Procedures for Digital Forensics and Incident Response on Including Data Integrity Constraints on Solid-State Drives (SSD) - A Literature Review

Abdul Shareef Pallivalappil [1, 2] & Jagadeesha S. N. [3]
[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India.
[2] Assistant Professor, Department of Forensic Science, Jain (Deemed-to-be-University), JC Road, Bangalore, India.
ORCIDID: 0000-0001-6221-7078; Email ID: shareef.abdul777@gmail.com
Contact Number: +917760777333.
[3] Research Professor, Institute of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India.
ORCIDID: 0000-0002-5185-2233; Email: jagadeesha2012@gmail.com

Area of the Paper: Computer Science.
Type of the Paper: Literature Review.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.6513305
Google Scholar Citation: IJCSBE

How to Cite this Paper:
Pallivalappil, Abdul Shareef, & Jagadeesha, S. N., (2022). Procedures for Digital Forensics and Incident Response on Including Data Integrity Constraints on Solid-State Drives (SSD) - A Literature Review. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 6*(1), 328-350. DOI: https://doi.org/10.5281/zenodo.6513305

International Journal of Case Studies in Business, IT and Education (IJCSBE)
A Refereed International Journal of Srinivas University, India.

Crossref DOI : https://doi.org/10.47992/IJCSBE.2581.6942.0167

Paper Submission: 17/04/2022
Paper Publication: 04/05/2022

Procedures for Digital Forensics and Incident Response on Including Data Integrity Constraints on Solid-State Drives (SSD) - A Literature Review

Abdul Shareef Pallivalappil [1, 2] & Jagadeesha S. N. [3]
[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India.
[2] Assistant Professor, Department of Forensic Science, Jain (Deemed-to-be-University), JC Road, Bangalore, India.
ORCIDID: 0000-0001-6221-7078; Email ID: shareef.abdul777@gmail.com
Contact Number: +917760777333.
[3] Research Professor, Institute of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India.
ORCIDID: 0000-0002-5185-2233; Email: jagadeesha2012@gmail.com

ABSTRACT

Background/Purpose: *To get evidence from suspect computers running on Windows Operating System, law enforcement agencies and corporations follow many standard procedures relevant to Digital Forensics and Incident Response processes. The primary contrast between forensics and incident response is that forensics is evidence-driven and is often more closely connected with criminal activity, while incident response is more focused on discovering, containing, and recovering from breach of security incidents. A guideline is often intended to simplify certain procedures in accordance with a predefined routine or good practice. As data storage technology progresses from hard disc drives (HDDs) to solid-state drives (SSDs), it has become more difficult for Digital Forensics Analysts to perform evidence acquisition tasks from suspicious systems due to file integrity issues. Existing forensic principles and methods were created mostly on the basis of hard disc drive technology. This literature survey analyses several guidelines to identify gaps in SSD Forensic challenges and makes recommendations for improvement.*
Objective: *To survey leading Digital Forensics and Incident Response guidelines on how SSD forensic acquisition procedures are outlined and to find the gaps and suggest enhancements that might be made.*
Design/Methodology/Approach: *Data from academic papers, web articles, and other sources is analysed and presented using ABCD analysis.*
Findings/Results: *Cyber Security Framework is a vital aspect of an organisations strategy to safeguard its IT assets from cyber assaults and other form of damages. Most organisation use NIST framework since it is being generally acknowledged. However, owing to quick improvement in new technologies CSF's need to be kept up to date in order to confront emerging cyber security threats. After verifying the policy framework of NIST 800-61, it was determined that the SSD forensic gathering approach which raises problems about data integrity has not been addressed.*
Originality/Value: *A study comparing and contrasting different CSFs in the field of Digital Forensics and Incident Response with the most recent emerging technologies will draw more attention to this area from a wider range of stakeholders, allowing the policy framework to keep pace with the most recent emerging technologies in the same time frame.*
Paper Type: *Literature Review Paper.*
Keywords: Digital Forensics, Incident Response, SSD, HDD, Forensic Acquisition

1. INTRODUCTION :

The cyber security framework (CSF) is a collection of management principles for corporate cybersecurity threat that are according to the prevailing industry standards, guidelines, and best practises. It contains cybersecurity categorization at a high level with objectives and a procedure for analysing and managing them, as well as guidelines for preserving privacy and civil rights in a cybersecurity context. Digital forensics and incident response is a subfield of cyber security dealing with the aftermath of an incident. There are various policies and guidelines accessible and utilized by law enforcement agencies and businesses to undertake digital forensics and incident response processes. One such widely accepted framework is The Computer Security Incident Handling Guide, NIST-800-61 by the National Institute of Standard and Technology of the United States Department of Commerce [1], which outlines pre-defined procedures for resolving an incident whenever it occurs. One of the primary facets of digital forensics is the acquisition of data from suspicious devices using a bit-to-bit imaging while maintaining file integrity via hash algorithms. These processes are exhaustively described in NIST-800-61. However, the operations outlined in this framework are more closely tied to HDD's. In recent years, HDD has been less favoured as a secondary storage medium than SSD owing to the latter's falling costs, higher performance and shock resistance. Due to the widespread usage of SSDs, digital forensics and incident response techniques for obtaining data from a suspicious SSD while maintaining data integrity have become a concern [2]. The TRIM mechanism and the SSD's background trash collection make it difficult to recover erased artefacts. The conventional disc write blocker is incapable of terminating the background process. There is uncertainty associated with the collecting of SSD data and it is hard to prove the SSD's credibility in a court of law, casting doubt on the SSD's legal acceptability [3]. Additionally, the NIST-800-61 framework does not specifically define methods for conducting acquisitions on SSDs, creating a challenge for various sectors to agree on a uniform methodology. The goal of this research is to assess several aspects of the NIST-800-61 framework and to compare its application to the acquisition and integrity of data from SSDs.

2. OBJECTIVES :

(1) To understand Digital Forensics and Incident Response life cycle.
(2) To get an understanding of current research status of Cyber Security Frameworks.
(3) To compare and contrast different topics in the NIST-800-61 framework pertaining to data acquisition.
(4) To analyse the issues and challenges that must be resolved through further research.

3. LITERATURE REVIEW :

Every organization needs digital forensics and incident response to investigate and deal with the aftermath of an occurrence. Data acquisition issues from SSDs constitute a significant concern in the digital forensic investigation process, and appropriate rules must be included in CSFs to protect evidence. A brief literature review is undertaken in this field of research as follows:

Azmi, R. et al [4] examined the background and common principles of cybersecurity frameworks and synthesized many diverse views on CSFs and condensed them into a compact vision by the use of contrasts between diverse goals and the distillation of shared concepts.

Dedeke, A., [5] discussed about the commercial data breaches on the increase, NIST released the 2014 CSF to assist businesses in mitigating cybersecurity threats to their critical infrastructure. The critical components of the CSF are outlined, along with advice for businesses at different stages of implementation.

Gourisetti, S. N. G., et al [6] analysed the cybersecurity framework through Real-World Cyber Attack. It discussed about the CSF webtools to provide actionable capabilities that a facility operator may employ to enhance the security of their critical infrastructure in a timely manner.

Syafrizal, M., et al [7] studied about identifying features of cybersecurity standard and framework that may help a business or government choose the right standard and framework, CSF webtools that offer actionable tasks that facility operators may use to improve critical infrastructure security.

Benz, M., et al [8] discussed about cybersecurity evaluation tool for small and medium enterprises and proposed a SME cybersecurity evaluation tool (CET) consisting of a 35-question online survey that IT directors may use to self-assess their maturity level in each of the five NIST framework areas.

Oyelami, J. O., et al [9] suggested standards for cyber security measures in businesses by integrating and synthesising current practises and to build and propose a Cyber Security Defence Policy.

Githinji, S., [10] deliberated about digital forensics policies for forensics readiness in organizations. The goal of the study was to find forensic rules that would allow companies to conduct investigations and gather and analyse digital evidence effectively.

Pathak, J., et al [11] proposed a confidentiality integrated forensic investigations using a goal-based framework. It discussed about how data privacy regulations influence integrated device forensics investigations, the function of anti-forensics, and how to cope with privacy problems in embedded forensics.

Sav, U. M., et al [12] discussed about cyber security policies for anomaly in the workplace. The study analysed cyber security rules and previous studies were analysed in order to protect the firm from compromised users by recognising their unusual behaviour at work place.

Lewallen, J., [13] elucidated on emerging technology and uncertainty in the problem descriptions by investigating the influence of evolving technology on the development of cybersecurity policy in the United States.

Joshi, B. R., et al. [14] conducted an experiment using basic procedures used on standard HDDs and enhanced techniques used on SDDs. They looked at how TRIM functionality was used across a variety of operating systems, disc formats, and cable types to see what obstacles were there in forensically investigating SSDs. The results of the trials demonstrated that enabling/disabling TRIM in SSDs and current operating systems may assist increase and decrease write performance. The usage of TRIM enabled an operating system to alert an SSD of faulty or erased data blocks, which the SSD could then wipe away entirely internally, leaving no traces. The hash value of an SSD may differ depending on when the picture was produced for analysis and evaluation.

Arshad, H., et al [15] discussed that due to the complexity and rapidity of growth in the medium, developing global standards for digital forensics is difficult, if not impossible. At the same hand, typical scientific testing methods such as testing on a standard data corpus make it difficult to corroborate forensic procedures. As a result, researchers may help to improve the accuracy of recommended procedures and confirm that proposed approaches fit legal standards in the courts. Before being used, the procedures must be properly tested and validated for correctness. Before adopting these methodologies, it is necessary to understand their possible error rates and limits, as well as to support additional testing under various conditions. In addition, substantial testing and systematic verification are required to gain a strong presumption of validity. To secure the progress and future sustainability of digital forensics, highly accurate methodologies based on sound scientific standards and foundations are the only alternative.

Nikkel, B. [16] highlighted the debut of (Non-Volatile Memory Express) NVME drives on the customer marketplace along with emerging issues for the digital forensics field. Forensic laboratories must be aware of NVME and adjust protocols to incorporate NVME drive processing, examining various modules, and collecting accessible artefacts that are specific to NVME drives. Software providers must test their products to guarantee that they are compatible and behave properly with NVME devices. The paper discusses that it is impossible to assume that existing forensic applications will perform as intended with NVME systems. Developers may demand additional functionality in order to examine and obtain new forensic data connected to NVME technology. Manufacturers of hardware write-blockers confront a problem in developing new solutions that conduct write-blocking of NVME devices by reading instructions sent to the PCI Express bus's NVME interface. Developers of software write-blockers have a similar issue in adapting their code to accommodate the NVME command set. Forensic standards organisations like NIST Computer Forensics Tool Testing must develop equivalent testing protocols for NVME write-blocking tools and verify NVME write-blocking hardware or software when they become available. It is unclear how common NVME drives will become in the future, according to the report, particularly in the consumer market, as of this writing. The AHCI standard is still used by the majority of PCI-based storage devices today. The performance and efficiency advantages of NVME, on the other hand, are attractive, and will become more so as SSD capacities grow and manufacturing costs fall.

Barbara, J. [17] discussed that when compared to a traditional HDD, SSDs have a completely different architecture and functioning. These distinctions have several benefits, including the absence of moving elements, short random-access times, and shock and vibration resistance. Their design and functioning,

on the other hand, generate some significant challenges in terms of forensic investigation. Data self-corrodes as a result of processes like wear levelling and trash collection, and there is no scope to recover destroyed data regardless of whether the drive is imaged live or write-blocked and reviewed post mortem. The fact that the SSD may plainly self-modify its contents after being imaged is quite troublesome, since it can lead to Hash Value differences and data corruption. Finally, an encrypted SSD will very certainly be unable to supply any useful information. With all of these and other forensic concerns, an examiner's best bet is to treat an SSD like any other piece of volatile evidence. To properly extract and retain the evidential value of any probative information obtained, examiners would require a thorough grasp of SSD design and operation, as well as significant documentation of their forensic methods and processes.

Roussev, V. [18] in the book, discussed about the rapid rise in acceptance of solid-state discs (SSD) poses a new challenge. The reason for this is because in order to be reused, SSD blocks must be written again. The first write clears the state of the block, enabling it to be reused. The UNMAP and TRIM instructions were introduced to the ATA and SCSI command groups to increase performance. They provide the file system a way to inform the storage device that which SSD blocks should be trash collected and prepped for reuse.

Jazzar, M., et al [19] discussed in their paper that historically data was stored on HDDs. While solid-SSDs are employed for the same function, they might be thought of as the HDD's replacement. Even though the storage media market began with hard disc drives, every tool has an expiration date, and hard disc drives have demonstrated that they cannot provide the needed speed for users and the entire industry in general. Due to the fact that SSDs are still relatively new goods, they bring with them new obstacles and difficulties.

Luciano, L., et al [20] highlighted critical issues that the community should solve, concentrating on where the security domain is presently, where it needs to go, and the measures necessary to enhance it. The findings indicated that financing for research and development in developing fields was constrained and a lack of uniformity across all facets of the sector, particularly in the areas of policies and ethics. The paper also discussed about the standing of cyber forensics has to be elevated in order to establish it as a credible field.

Riadi, I., et al [21] in their paper examined experimental forensic investigations on a computer with a SSD, HDD in a frozen state. Despite the fact that solid state drives and hard disc drives operate differently, forensic operations may be performed on both. Based on experimental results, the extraction and evaluation operations will be performed utilising frozen software and a variety of forensic tools. As a result, not all files can be restored successfully due to the file structure and contents being destroyed. Not all forensic instruments are capable of reading all artefacts, and only a subset of forensic devices produce meaningful results.

Bell, G. B., et al [22] discussed how a paradigm change has occurred in technological storage, with sophisticated, transistor-based systems for primary storage becoming more prevalent. While the majority of people are familiar with the move between floppy discs to portable USB transistor flash devices has been seamless. From HDDs to SSDs within modern computers has received little attention from the scholarly community thus far. The paper demonstrates that relying on present evidence gathering systems and procedures is not appropriate and perhaps irresponsible, and that common assumptions regarding the behaviour of storage medium are no longer true.

Gibson, M., et al [23] experiment results showed that the evidence drive's most intriguing outcome was the disparity in data collected between the baseline image and the cloned SSDs. The bulk of evidence-based reports revealed more artefacts from the baseline picture than could be extracted from the SSDs. These discrepancies are the result of the SSD controllers actively attempting to organise the duplicated data more effectively through the use of wear levelling, TRIM, and other unique data organizing methods. By simply powering the SSDs during the evidence recovery procedure and during the final run of the baseline image, the control systems were able to clean out information that had been copied to the drive but had been designated for deletion, resulting in a substantial decrease in identified artifacts in a number of categories.

Jaatun, M. G., et al [24] introduced the Incident Response Management technique, which applies generally incident response with practical education and socio-technical viewpoints to create an effective incident response management system. In addition to integrated operations within the petroleum sector, the IRMA technique has applications in a variety of other industries that depend on

process control applications.

Catota, F. E., et al [25] as part of its investigation into the challenges that the Ecuadorian financial business faces when interacting with cybersecurity incidents, this study looked at two possible methods that have been successfully implemented in the advanced world CSIRT and information sharing that could be used to enhance the sector's cybersecurity capabilities and thus its ability to react to the associated risk. Using a combination of organised and open-ended questions, as well as two cyber-attack scenarios, several semi-structured interviews with many stakeholders were performed using both organized and open-ended queries. This study, which is based on a qualitative text analysis, describes experiences with security events, as well as hurdles to reacting to threats and the intended actions of key parties.

Ramadhan, R. A., et al [26] built a framework for Digital Forensic investigations in their research by displaying proof in the form of a non-volatile architecture and then putting the framework into practice. The National Institute of Justice is a resource that has been often used by academics in previous research projects. As a reference, the design also includes steps that must be completed as part of the process of collecting digital evidence. In designing this framework, the intention is for it to serve as a legal approach that can be applied exactly to the practice of collecting non-volatile digital evidence. Prior to beginning work on the design, the author conducted a literature review on the NIST SP 800-86 and ISO 27037:2012 standards, after which he combined them to produce a hybrid nomenclature. As a result of this research, a combination of the two standards is being developed, which will serve as a basis for monitoring and analysing Digital Forensic science in the years to come.

Göbel, T., et al [27] articulated that a large quantity of realistic, timely training data is required in order to properly educate experts and to maintain their knowledge and skills up to date. In contrast, a significant gap in digital forensic training statistics owing to a variety of factors such as privacy concerns, secrecy concerns, and intellectual property rights. A number of synthesis frameworks for generating realistic digital forensic data sets have emerged in recent years. While no one framework provides a complete approach to the development of realistic digital forensic relevant traces from a range of sources, there are many frameworks that may be used in conjunction. According to the research, ForTrace is a complete framework for the simultaneous development of durable, volatile, and network traces, which is presented in this article.

Javed, A. R., et al [28] proposed in their research survey is to identify current state-of-the-art digital forensics concepts in current studies, to focus attention on research problems, and to provide a thorough description of different computer forensic contexts and forensic toolkits used for computer forensics in the current era of information technology, according to the article. In addition, the survey that has been proposed gives a comparative analysis based on the characteristics of the instrument, which will aid investigators in the selection of tools throughout the forensics investigation process. In the end, the suggested survey analyses and deduces present issues in computer forensics, as well as prospective research objectives in the field.

Riadi, I., et al [29] emulated delivering spamming emails to a single victim, with a total of forty spamming emails sent to the victim. Network Forensics Development Life Cycle approach is used in this study, which includes the phases of commencement, acquisition and execution as well as the stages of functioning, maintenance, and disposal. Wireshark tools are used to simulate delivering email using simple email spammer tools and to verify the delivery of email. In the test, forty emails were successfully received or inserted into the victim's inbox, and the test was successfully completed by receiving results based on present criteria, which demonstrated that the test was effective.

Rachman, H., et al [30] explained that the growing number of people who utilize computer technology opens the door to the prospect of crimes taking use of information technology continuing to grow, either directly or via indirect means. Criminals often use computer gadgets in their criminal activities. The fact that this is a major source of worry means that the necessity to handle digital evidence has become substantially more critical. As a result, a forensic storage architecture is necessary for the administration of digital evidence. The composite logic technique is used to develop the framework under consideration in order to determine the role model of each variable or the beginning pattern of the phases to be agreed on. Composite logic provides a role model, which may then be utilised to construct patterns in order to achieve the same goal as original logic. This technique collaborates on a framework for managing the pre-existing hard disc drives, solid state drives, and virtual machines, which are then incorporated into a forensic storage framework.

Ninahualpa, G., et al [31] supported the automation of information retrieval on SSD using an application called Carvers Suite, which is supported by recovery approaches and methodologies (File Carving); affectation variables, and the most probable circumstances as elements that cause this loss. In addition to the work done in SSD, the scientific approach was established in line with the experiments and was based on the work done in SSD and the usage of File Carving forensic recovery techniques.

Nnoli, H., et al [32] suggest in this study that large organisations with a need for forensically sound practise implement a corporate forensic governance framework in order to improve their preparedness for forensic investigations, governance, and management, as well as to increase the use of automated forensic methods and forensically sound practises in-house.

Nordvik, R., et al [33] In the context of file system interpretation for digital evidence of system files analysis, this paper examined current best practises for Digital Forensic tool and method validation. In criminal investigations, reverse engineering of file systems is essential to meet legal and scientific criteria. In the present state of things, there is no standard process for verifying the dependability of file systems reverse engineering. Ideal validation criteria do exist, but they are at a top standard, and there is no practical application of these criteria in practice. The authors suggest a systematic dependability validation technique for file system reverse engineering in this study, which comprises describing the forensic workflow, including the tools utilized, and confirming the method's and findings' availability and repeatability. It is also discussed about the benefits of formal serviceability validation procedures for system file reverse engineering.

Perumal, S. [34] proposed digital forensics model according to Malaysia Cyber Law, that will encompass the whole range of an investigative process. It is also essential to measure the suggested model to the actual model, which is presently accessible and being used in the course of the investigation process.

Yusoff, Y., et al [35] looked at a few chosen investigative methodologies throughout the years and then found the processes which were most often used by everyone. The authors hope that, by identifying the most frequently used fragment process, it will be simpler for new users to grasp the procedures and will also act as the fundamental underpinning idea for the construction of a new set of processes. Thus, authors created a general computer forensics investigation model, known as the GCFIM, based on the methods that were routinely used.

Reith, M., et al [36] explored the progress of the digital forensic inquiry, assesses four distinct forensic methodologies, and, as a consequence of its results, proposes an abstract model of the digital forensic process. As a result of its efforts to overcome some of the drawbacks of earlier techniques, this model offers the following benefits: An abstraction structure that allows for the inclusion of nondigital electronic devices within the abstraction structure; a mechanism for adapting the abstraction structure to future digital technologies; a generalised approach that judicial members can use to relate technology to non-technical observers; and a consistent and standardised framework for the creation of digital forensic tools.

Carrier, B., et al [37] Introduced the notion of a digital crime scene, replete with witnesses, evidence, and events, all of which may be investigated in the same manner that a real-world crime scene could be. If the proposed technique is followed in its entirety, the physical crime scene investigation is merged with the digital crime scene investigation in order to identify the person who is responsible for the digital activity. The suggested approach may be used in both law enforcement and business investigations, according to the authors.

Kyei, K., et al [38] using the Systematic Digital Forensic Investigation Model, an overview and comparison research of the current digital forensic investigation models were explained and suggested an improved model based on the findings of the study. One key problem of digital forensic inquiry is that it does not always focus enough attention on the legality of the evidence acquired. This is a fundamental shortcoming. For a prosecution, the digital forensic inquiry must comply to the standard of evidence and the validity of the evidence. As a result, the techno-legal aspect of this suggested model, together with the adoption of best practises from other models, distinguishes it from others.

Wazid, M., [39] discussed that hacktivism is the most significant problem that the online world is now facing. Many digital forensic tools are being created to cope with this difficulty, but hackers are also inventing counter-measures at the same rate as the tools themselves. This article covers the fundamentals of digital forensics as well as the most current developments in hacktivism, including

social networking sites, cloud computing, websites, and phishing attacks. The numerous forensics tools, as well as the platforms on which they may be used, as well as their most current versions and license information, are reviewed.

Pilli, E. S., et al [40] provided an in-depth examination of the different network forensic frameworks that have been presented so far. On the basis of several current models of digital forensics and on the basis of these models, a generic process model for network forensics is offered. This model is based on diverse current models of digital forensics and is constructed on the basis of such models. The definition, classification, and objective for network forensics are all clearly explained in this document. In this article, the capability of several Network Forensic Analysis Tools and Network Security Monitoring Tools, which are accessible to forensics examiners, is explored in detail.

Halboob, W., et al [41] suggested several degrees of privacy for computer forensics. To start, all forensic data must be categorized, and all shared data possibilities in computer forensics must be thoroughly investigated and tested. Then, depending on the discovered access possibilities, it defines a number of different privacy levels. The privacy levels that have been developed result in a more efficient privacy-preserving computer forensics system.

Rogers, M. K., et al [42] conducted pilot research and the purpose was to contribute to the expanding quantity of knowledge addressing the unique problems in computer forensics. To choose the top five difficulties in computer forensics in an Internet-based poll, which was conducted as part of the research. Using a free form text box, sixty respondents provided their responses to the survey. According to the findings, education, training, and certification were the most often cited issues while a lack of funds was the least frequently reported concern.

Bennett, D. [43] discuss that, when acquiring information from mobile devices, a forensic investigator may encounter a number of legal obstacles, such as those posed by the Fourth Amendment, and chain of custody concerns, which are all discussed in detail in the article. The reader will get an understanding of the difficulties associated with efficiently managing digital evidence gathered from such mobile devices, as well as some of the difficulties associated with employing some of the more popular forensic tools now available on the market.

Yasinsac, A., et al [44] show that the use of science and education in computer-related criminal forensics is still primarily restricted for government law enforcement organizations. In addition to supporting the constantly rising area of computer and network forensics, it is necessary to build an appropriate workforce programme.

Kumari, N., et al [45] discuss that in the event of the spread of modern computing accelerates, cybercrime expands, and crime investigation matures into a more demanding subject that must be addressed. Though many good digital forensic tools have been created, the investigation of the majority of cybercrime is challenging owing to a lack of appropriate forensic techniques and specialised instruments in most situations. An effective forensic strategy, as well as effective forensic analysis tools, are required for a cybercrime investigation. In this article, it has been explored how the many digital forensics branches interact with one another and with the various forensics tools that are accessible.

Beebe, N. L., et al [46] have devised a complex hierarchical system to guide their digital research efforts. The structure is divided into phases and sub-phases based on goals that are applicable to various levels of information and to which further layers of information may be easily added as necessary. The framework is divided into stages and sub-phases that are appropriate for projects with varying degrees of complexity. In addition, the framework incorporates ideas that may be used in a variety of ways throughout all stages. An example of how the architecture may be further filled and used is the data analysis function, which is meant to discover and retrieve forensic evidence.

Alzaabi, M., et al [47] A digital forensics system based on relative importance, known as the crime investigation system, was discussed to help forensic investigators in determining the most powerful people of a criminal organization who are related to known members of the group, for the purpose of conducting an investigation. Authors have created the CISRI framework to deploy a network diagram that depicts the structural relationships that exist between members of a criminal organisation. An individual node in such a graph represents a member of an illegal organisation, each edge linking two nodes indicates the connection between those two members, and the weight assigned to any given edge reflects the degree of relationship between those two members, as seen from above.

Shrivastava, G. [48] provided an in-depth examination of network forensics since 2005. At first, the article provides an overview of network forensics and security frameworks, followed by a discussion

of their related work, which includes a survey paper, and finally a review of several Network Forensics Analysis tools and their process model.

Vlachopoulos, K., et al [49] discuss about a paradigm for examining crime scenes using hybrid evidence model. The methodology integrates the evidence collection processes and policies associated with the collecting and investigation of digital and physical evidence, while taking into account the distinct features of each kind of evidence collected and examined.

Mohite, M. P., et al [50] proposed an advanced crime scene investigation tool and related framework based on cloud computing, in order to provide an advantage to advanced crime scene investigations in a cloud system. This programme has a number of functions that may be used to investigate the evidence, including sorting, data recovery, hex viewer, indexing, etc.

Yasin, M., et al [51] proposed in this study to develop the DigLA GUI-based forensic tool, that is intended to be used by laymen and to offer a single platform for analysing Digsby log data at various degrees of complexity.

Rogers, M. K., et al [52] suggest the use of an onsite or field strategy for providing identification, analysis, and clarification of digital evidence in a short period of time, rather than needing that the system/media be taken lab for an in-depth examination or the acquisition of complete forensic images. This model is known as The Cyber Forensic Field Triage Process Model. After the initial field triage has been completed, the proposed paradigm is consistent with generally accepted forensic concepts and does not rule out the possibility of transporting the system storage media back to a lab setting for a more in-depth inspection and analysis after the initial field triage has been completed.

Nicholson, A., et al [53] discuss that attribution that may be used to defend against a wide range of adversaries. The attribution of cybercrime may assist police investigations in identifying and apprehending cyber offenders. When it comes to cyber warfare and conflict, an attribution capability is sought to aid in the decision-making process and cyber security framework of Computer Network Operations (CNO). The identification and attribution of terrorist cyber-attacks may aid in the prevention of future attacks. Assaults that have received widespread attention, such as Stuxnet and Night Dragon, have been subjected to extensive investigation.

Cohen, M. I., et al [54] elucidate that with the GRR Rapid Response Framework, an open-source tool for corporate forensic investigations that allows remote raw disc and memory access. GRR is intended to be expandable, which opens the door to ongoing enterprise-wide forensic analysis in a centralized location. This article outlines the architecture used by GRR and demonstrates how it is commonly utilised to speed corporate forensic investigations.

Vömel, S., et al [55] discuss that various technological advancements, such as rapidly increasing storage capacities of hard drives, memory-resident malicious software applications and the increasing use of encryption routines in computer forensic investigations, have resulted in the limitations of conventional enduring data-oriented strategies in computer forensic investigations. The result of these limits is that conducting an in-time inquiry is becoming more difficult. In order to deal with these challenges, security experts have begun to investigate alternate data sources and, more recently, have emphasised the importance of volatile system information stored in random access memory (RAM). In this article, we provide an overview of the most widely used methodologies and approaches for collecting and analysing the contents of a computer's memory space. Individual solutions are described in terms of their qualities, advantages, and limitations, and potential for future study in this rapidly growing area of information security are discussed as well.

Shosha, A. F., et al [56] a forensic analysis framework for questionable programmes that are in executable binary form is described in further detail. This approach is intended to recreate high-level forensic actions and accurately estimate action claims from low-level assembly code; in other words, the recreated acts will assist in the deduction of evidence and traces caused by a great interest within an operating system under investigation in the field of forensics.

Latzo, T., et al [57] provided a taxonomy of acquisition strategies and a framework based on a well-defined partial order that generalises the idea of ring-based privilege separation. They also provide examples of acquisition techniques. It also includes information about the acquisition process. Using the taxonomy that has been constructed, we can provide a comprehensive review of the most up-to-date memory acquisition methodologies that are independent of the operating system being used or the hardware architecture being used.

Marturana, F., et al [58] discussed that the result of an investigation on the categorization of mobile

phones in the context of a real-life paedophilia investigation. Based on the categorization idea from Mobile Forensics and the use of self-knowledge algorithms for categorising mobile devices, it is concentrated on the efforts on developing a realistic method and framework for predicting phone use categories in real time.

Luoma, V. M. [59] discuss that result of disobedience with discovery demands for electronic records, recommends some proactive activities that an organisation might take to reduce the probability of judicially fines. The first stage is the construction of an Information Management Team, which will comprise professionals in information management, law, computer forensics, information technology, and auditing as well as other disciplines. The next stage is to create and execute a security policy for the retention and destruction of electronic documents.

Dahbur, K., et al [60] discuss that computer forensic scientists and investigators have developed a variety of research method, frameworks, process workflows, and technological tools that have been successfully applied to assist them in collecting and analysing digital evidence for the purpose of resolution of cases that involve the use or misappropriation of computers. Anti-forensics poses a number of difficulties, which this study attempts to address by examining a number of different anti forensic processes, tools and approaches, providing a logical taxonomy for them, and discussing their efficacy. Furthermore, the authors examine the difficulties associated with putting in place effective remedies against these tactics.

Law, F. Y., et al [61] attempt to deal with problem of protecting data privacy and provide an encryption model and framework that may be integrated into the existing digital investigation framework.

Reddy, K., et al [62] provided a framework meant to help organizations in creating a forensic ready capacity in the event of an incident involving information privacy. To be more specific, the framework offers direction on defining policies, business processes, and organisational functions at the highest levels of government. It also aids in the selection of device-level forensic methods, standards, and processes that are necessary to deal with information privacy events when dealing with a breach of confidentiality.

Rekhis, S., et al [63] in this study, have built a theoretical approach to digital inquiry that is cognizant of anti-forensic assaults. Following the description of an investigation procedure that is capable of addressing these assaults, for the installed security solution, the evidence they provide, and the library of attacks that have been found, a state-based logic model was built to describe the investigated system. Anti-forensic threats are being mitigated, and prospective scenarios are being generated from hints that have been aimed by these attacks.

Liu, Y., et al [64] discuss that using upgraded SSD-based electronic evidence screening approach, it is recommended that the SSD neural network be optimized flexibly, the process component be integrated into the superficial permutation layer of the network to improve the representation ability of the feature map, and features from different convolution be fused with multi-scale systems to increase the narrow features.

Alhasan, H., et al [65] presented a unique command set in SSD, Read-Verify Overlap, that recaptures the unneeded power from the hyperbole and uses it to compensate for the lost concurrency in a distributed computing environment. In order to achieve practical fine-grained power management, it also provides a generic power-aware scheduler in conjunction with RVO. Also shown via studies is the ability of RVO-based video analytics systems to achieve zero frame drop while maintaining compliance with industrial read latency requirements, particularly in write-intensive workloads, even while employing RVO. This study gives insights about density and parallelism in SSD data storage.

4. CURRENT STATUS OF INCORPORATING SSD FORENSIC ACQUISITION IN CSF's :

The literature review emphasises the fact that CSFs are an integral part of any organization's IT process and IT infrastructure, but the specific emerging challenges that must be addressed in CSFs have not been covered in detail. This is especially true when imaging an SSD and then ensuring the file integrity so that it can be used in a court of law or for the reconstruction of evidence has not been covered in detail. In digital forensics investigation process, in order to ensure that data is accurate, replicable, and hence useful, businesses in both the regulated and unregulated sectors must place data integrity at the centre of their informatics operations, regardless of their size or industry. The analysis of literature provides no clarity on the framework guidelines for SSD acquisition that ensures data integrity in the digital forensic collection procedure.

5. DESIRED STATUS IN CSF's TO INCLUDE DATA INTEGRITY CONSTRAINS ON SSD's:

One of the most important parts of the digital forensic investigation process is data integrity. During the acquisition process of secondary memory, such as HDD or SSD, where data is kept permanently, an imaging process is carried out, in which the secondary memory data is transferred bit-by-bit to an external sterile medium is carried out. Once the data has been imaged, it must be validated for file integrity using one of the hashing techniques available, such as MD5 or SHA256, before being used. This is done to guarantee that the imaged data corresponds to the data from the original source. The hash value of the imaged source must be the same as the hash value of the original source; otherwise, it will be considered evidence tampering and will not be accepted in a court of law [67]. The rationale for this is because when doing digital forensic analysis, investigators should avoid working on the original source since there is a risk of evidence manipulation or loss. It is possible to understand various aspects of the digital forensic analysis process within the current framework, such as NIST 800-61, however it is not relevant in the case of SSD's. Since of SSD functions such as TRIM and Garbage collection, maintaining data integrity after image acquisition is difficult because the hash value produced by the SSD differs from the hash value produced by the original source. As a result, the data integrity of SSD's cannot be verified in a court of law. As more than just a consequence, a complete methodology should be incorporated in leading CSFs such as the NIST 800-61 so that adversaries who take advantage of the gap in digital forensic inquiry are dealt with in the proper manner.

6. RESEARCH GAP :

Law enforcement organisations and businesses operate under distinct frameworks for digital forensics and incident response procedures. The NIST-800-61 is one such generally established framework. It discusses the rules and actions for responding to a cyber-attack situation. Data acquisition from a suspicious device is a critical element of the digital forensic life cycle. However, as secondary storage technologies progress and hard disc drives are increasingly being replaced by solid state drives, it has become more difficult for digital forensics and incident response experts to obtain data from SSDs while maintaining data integrity and retrieving erased information. There is no mention of this issue or strategy for resolving it in the NIST-800-61 framework. The goal of this research is to assess the NIST-800-61 framework and identify areas that need revision.

7. RESEARCH AGENDA :

(1) To elucidate the challenges faced in conducting forensic acquisition in SSD's compared to HDD's.
(2) To understand how important is CSFs in an organization.
(3) To point towards the disparity between the latest technologies in the field of information technology and cyber security frameworks.
(4) Suggest improvements to limit cyber security adversities within the purview of CSFs.

8. METHODOLOGY :

Explanatory study is conducted to determine the kind of security policies and correlation with emerging technologies in order to assess the impacts of specified regulations, various practises, and so on. Journals, conference papers, media articles, and public documents were used to compile the information for this literature review.

9. INCIDENT RESPONSE LIFE CYCLE :

The process of incident response is divided into numerous stages. The first phase entails the formation and training of an incident response team, and the acquisition of relevant tools and resources. Furthermore, the organisation aims to decrease the number of occurrences that will happen during the initial stage by choosing and implementing a set of controls depending on the risks identified. Nevertheless, residual risk will always exist after safeguards have been implemented. Because of this, it is necessary to identify security breaches in order to notify the organisation whenever a breach takes place. Based on the intensity of the crisis, the organization may be able to contain it and finally recover. Detection and analysis are often used during this phase, for example, to verify if new systems have been infected by malware when removing a malware event. The organization prepares a report documenting

the incident's cause and cost, as well as the activities the organization should take to avoid similar incidents, once it has been properly handled [66].

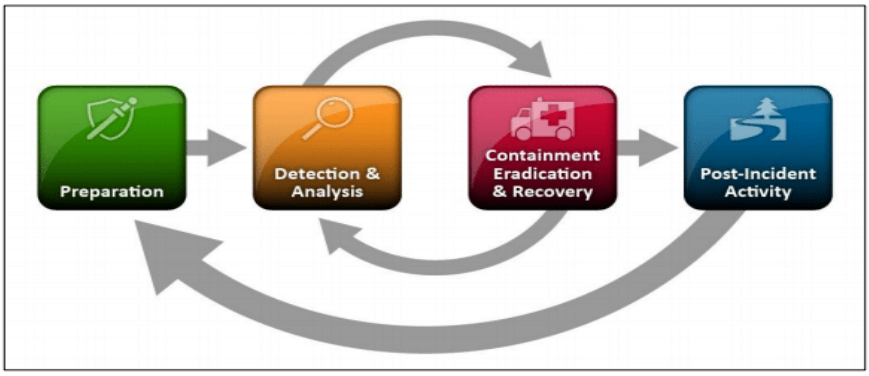

Fig. 1: Illustrates incident response life cycle. (Source: cynet.com)

10. DIGITAL FORENSICS INVESTIGATION PROCESS :

a) **Identification:** The first step in the forensic analysis of digital devices is to identify them. Searching for and identifying and documenting possible digital evidence is part of this process. Prioritizing evidence collecting based on volatility is an important part of this process, as it helps to ensure that evidence is gathered in the proper sequence. In order to get the greatest evidence possible, this minimizes the harm to the prospective evidence. Some digital storage spaces are difficult to be identified by the incident response specialists, forensic laboratory managers and digital evidence experts.

b) **Collection:** The second step is all about deciding whether or not to gather or acquire digital evidence that may be relevant to the case. As part of the collection phase, devices that may contain digital artefacts are gathered and brought to a laboratory for further analysis.

c) **Acquisition:** A bit to bit image, such as an entire HDD, partition, chosen data, and all acts and techniques are all part of the acquisition. The acquisition of a product should be recorded in detail for any changes that are necessary. To guarantee that a copy collected hasn't been tampered with in any way, the integrity of the data acquired is safeguarded.

d) **Preservation:** The final process is called Preservation. It is the process of ensuring that property is safe and secure without tampering with the data that is stored on devices and removable media. For digital artefacts to be relevant in an investigation, the preservation procedure must be established and maintained throughout the various stages of the process and for the acceptability of digital evidence in a court of law [67].

Fig. 2: Shows digital forensics investigation process.

11. DIGITAL FORENSICS PROCESS WITHIN THE INCIDENT RESPONSE LIFE CYCLE:

Incident Response (IR) and Digital Forensics (DF) are two independent process models with comparable aims. While both aim to investigate and contain computer security events, Incident Response is more concerned with restoring regular service, whereas Computer Forensics is more concerned with providing evidence that may be used in a justice system [68]. When a cyber event occurs within an organization, the first step is to establish whether or not the situation is concerning. If the triggered event is classified as significant, it enters the IR process and is further examined through Incident Analysis Validation, Incident Classification, and Incident Prioritization. After this procedure

is complete, the incident will be communicated to the organization's other departments, and the IR team will focus on incident containment, evidence collection, and forensic investigation, before concluding the process of eradication, recovery, and incident recording [69].

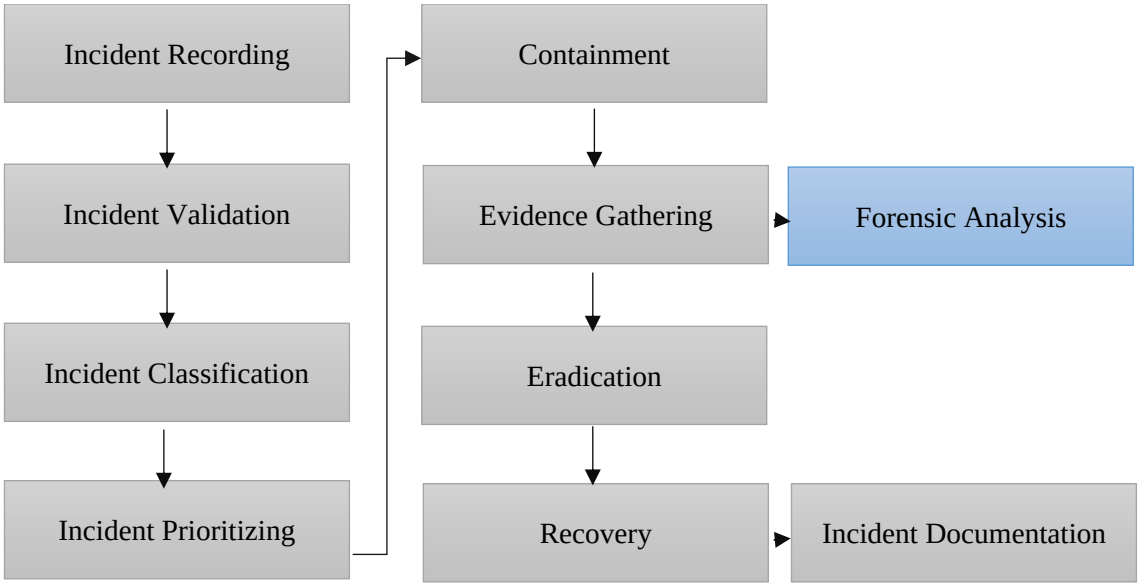

Fig. 3: Explains DF procedures within IR process. (Source: NIST)

12. NIST COMPUTER SECURITY INCIDENT HANDLING GUIDE 800-61 REVISION 2 :

The National Institute of Standards and Technology is a US government-funded organisation. With the exception of national security systems, NIST is in charge of establishing standards and recommendations, including minimum requirements, for maintaining effective information security for all agency operations and assets. The guide for managing computer security incidents 800-61 revision 2 aims to support organizations in reducing the risks associated with IT security events by giving applied instructions for successfully and efficiently reacting to occurrences. It offers suggestions for developing a successful incident response programme and major focus is on detecting, evaluating, prioritising, and dealing with problems [66]. Organizations are urged to adapt the suggested policies and solutions to their unique security and mission requirements.

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Fig. 4: Illustrates incident handling checklist. (Source: NIST)

13. EVIDENCE RETENTION PROCESS RECOMMENDATION OF NIST 800-61 :

According to NIST 800-61 recommendations, organizations should develop policies for the retention of evidence from incidents. The majority of organisations maintain all evidence for months or even years after an incident occurs. The following things should be taken into account while developing a policy [66]:

- Acquire tools and materials that may be useful in the event of an incident. If numerous tools and resources are already accessible to the team, they will be more efficient at addressing crises.
- Prevent mishaps by protecting the security of your networks, systems, and applications. Eliminating occurrences helps the organization while also easing the burden on the incident response team. Conducting frequent risk assessments and mitigating identified hazards effectively reduces the frequency of events.
- Warnings produced by different types of security software can be used to identify precursors and symptoms. Early identification of issues is aided by intrusion prevention and detection systems, file integrity checking software and an antivirus application. Different form of software has the capability to identify instances that the other software cannot, which is why it is strongly suggested to employ many types of computer security software.
- Establish channels for reporting events by third parties. External parties may choose to report issues to the organization. Organizations should make available a phone number and email address for reporting such instances to third parties.
- Require a good degree of auditing and logging on important systems. Operating system, service, and application logs usually include useful information during incident investigation, especially if auditing is allowed.
- Profiling establishes the features of predicted activity levels in order to facilitate the identification of variations in patterns. Whenever the profiling procedure is automated, anomalies from projected activity levels may be quickly discovered and reported to administrators, allowing for early detection of occurrences and operational issues.
- Maintain synchronisation of all host clocks. Event correlation gets more challenging when the devices reporting events utilise different time zones. Clock inaccuracies might also be problematic from an evidence viewpoint.
- Build and use a knowledge skill set. While incident analysts need rapid access to information, a centralised knowledge base offers a consistent, sustainable source of information. Antecedents and indications of prior occurrences, should be included in the knowledge base.
- Begin collecting data as soon as the team senses an event has happened. Each action done, from the moment an event is noticed until the time it is resolved, should be recorded and timestamped. This kind of information will be useful in court of law. Keeping track of the actions taken may also result in a more efficient, methodical, and error-free solution.
- Protect incident data. It often includes vital data about vulnerabilities, security loop-holes, and users who might have engaged in improper behaviour. Access to incident data should be adequately limited, both conceptually and physically.
- Prioritize incident management depending on relevant variables. Due to resource constraints, Incidents must not be dealt with on a first-come, first-served basis. Companies could instead develop written guidelines that specify how quickly the team must respond to an occurrence and what procedures should be taken, taking into account critical factors such as the incident's functional and informational impact, as well as the incident's projected recoverability.
- Include incident reporting provisions in the organization's incident response policy. Administrations must establish the kind of occurrences that must be reported, when they must be reported, and to whom they must be reported.
- Develop strategies and processes for incident containment. It is critical to control accidents swiftly and efficiently in order to minimise their impact on the company. Organizations should establish acceptable risks associated with incident containment and adopt appropriate methods and processes. Containment techniques should be tailored to the event nature.

- Adhere to established protocols for the collection and processing of evidence. The team should record in detail how every evidence was maintained. At all times, it is necessary to account for the evidence. To build evidence handling protocols, the group should engage with legal advisors and law enforcement agencies, and then develop procedures based on those discussions.
- Preserve the integrity of volatile data from systems and utilise it as proof. There is a list of network connections, processes, login sessions, open files, network interface settings, and the contents of the memory space in this portion of the log. Exercising caution in the execution of properly selected commands from dependable media may be sufficient to get the essential information without jeopardizing the integrity of the system's proof.
- When creating system snapshots, it is necessary to use whole forensic disc images rather just file system backups in order to assure that they are correct. Disc images should be created using write-protectable or write-once media that has been cleansed before being burned on a disc. When it comes to investigation and evidential reasons, this strategy is better than a file system backup in most situations. Additional advantages of image processing include the fact that analysing an image is far safer than analysing the underlying system, since the analysis may mistakenly impact the actual system if the picture has been altered.
- Following major incidents, have lessons-learned workshops to discuss what happened. Lessons learned meetings are particularly beneficial for enhancing security measures and the incident response process.

14. DATA INTEGRITY CONSTRAINTS ON SSD's DURING DIGITAL FORENSIC ANALYSIS :

In computing, a solid-state drive (also known as an SSD) is a solid-state device that saves data via the use of an electronic circuit assembly. It has no moving components, unlike the HDD; hence, it is mentioned as solid state. SSDs are powered by Flash memory. SSD is not a technological advancement of the HDD; instead, it is a whole new technology that replicates the properties of the HDD [70].

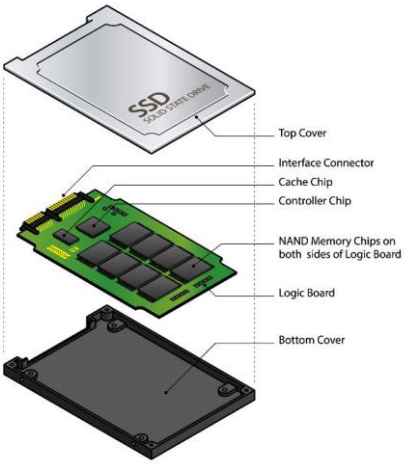

Fig. 5: Shows components of SSD. (Source: uwaterloo.ca)

14.1 SSD Concepts: As with any other storage medium, SSDs have a variety of functions such as erasing, rewriting, and other operations such as Wear Levelling, TRIM and Garbage Collection. These are explained as follows.

- **TRIM** is a method for deleting data from an SSD. It erases data blocks that have been designated as deleted. TRIM is an ATA command that communicates between the file and block levels, notifying the SSD of deleted files and notifying it to mark those pages as obsolete. Although reads and writes are bad for flash memory, the TRIM command tells the SSD to wait until the next block is wiped before rewriting data. This contributes to the SSD's increased lifespan. TRIM, in conjunction with

trash collection and the wear-levelling mechanism, all contribute to the SSD's increased lifespan [71].

- **Garbage Collection** is a critical step in SSDs since NAND devices cannot overwrite existing data and must go through an erase cycle. SSDs copy data first and then write it to blank pages in a separate block. The new block's cells are then deleted and fresh data is written [72].
- **Wear Levelling** is a protection mechanism that assures no NAND block is written or deleted more frequently than the others. This technique is used by manufacturers to prolong the life of their devices and counteract NAND flash degradation. Wear levelling ensures that data is distributed evenly across physical cells.

14.2 Challenges to overcome in SSD Forensics: SSD Forensics is not as basic as conventional hard disc drive forensics, which presents a challenge for forensics investigators [73].

- Wiping data using the Secure Erase approach eliminates digital evidence considerably more quickly than with an HDD [69].
- The evidence self-destruction procedure is initiated when the operating system issues the TRIM command to the SSD controller in response to the user deleting a file, formatting the drive, or deleting a partition. The TRIM process is totally linked with instructions at the partition and volume level. This covers disc formatting and partition deletion; file system commands for data truncation and compression; and System Restore (Volume Snapshot) procedures [74].

Several stages are followed by the investigator during the investigation of a cyber event. The first step is to do live forensics of volatile data, followed by powering down the computer system and disconnecting the SSD from the suspicious PC. After that, a write-blocker will be connected and imaging will be conducted to assure file integrity using hashing algorithm. Because SSD data recovery is difficult due to the fact that it does not save data after erasure, it is a difficult process. In SSD, examining fragmented data is similarly a challenging operation, and it takes the investigator longer to complete the investigation. To liberate up space, TRIM and Garbage Collection functions wipe the SSD clean. Even if data can be recovered using the SSD's factory default features, self-corrosion wipes up all residual data traces [75]. This capacity is so robust that data destruction will resume when the system is switched back on, even if the system is shut down or powered off. The device will work even if it is linked to a write-blocking imaging device. The TRIM command, which is issued to the SSD controller by the operating system whenever the user reformats the drive or erases a file or partition, triggers self–destruction [76].

15. THE NEED TO UPDATE NEW CHALLENGES FACED IN DIGITAL FORENSIC AQUISITION AND THE IMPORTANCE OF CYBER SECURITY FRAMEWORK IN AN ORGANIZATION :

When investigating a crime, it is important to adhere to and refer to device or information systems forensics rules. Although specific procedures, processes, and controls may be retained by nations, organisations, and individual investigators, standardisation is intended to the acceptance of comparable, if not similar, methods globally. This makes it easy to compare, integrate, and differentiate the findings of such investigations, even when they are carried out by different persons or groups in various jurisdictions. Investigative standards should be followed by forensic examiners, and all cases should be treated as though they would end up in court. This entails using sufficient rigour in the collecting and preservation of digital evidence in order to defend the evidence's credibility. An integrated application of forensics standards has a variety of benefits, including comprehensiveness and an increase in the quality as well. Introducing one forensic standard before the other, or using both forensic standards at the same time, may benefit forensic investigators [77]. There are hundreds of different information security framework options available today, but the NIST Cybersecurity Framework is swiftly becoming the industry standard [78][79]. However, from the data presented in this paper, it is evident that the NIST 800-61, which governs the forensic analysis technique of the incident response process, does not define data acquisition from SSDs to ensure data integrity which is very crucial in the digital forensic investigation process.

16. RESEARCH PROBLEM CONSIDERED FOR FURTHER RESEARCH :

CSF's must be synced with the latest developments in data storage technology, both volatile and non-volatile, since they will be critical for both law enforcement agencies and business organisations in the future. In the event that there is a discrepancy between the CFS's and the obstacles experienced in digital forensics analysis, new adversaries will emerge since there will be no guidelines in place on how to deal with these concerns. Current and future research should be focused on integrating both components, such as developing technology constraints in digital forensic analysis, as well as incorporating such problems with specified processes inside CSF's like NIST 800-61.

17. ABCD ANALYSIS OF RESEARCH PROBLEM :

ABCD model studies are based on four constructs: advantages, benefits, constraints, and disadvantages. By examining the fundamental concerns and defining the essential component aspects, this approach examines and analyses all determinants in key areas [80].

Table 2: ABCD Analysis

Advantages	CSF is essential for an organization to deal with cyber security threats in an efficient manner. • Provide long-term security and risk management capabilities. • There are ripple effects that occur across supply chains and vendor lists. • Bridging the gap between scientific and business-oriented parties. • The Framework's versatility and adaptability are key features. • Designed to satisfy regulatory and compliance standards in the future.
Benefits	CSF plays a critical role in the establishment and maintenance of unexpected cyber circumstances, providing firms with a competitive advantage against cyber criminals. • The identify function assists an organisation in identifying the current cyber contact points in a company's operating environment. These might include IT assets, resources, information, and other types of information. • Protect: This one is responsible for access control, data security, data validity, and maintenance in order to ensure that the cybersecurity is maintained in and around the company's facilities. Most likely, it is a phase of business cybersecurity that is proactive in nature. • Monitoring logs and taking care of intrusion detection methods at the network and device level are two ways in which a company might uncover possible breaches. This technique covers the administration of security information and events, among other things. • Respond: Once a breach has been discovered, businesses must take care of the response method, which includes determining the nature of the breach, repairing the vulnerability, and moving on with the recovery. • Recovery: During this stage of the cybersecurity framework strategy, methods for recovery, such as disaster recovery systems and backup plans, will be addressed.
Constrains	• The CSF is a set of recommendations or an optional advice that businesses may use to better manage and minimise cybersecurity risk. • It's based on standards, norms, and practises, and it's meant to assist them. • Investigation, research, and creation of CSFs in response to evolving threats are time-consuming and costly endeavours that need specialised knowledge.

Disadvantages	• The majority of the CSF need years, if not decades, of updating with latest trend in technologies (such as SSD Forensics). • Time-consuming procedures such as bureaucratic committees, public comment periods, and modifications are required. • In the case of rules and regulations, various stakeholders might hinder the implementation of swift changes in government policy [81].

18. CONCLUSION :

CSF is very significant in the management and protection of an organization's information technology infrastructure. NIST is one of the most extensively acknowledged and used CSFs in the world. The NIST defines critical parts of cyber security measures that most firms integrate into their playbook and implement. However, in the same way that we watch the application of the NIST framework, it should also be highlighted that it is important to stay on top of the latest and most promising technologies. In this study, we discussed the difficulties encountered in the acquisition of SSD forensics, as well as the importance of data integrity in the acquisition of digital forensics. The NIST 800-61 does not clearly suggest strategies to alleviate this problem. However, it should be highlighted that the National Institute of Standards and Technology (NIST) has not yet produced an updated regulatory framework to minimize these difficulties. According to the findings of this literature review article, CSFs should be updated on a regular basis to integrate data integrity methods in digital forensics and incident response whenever new technology is introduced.

REFERENCES :

[1] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147. Google Scholar↗

[2] Shah, Z., Mahmood, A. N., & Slay, J. (2014, September). Forensic potentials of solid-state drives. In *International Conference on Security and Privacy in Communication Networks*, 113-126. Google Scholar↗

[3] Kumar, M. (2021). Solid state drive forensics analysis—Challenges and recommendations. *Concurrency and Computation: Practice and Experience*, *33*(24), 22-42. Google Scholar↗

[4] Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy*, *3*(2), 258-283. Google Scholar↗

[5] Dedeke, A. (2017). Cybersecurity framework adoption: using capability levels for implementation tiers and profiles. *IEEE Security & Privacy*, *15*(5), 47-54. Google Scholar↗

[6] Gourisetti, S. N. G., Mylrea, M., Ashley, T., Kwon, R., Castleberry, J., Wright-Mockler, Q., & Brege, G. (2019, November). Demonstration of the cybersecurity framework through real-world cyber-attack. *In 2019 Resilience Week (RWS)*, 19-25. Google Scholar↗

[7] Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417-432. Google Scholar↗

[8] Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531-540. Google Scholar↗

[9] Oyelami, J. O., & Kassim, A. M. (2020). Cyber security defence policies: A proposed guidelines for organisations cyber security practices. *International Journal of Advanced Computer Science and Applications*, *11*(8), 1-8. Google Scholar↗

[10] Githinji, S. (2021). Digital Forensics Policies for Forensics Readiness in Organizations. *Journal of Language, Technology & Entrepreneurship in Africa*, *12*(2), 172-186. Google Scholar↗

[11] Pathak, J., Sankaran, S., & Achuthan, K. (2019, December). A SMART Goal-based Framework for Privacy Preserving Embedded Forensic Investigations. In *2019 9th International Symposium on Embedded Computing and System Design (ISED)*, 1-5. Google Scholar↗

[12] Sav, U. M., & Magar, G. (2019). Cyber Security Policies for User's Anomalous Behaviour At Workplace. *International Journal of Advance and Innovative Research*, *1*(6), 363-367. Google Scholar↗

[13] Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, *15*(4), 1035-1052.Google Scholar↗

[14] Joshi, B. R., & Hubbard, R. (2016, May). Forensics analysis of solid state drive (SSD). In *2016 Universal Technology Management Conference (UTMC)*, 1-12. Google Scholar↗

[15] Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, *14*(2), 346-376. Google Scholar↗

[16] Nikkel, B. (2016). NVM express drives and digital forensics. *Digital Investigation*, *16*(1), 38-45. Google Scholar↗

[17] Barbara, J. (2014). Solid state drives: Part 5. *Forensic Magazine*, *11*(1), 30-31. Google Scholar↗

[18] Roussev, V. (2016). Digital forensic science: issues, methods, and challenges. *Synthesis Lectures on Information Security, Privacy, & Trust*, *8*(5), 1-155. Google Scholar↗

[19] Jazzar, M., & Hamad, M. (2022). Comparing HDD to SSD from a Digital Forensic Perspective. In *Proceedings of International Conference on Intelligent Cyber-Physical Systems*, 169-178. Google Scholar↗

[20] Luciano, L., Baggili, I., Topor, M., Casey, P., & Breitinger, F. (2018, August). Digital forensics in the next five years. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 1-14. Google Scholar↗

[21] Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods. *Lontar Komputer: Jurnal Ilmiah Teknologi Informasi*, *3*(9), 169-181.Google Scholar↗

[22] Bell, G. B., & Boddington, R. (2010). Solid state drives: the beginning of the end for current practice in digital forensic recovery? *Journal of Digital Forensics, Security and Law*, *5*(3), 1-17. Google Scholar↗

[23] Gibson, M., Medina, N., & Nail, Z. (2020). SSD forensics: Evidence generation and analysis. In *Digital Forensic Education*, *1*(1), 203-218. Google Scholar↗

[24] Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1), 26-37. Google Scholar↗

[25] Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, *4*(1), 14-19. Google Scholar↗

[26] Ramadhan, R. A., Setiawan, P. R., & Hariyadi, D. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037: 2012 and NIST SP800-86 Framework. *IT Journal Research and Development*, *6*(2), 162-168. Google Scholar↗

[27] Göbel, T., Maltan, S., Türr, J., Baier, H., & Mann, F. (2022). ForTrace-A holistic forensic data set synthesis framework. *Forensic Science International: Digital Investigation*, *40*(1), 301-314. Google Scholar↗

[28] Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*, *10*(1), 11065-11089. Google Scholar↗

[29] Riadi, I., Sunardi, S., & Fitri, F. T. (2022). Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method. *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, *6*(1), 108-117. Google Scholar↗

[30] Rachman, H., Sugiantoro, B., & Prayudi, Y. (2021). Forensic storage framework development using composite logic method. *ILKOM Jurnal Ilmiah*, *13*(1), 58-66. Google Scholar↗

[31] Ninahualpa, G., Yugcha, M., Gálvez, C., Guarda, T., Díaz, J., & Piccirilli, D. (2021, March). Carvers Suite–Smart Application for Data Recovery in SSD. In *World Conference on Information Systems and Technologies*, 450-460. Google Scholar↗

[32] Nnoli, H., Lindskog, D., Zavarsky, P., Aghili, S., & Ruhl, R. (2012, September). The governance of corporate forensics using COBIT, NIST and increased automated forensic approaches. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, 734-741. Google Scholar↗

[33] Nordvik, R., Stoykova, R., Franke, K., Axelsson, S., & Toolan, F. (2021). Reliability validation for file system interpretation. *Forensic Science International: Digital Investigation*, *37*(1), 30-41. Google Scholar↗

[34] Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, *9*(8), 38-44. Google Scholar↗

[35] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *AIRCC's International Journal of Computer Science and Information Technology*, *3*(3), 17-31. Google Scholar↗

[36] Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1-12. Google Scholar↗

[37] Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence*, *2*(2), 1-20. Google Scholar↗

[38] Kyei, K., Zavarsky, P., Lindskog, D., & Ruhl, R. (2012, October). A review and comparative study of digital forensic investigation models. In *International conference on digital forensics and cyber crime*, 314-327. Google Scholar↗

[39] Wazid, M., Katal, A., Goudar, R. H., & Rao, S. (2013, April). Hacktivism trends, digital forensic tools and challenges: A survey. In *2013 IEEE Conference on Information & Communication Technologies*, 138-144. Google Scholar↗

[40] Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. *digital investigation*, *7*(2), 14-27. Google Scholar↗

[41] Halboob, W., Mahmod, R., Udzir, N. I., & Abdullah, M. T. (2015). Privacy levels for computer forensics: toward a more efficient privacy-preserving investigation. *Procedia Computer Science*, *56*(1), 370-375. Google Scholar↗

[42] Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security*, *23*(1), 12-16. Google Scholar↗

[43] Bennett, D. (2012). The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. *Information Security Journal: A Global Perspective*, *21*(3), 159-168. Google Scholar↗

[44] Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy*, *1*(4), 15-23. Google Scholar↗

[45] Kumari, N., & Mohapatra, A. K. (2016, March). An insight into digital forensics branches and tools. In *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 243-250. Google Scholar↗

[46] Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147-167. Google Scholar↗

[47] Alzaabi, M., Taha, K., & Martin, T. A. (2015). CISRI: A crime investigation system using the relative importance of information spreaders in networks depicting criminals communications. *IEEE Transactions on Information Forensics and Security*, *10*(10), 2196-2211. Google Scholar↗

[48] Shrivastava, G. (2016, March). Network forensics: Methodical literature review. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 2203-2208. Google Scholar↗

[49] Vlachopoulos, K., Magkos, E., & Chrissikopoulos, V. (2012). A model for hybrid evidence investigation. *International Journal of Digital Crime and Forensics (IJDCF)*, *4*(4), 47-62. Google Scholar↗

[50] Mohite, M. P., & Ardhapurkar, S. B. (2015, April). Design and implementation of a cloud based computer forensic tool. In *2015 Fifth International Conference on Communication Systems and Network Technologies*, 1005-1009. Google Scholar↗

[51] Yasin, M., & Abulaish, M. (2013). DigLA–A Digsby log analysis tool to identify forensic artifacts. *Digital Investigation*, *9*(4), 222-234. Google Scholar↗

[52] Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, *1*(2), 2-7. Google Scholar↗

[53] Nicholson, A., Watson, T., Norris, P., Duffy, A., & Isbell, R. (2012, July). A taxonomy of technical attribution techniques for cyber-attacks. In *European conference on information warfare and security*, 1-8. Google Scholar↗

[54] Cohen, M. I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the enterprise. *digital investigation*, *8*(1), 101-110. Google Scholar↗

[55] Vömel, S., & Freiling, F. C. (2011). A survey of main memory acquisition and analysis techniques for the windows operating system. *Digital Investigation*, *8*(1), 3-22. Google Scholar↗

[56] Shosha, A. F., Tobin, L., & Gladyshev, P. (2013, May). Digital forensic reconstruction of a program action. In *2013 IEEE Security and Privacy Workshops*, 119-122. Google Scholar↗

[57] Latzo, T., Palutke, R., & Freiling, F. (2019). A universal taxonomy and survey of forensic memory acquisition techniques. *Digital Investigation*, *28*(1), 56-69. Google Scholar↗

[58] Marturana, F., Me, G., Berte, R., & Tacconi, S. (2011, November). A quantitative approach to triaging in mobile forensics. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, 582-588. Google Scholar↗

[59] Luoma, V. M. (2006). Computer forensics and electronic discovery: The new management challenge. *Computers & Security*, *25*(2), 91-96. Google Scholar↗

[60] Dahbur, K., & Mohammad, B. (2013). Toward understanding the challenges and countermeasures in computer anti-forensics. In *Cloud Computing Advancements in Design, Implementation, and Technologies*, 176-189. Google Scholar↗

[61] Law, F. Y., Chan, P. P., Yiu, S. M., Chow, K. P., Kwan, M. Y., Hayson, K. S., & Lai, P. K. (2011, May). Protecting digital data privacy in computer forensic examination. In *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 1-6. Google Scholar↗

[62] Reddy, K., & Venter, H. (2009, January). A forensic framework for handling information privacy incidents. In *IFIP International Conference on Digital Forensics*, 143-155. Google Scholar↗

[63] Rekhis, S., & Boudriga, N. (2011). A system for formal digital forensic investigation aware of anti-forensic attacks. *IEEE transactions on information forensics and security*, *7*(2), 635-650. Google Scholar↗

[64] Liu, Y., Jiang, L., Liu, T., & Zhang, Y. (2021, April). Image Electronic Evidence Screening Based on Improved SSD. In *2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)*, 674-680. Google Scholar↗

[65] Alhasan, H., Chen, Y. C., & Ho, C. C. (2021, July). RVO: Unleashing SSD's Parallelism by Harnessing the Unused Power. In *2021 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, 1-6. Google Scholar↗

[66] Spring, J. M., & Illari, P. (2021). Review of human decision-making during computer security incident analysis. *Digital Threats: Research and Practice*, *2*(2), 1-47. Google Scholar↗

[67] Ajijola, A., Zavarsky, P., & Ruhl, R. (2014, December). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev. 1: 2014 and ISO/IEC 27037: 2012. In *World Congress on Internet Security (WorldCIS-2014)*, 66-73. Google Scholar↗

[68] Johnson, L. R. (2014). Forensics process. *Computer Incident Response and Forensics Team Management*, *37*(1), 97-106. Google Scholar↗

[69] Reddy, N. (2019). *Solid state device (SSD) forensics in Practical Cyber Forensics:* Berkeley: Apress, 379-400. Google Scholar↗

[70] Sliwa, C. (2018, February 13). What is SSD trim? - definition from whatis.com. SearchStorage. Retrieved on April 16, 2022, from https://www.techtarget.com/searchstorage/definition/TRIM

[71] Tokar, L. (2022). Garbage Collection and TRIM in SSDs Explained – An SSD Primer - The SSD Review. The SSD Review. Retrieved on 16 April 2022, from https://www.thessdreview.com/daily-news/latest-buzz/garbage-collection-and-trim-in-ssds-explained-an-ssd-primer/.

[72] Benusa, A., Jeganathan, S., & Schmidt, M. (2016). Forensic Analysis Challenges: Shifting from Hdd to Ssd Storage. *Journal Of Information System Security*, *12*(3), 131-149. Google Scholar↗

[73] Focus, F. (2022). Recovering Evidence from SSD Drives in 2014: Understanding TRIM, Garbage Collection and Exclusions - Forensic Focus. Forensic Focus. Retrieved on 16 April 2022, from https://www.forensicfocus.com/articles/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/.

[74] Fernando, V. (2021, April). Cyber forensics tools: A review on mechanism and emerging challenges. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1-7. Google Scholar↗

[75] Aldaej, A., Ahamad, M. G., & Uddin, M. Y. (2017, March). Solid state drive data recovery in open-source environment. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, 228-231. Google Scholar↗

[76] What Is A Cybersecurity Framework And Why Is It Important For Your Organization? – Secure Sense. Secure Sense. (2022). Retrieved on 16 April 2022, from https://securesense.ca/what-cybersecurity-framework-important-your-organization/.

[77] Cybersecurity Frameworks Around the World - MSSP Alert. MSSP Alert. (2022). Retrieved on 16 April 2022, from https://www.msspalert.com/cybersecurity-news/cybersecurity-frameworks-around-the-world/.

[78] Cybersecurity Frameworks; The Complete Guide - (2022). Retrieved on 16 April 2022, from https://preyproject.com/blog/en/cybersecurity-frameworks-101/.

[79] Aithal, P. S. (2016). Study on ABCD analysis technique for business models, business strategies, operating concepts & business systems. *International Journal in Management and Social Science*, *4*(1), 95-115. Google Scholar↗

[80] When Will Security Frameworks Catch Up With the New Cybersecurity Normal?. Dark Reading. (2022). Retrieved on 16 April 2022, from https://www.darkreading.com/endpoint/when-will-security-frameworks-catch-up-with-the-new-cybersecurity-normal-.

[81] Nicole.keller@nist.gov. (2021, June 2). *Framework update process*. NIST. Retrieved on April 16, 2022, from https://www.nist.gov/cyberframework/online-learning/update-process

****