & Mesbah, S. (2022). A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. Symmetry, 14(2), 1–16. https://doi.org/10.3390/sym14020334

Alruwaili, F. F. (2021). Custodyblock: A distributed chain of custody evidence framework. Information (Switzerland), 12(2), 1–12. https://doi.org/10.3390/info12020088 Alwis, C. De. (2018). Evidence Acquisition Using AccessData FTK Imager Acquiring volatile memory using FTK Imager. 1–5. https://articles.forensicfocus.com/2018/03/02/evidence-acquisition-using-accessdataftk-imager/%0AForensic

Amato, F., Cozzolino, G., Moscato, V., & Moscato, F. (2019). Analyse digital forensic evidences through a semantic-based methodology and NLP techniques. Future Generation Computer Systems, 98, 297–307. https://doi.org/10.1016/j.future.2019.02.040

Opentext. (2019). OpenText EnCase Forensic. Opentext/Guidancesoftware.Com, 1–3. https://www.guidancesoftware.com/docs/default-source/document-library/productbrief/encase-forensic-product-overview.pdf?sfvrsn=761867a2_34

Raja Sree, T., & Mary Saira Bhanu, S. (2020). Data Collection Techniques for Forensic Investigation in Cloud. Digital Forensic Science, Vm. https://doi.org/10.5772/intechopen.82013 Riadi, I. (2018). Examination of Digital Evidence on Android-based LINE Messenger. International Journal of Cyber-Security and Digital Forensics, 7(3), 336–343. https://doi.org/10.17781/p002472 Romero, M., MacAs, E., Rosero, D., Quisnancela, H., & Grijalva, J. (2019). OVJESMO Methodology: Data Collected for Forensic Analysis in Hard Disk Drives Applying the ISO / IEC Standard. Proceedings - 2019 International Conference on Information Systems and Computer Science, INCISCOS 2019, 136–143. https://doi.org/10.1109/INCISCOS49368.2019.00030

Sachdeva, S., Raina, B. L., & Sharma, A. (2020). Analysis of Digital Forensic Tools. Journal of Computational and Theoretical Nanoscience, 17(6), 2459–2467. https://doi.org/10.1166/jctn.2020.8916 Sadiku, M. N. O., Shadare, A. E., & Musa, S. M. (2017). Digital Chain of Custody. International Journal of Advanced Research in Computer Science and Software Engineering, 7(7), 117. https://doi.org/10.23956/ijarcsse.v7i7.109

Schneider, J., Wolf, J., & Freiling, F. (2020). Tampering with Digital Evidence is Hard: The Case of Main Memory Images. Forensic Science International: Digital Investigation, 32, 300924. https://doi.org/10.1016/j.fsidi.2020.300924