International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

Article – e002

FORENSIC CHIP OFF ACQUISITION OF NOR FLASH MEMORY IN EMBEDDED DEVICES

Aaditi Dawle[1], **Ashish Ranjan**[2], **Tanushri Johari**[3]

[1] *Master of Science, Forensic Science, Oriental University, Indore, Madhya Pradesh, India*
[2,3] *Assistant Professor, Forensic Science, Oriental University, Indore, Madhya Pradesh, India*

Received: 2026-08-16 **Revision Received:** 2026-09-10 **Accepted:** 2026-09-23

ABSTRACT

In digital forensics, the most important element is data; it can be any information such as images, documents, log files, and user credentials stored in a device. As our world moves forward, the digital devices are also advancing with technological developments, evolving from early computing systems such as ENIAC to modern flash-memory-based storage, whereas the data has become more fragile and prone to attackers. This review examines the application of Chip-off Acquisition on NOR Flash Memory in embedded devices. To prevent data recovery, digital devices are encrypted, physically damaged, or broken. Recovering data from these devices is a difficult aspect, as many challenges occur during the process. Traditional methods such as live acquisition, logical acquisition, and JTAG extraction have several limitations such as altering volatile data, requiring an active debug port etc. To overcome this issue Chip-off Acquisition is used. It is a hardware level data extraction technique involving removal of the chip, cleaning it, reading the raw data using a chip reader and processing the extracted raw data into the specialized software. Data from NAND Flash memory has been recovered by performing the acquisition, which has been studied. Chip-off Acquisition is also applicable to NOR Flash Memory. However, research specifically on NOR flash memory on various devices remains limited.

KEYWORDS: Chip-off Acquisition, Nor Flash Memory, Digital Devices

1. INTRODUCTION

The evolution of digital devices from the 1830s to the 21st century has involved many advancements in technology. It involves [1]

- 1830: Charles Babbage designed the first automatic digital computer
- 1880 - 1920: Herman Hollerith developed punched card machines

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

- 1930: Konard Zuse in Germany and John Stibitz at Bell Labs developed early binary calculators
- 1946 - 1960: ENIAC (Electronic Numerical Integrator and Computer) was first developed, an invention of transistors and IC
- 1990 - 2019: The World Wide Web became public, in 2007 the launch of iPhone
- 2020: Portable devices, AI, and IoT

Digital devices such as laptops, smartphones, smartwatches, mobile phones, and internet-based communication systems dominate everyday life [2] and are prone to being exploited by attackers involved in cybercrimes such as hacking, illegal surveillance, tampering and network attacks[3], here digital forensics plays a pivotal role involving the identification, preservation, acquisition, analysis and presentation of digital evidence [4].

Chip-off Acquisition is a hardware level data extraction technique involving the process of removing flash memory, cleaning it, analyzing it in a Chip reader and processing the extracted data into specialized software. Chip-off acquisition can be performed even when the device is non-functional.[5].

1.1 Solid State Storage:

It is a type of storage medium that stores the data and code in embedded devices. It can store data without a power supply. It can be erased and reprogrammed electrically which is frequently used in SD cards and USB flash devices. It is a revolutionized form of EEPROM; the only difference is that flash memory can be read and written, but erased at only block level. It often follows 12C or SPI protocol, which helps to communicate between two devices or chips [6].

.

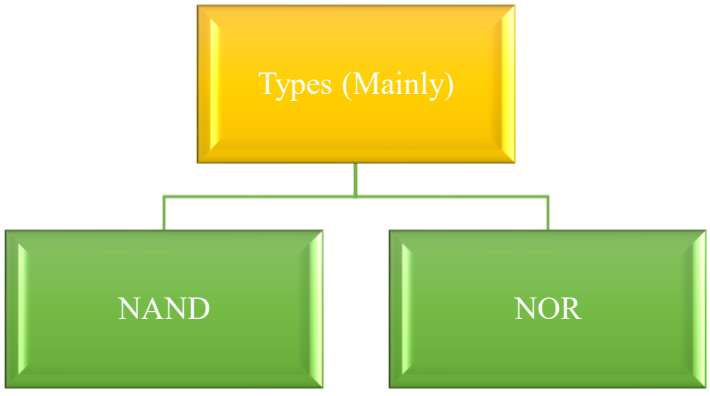


Fig 1.1: Classification of types of memory

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

1.1.1NAND Flash Memory:

- The invention of NAND by Toshiba Corp. In 1987 allowed only blocks of data to be streamed in or out. Cell designs are made in such a way that NAND flash memory becomes denser than NOR.
- It is arranged in pages and blocks.
- The cells are organized serially.
- It contains 4 times the design rules of the chip.
- SanDisk and Toshiba introduced the first MLC NAND storage medium in 2008.
- Digital photography and digital storage are the reasons that led to the invention of NAND [7].
- NAND flash memory operation: The flash forms a channel of columns and rows. Each channel holds two transistors, i.e., a floating gate and a control gate, separated by thin oxide layer.
- This procedure requires voltage; the condition of memory will remain charged or drained when the power supply is removed. This is what makes the chip non-volatile.

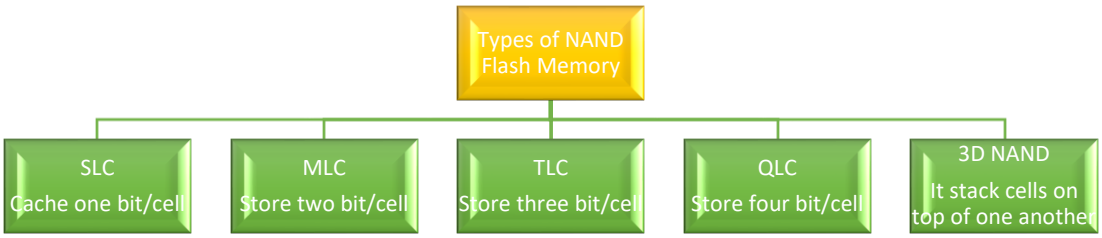


Fig 1.2: Classification of types of NAND Flash Memory

1.1.2 NOR Flash Memory:

- Intel first developed NOR Flash Memory in 1988.
- It transfers efficiently at short range from 1 to 104 MB, and at this rate, it is cost effective.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

- NOR has separate address lines and data lines, similar to SRAM, the data lines are connected to NOR cells.
- The storage density capacity of NOR is low, so storing a bit will cost more.
- The addition of 5G station is a boon for NOR flash memory.
- NOR flash memory is used in applications ranging from car cameras to driver-assistance systems.
- NOR flash supports both reading and writing
- Compared to NAND, the reading capacity is greater in NOR [8].

The objective of this paper is to use chip-off Acquisition of NOR Flash Memory from embedded devices. This study focuses on how chip-off can recover data from the devices that are physically damaged, burned or encrypted.

2. REVIEW OF LITERATURE

A review of literature shows that the studies have been grouped into 7 categories: studies related to recent advancements in Chip-Off Recovery, NOR Flash Systems and Digital Forensics; studies related to recent developments in mobile device data extraction and analysis; studies related to integrated perspective on Flash memory, Digital Forensics and eSIM techniques; studies related to emerging trends in Digital Evidence Extraction and NOR Flash Memory Applications; studies related to NOR Flash Technologies, CCTV Forensics, and Smartphone Chip-Off Analysis, Study related to IoT Security, Network Routing Mechanisms, and Embedded Monitoring Systems; and studies related to Review of Network-on-Chip Protection Mechanisms and Mobile Evidence Acquisition Techniques. However, fewer studies directly show the data extraction from devices and NAND Flash Memory through Chip-Off Acquisition, which helps in the present study.

2.1 *Study related to recent advancements in Chip-Off Recovery, NOR Flash Systems and Digital Forensics*

The first group of literature focuses on advanced Chip-off acquisition, NOR flash technology and digital forensic recovery. This work establishes a framework for selecting appropriate recovery techniques for damaged HDDs, experimentally validating chip-off Acquisition for recovering data from damaged NAND flash memory, examining the electrical characteristics of NOR Flash Memory to improve the CIM working, and developing the NF2FS file system to enhance NOR Flash efficiency while focusing on CCTV evidence recovery.

The major contribution of this literature is that it includes experimental validation, advanced recovery methodologies, enhancement of NOR flash performance, and forensic workflows. Most studies focus on NAND Flash memory, HDDs, or specific surveillance systems such as Hikvision and Dahua with limited focus on embedded systems using NOR Flash Memory. However, greater attention is needed in the areas of firmware extraction, integrity of evidence, and systematic Acquisition procedures. Overall, this literature demonstrates

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

practicable chip-off Acquisition and highlights the development of procedures that are less destructive for NAND Flash drives.

2.2 Study related to recent developments in mobile device data extraction and analysis

A second major group of literature focuses on mobile forensic data recovery. This literature evaluates the capabilities of Cellebrite UFED for extracting and analyzing data from functional mobile devices, while also focusing on recovering data from non-functional Android devices using data carving and chip-off acquisition. It performs both logical and physical acquisition, employing a four - stage workflow i.e., dismantling, removal of the chip, Acquisition of data and data carving.

The strength of this literature lies in the comprehensive extraction capabilities of UFED, including deleted file recovery, support for decryption, accommodating multiple devices while emphasizing legal considerations such as protection of privacy and maintaining chain of custody. These studies depend heavily on software-based approaches and provides limited validation on devices with encryption and damaged devices.

The literature also emphasizes AI driven forensic tools that can navigate complex data on mobile devices and improve support for encryption mechanisms.

2.3 Study related to Integrated Perspective on Flash Memory, Digital Forensics and eSIM Techniques

A third category of literature contributes to the advancement of flash memory technology. It aims to review the current status and challenges of charge trap flash memory, focusing on the architecture and future storage mechanisms in NOR and NAND memory. Alternatively, it provides a theoretical overview of cyber and digital forensics practices. It also proposes a procedure for investigating eSIM technology within IoT environments.

These studies are valuable because they provide a comprehensive review of flash memory architecture and fabrication processes, adopts a conceptual framework to examine digital and current practices, and develops a procedure for the examination of eSIM components.

Another contribution of the literature is that it provides an in-depth understanding of flash memory technologies and identifies innovations in storage technology. It also highlights the importance of forensic expertise, software updates and training programs.

However, none of the studies contributes to validating chip-off Acquisition for NOR flash memory; it primarily focuses on the architecture of memory rather than recovery acquisition. This is where the present paper can contribute a narrow and more targeted argument.

2.4 Study related to Emerging Trends in Digital Evidence Extraction and NOR Flash Memory Applications

A fourth group of literature examines a systematic chip-off procedure for Ball Grid Array integrated circuits used in digital investigation. It focuses on exploiting 3D NOR flash memory for CIM to accelerate general purpose matrix multiplication and investigates structural design and performance of 3D NOR flash memory devices.

This literature is highly relevant to the proposed study because it proposes a 6-stage workflow: dismantling, identification, removal, restoration, determination and data extraction. It also evaluates and develops a 3D NOR flash-based analog CIM architecture using a large-

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

scale memory array. It provides practical methodology that can guide an investigator during the Chip-off procedure. It demonstrates the versatility of NOR flash memory beyond storage mechanisms by achieving high-performance computing. It also contributes significantly to NOR flash memory architecture by improving the standard of speed, performance of erasing and integration of device.

Despite this contribution, human error remains a concern; much of this literature focuses on memory design rather than as the core research object.

2.5 Study related to NOR Flash Technologies, CCTV Forensics, and Smartphone Chip-Off Analysis

A fifth group of literature demonstrates significant progress in NOR flash memory and embedded device forensics. It focuses on evaluating the radiation tolerance of commercial NOR flash memories for space applications. It also emphasizes the forensic application of CCTV DVR evidence by comparing proprietary file extraction with playback video recording. It proposes a comprehensive workflow for acquiring and analyzing CCTV evidence across multiple manufacturers, highlighting challenges and diverse storage formats. Most studies concentrate on specific applications such as smartphones, CCTV systems, and hardware.

This literature also provides a valuable framework for examination of SSDs but its conceptual nature limits experimental verification. It demonstrates reliability of NOR flash memory under harsh conditions, improves CCTV evidence acquisition, proposes standardized methodologies, improving hardware authentication, and validates chip-off Acquisition for mobile devices.

2.6 Study related to IoT Security, Network Routing Mechanisms, and Embedded Monitoring Systems

A sixth group of literature examines the security and challenges in IoT environments, reviews the evolution and application of embedded flash memory technologies and presents practical techniques for router management including IOS backup and restoration. It also proposes an efficient NoC router architecture to improve data transmission while introducing an API based live forensic approach for Mikrotik RouterOS and developing a Linux - based embedded DVR monitoring system.

The literature adopts architectural analyses, development of frameworks, implementation of experimental systems, and practical approaches. The major strengths include identifying challenges in IoT forensics, improvements in management and architecture of routers and enabling live router data acquisition. These studies provide relevant technological insights that support digital investigation.

However, the literature has some notable restrictions. It mostly focuses on architecture of systems, performance of networks, or management of devices. It also addresses the use of live Acquisition rather than chip-off acquisition. The future direction includes integrating firmware extraction, verification of evidence integrity and AI assisted forensic techniques.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

2.7 Study related to Review of Network-on-Chip Protection Mechanisms and Mobile Evidence Acquisition Techniques

A seventh major group of literature develops an open-source software for coding and analyzing visual and acoustic readings, focused on enhancing the security of NoC routers by implementing countermeasures against routing table attacks. It provides a comprehensive overview of mobile forensic process, evidence acquisition, analysis and admissibility of evidence in court.

It supports multimedia analysis tools, security mechanisms, and a systematic model that addresses both technical and legal aspects of mobile forensics. However, their limitations are evident, as they primarily focus on multimedia annotation rather than acquisition, emphasizing network security without considering digital recovery.

The future research direction integrates with multimedia analysis, secures hardware architecture, and addresses the growing complexity of embedded systems and IoT devices.

2.8 Research Gap

The review of literature supports the principle of Chip-off Acquisition on devices, but a specific research gap remains as the application is only applied to mobile phones and NAND Flash Memory. Most studies are based on concepts that are not practically applied. Most studies discuss how Chip-off Acquisition works on Android phones, recovery of data through NAND Flash Memory or mobile evidence Acquisition techniques rather than extraction of data from NOR Flash Memory using Chip-off Acquisition.

This research gap can help in introducing a new framework for NOR Flash Memory, which can store BIOS firmware, operational code and other evident data. The present study, therefore, builds upon the past work while narrowing the focus to a more specific objective by summarizing the Forensic Chip-Off Acquisition of NOR Flash Memory in embedded devices and identifying types of artifacts in devices as evidence.

Table 1.1: Comparison of Literature Review

Literature Review	Work focused on or findings of the study	Key trends	Limitations	Future research direction
Recent Advancements in Chip-Off Recovery, NOR Flash Systems and Digital Forensics	Proposing an approach for data recovery processes and investigating the fundamental electrical mechanisms driving non-ideal current behavior in NOR Flash based compute-in-memory	Combination of hybrid recovery methods, standard procedures for recovery of data from NAND memory, development of NOR Flash File System.	Small sample size, demonstrated on single flash drive, focused on hardware recovery rather than forensic data recovery practically, and limited to Hikvision and Dahua	Future automation using AI-driven decision support systems in digital forensics and the development of less destructive methods for NAND Flash drives.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

	arrays.		surveillance systems only.	
Study related to recent developments in mobile device data extraction and analysis	The data extraction process was made easier by using different devices to check the complexity of these techniques through specialized software and techniques and this study also compares various tools used for data carving as well as highlights the challenges involved in the forensic analysis of mobile devices.	Increased reliance on mobile forensic tools for data extraction, use of chip-off and data carving techniques, recovery of encrypted, deleted and hidden data.	It does not work when the phone is encrypted or system updates, expensive hardware, Chip-off Acquisition is a destructive process.	AI driven forensic tools can navigate complex data on mobile devices and improving support for encryption mechanisms.
Study related to integrated perspective on Flash memory, Digital Forensic and eSIM techniques	Suggesting directions for future storage devices based on the ionic mechanism, which may overcome the inherent problems of flash memory devices and developing flowchart for the understanding of forensic scientists.	Advancement of charge trap flash memory, evolution of digital forensic tools, focuses on eSIM and IoT devices.	3D NAND layers create fabrication challenges, limited standard forensic methodologies for eSIM and IoT systems.	Developing adaptive forensic software, standardized methods for eSIM and evidence extraction technique.
Study related to emerging trends in Digital Evidence Extraction and NOR Flash Memory Applications	Demonstrating the potential of NOR Flash memory beyond storage applications and showing that the proposed method improves the architecture and performance of	Development of chip-off method for BGA IC devices, CIM for AI acceleration, enhancement of 3D NOR Flash architecture.	Human error, methodology is not suitable for all devices, worked on prototype architecture rather than commercial systems, limited NOR Flash	Validating methodology across wide range of devices, reducing human intervention, optimization of the fabrication process.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

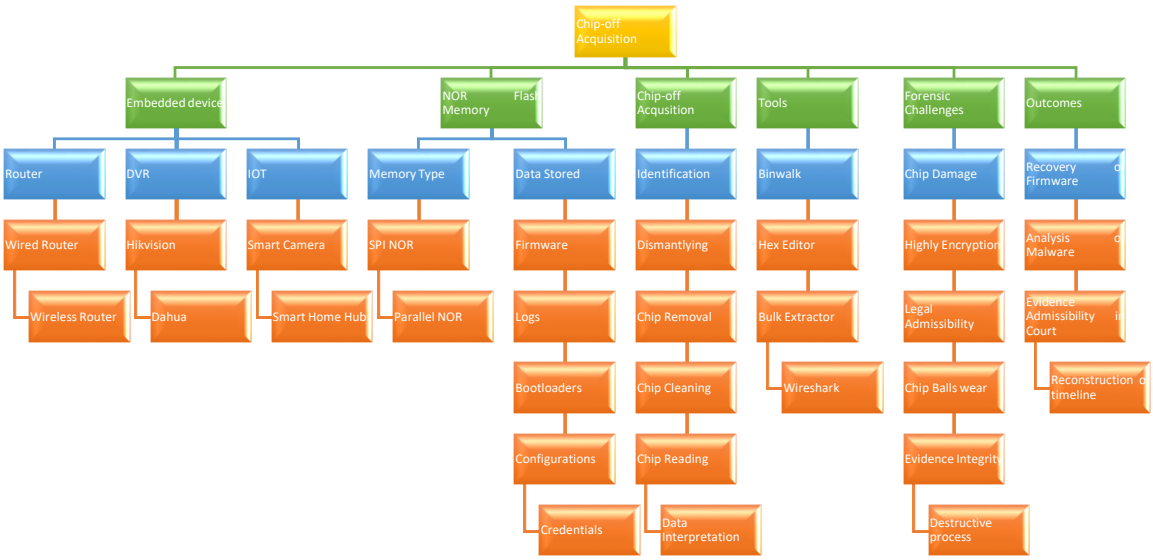
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

	NOR flash memory.		devices.	
Study related to NOR Flash Technologies, CCTV Forensics, and Smartphone Chip-Off Analysis	NOR provides fast random access read capability, making it highly suitable for long duration space missions to store critical data such as boot code or configuration files. Also reviews the current approach to CCTV forensics in literature, and identifies challenges in CCTV forensics.	Evaluation of CCTV Acquisition methods, development of CCTV workflows for handling large - scale of CCTV evidence, developing standards for SSDs.	Results developed on limited DVR models, diverse proprietary formats, implementation of watermarking causes production complexity, specialized expertise for Chip - off acquisition.	Development of standardized procedures for all types of DVRs and NVRs, automated forensic tools for emerging smart devices, standardized procedures for CCTV workflows.
Study related to IoT Security, Network Routing Mechanisms, and Embedded Monitoring Systems	Explaining the major security challenges that exist in IoT environments as well as forensic challenges, summarizing the principles of operation, and exploring the most commonly installed routers.	Focus on IoT devices and digital forensic challenges, advancement of router and multilayer architecture, development of NoC routers, introduction of API based live forensic acquisition.	IoT devices are unpredictable, reduced functionality in traditional router architecture, not addressing forensic implications, focuses on storage application rather than extraction and analysis of evidence.	Developing IoT frameworks, AI threat detection systems, developing high-density, low powered flash technologies, developing Acquisition techniques for modern router architecture.
Study related to the review of Network-on-Chip Protection Mechanisms and Mobile Evidence Acquisition Techniques	Addressing the challenge that researchers frequently face the need to code considerable quantities of video recordings with relatively flexible software, often constrained by species-specific options or exact settings.	Use of open-source software, integrating security mechanisms into NoC routers, establishing mobile forensic process.	Mainly focused on behavioral analysis rather than digital forensic investigation, many techniques are outdated for modern devices.	Open-source software with forensic value, updating of forensic software according to devices.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

	Also highlighting the critical stages of mobile forensics and weaknesses in the Acquisition of digital evidence from mobile devices.			

Taxonomy of Forensic Chip-off Acquisition of NOR Flash Memory in Embedded Devices



3. Related Work

Research on Forensic Chip-off Acquisition of NOR Flash Memory in embedded devices has grown steadily due to the increasing use of embedded devices such as IoT devices, routers, DVRs, automotive control units etc. in both domestic and industrial environments. Existing literature work encompasses Chip-off Acquisition as a reliable extraction technique when conventional techniques fail to extract.

Most published studies focus on technical approaches to chip-off acquisition, firmware extraction and recovery of data techniques. Researchers have evaluated the feasibility of various tools and workflows for recovering data from NOR flash memory while addressing the hurdles such as complexity in soldering, risk of damaging chip, and heat adjustment. However, comparatively fewer studies examine the forensic Acquisition procedures across different embedded devices and assess the reliability.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

This gap provides an opportunity for the present review, which critically examines the forensic chip-off Acquisition of NOR flash memory in embedded devices. The review integrates existing methodologies, Acquisition tools and challenges while understanding research gaps and future directions for reliable data extraction from different embedded devices.

CATEGORY A – CHIP-OFF ACQUISITION STUDIES

3.1 Study related to recent advancements in Chip-Off Recovery, NOR Flash Systems and Digital Forensics

Z. Kadyr (2025) has presented a structured comparison of chip-off and imaging techniques and proposed an intelligent hybrid approach to optimize data recovery success. The proposed methodology involves a three-stage process: assessing the condition of the drive, selecting the optimal recovery method and executing the data Acquisition with specialized tools. The researcher used 15 damaged legacy HDDs with varying failure conditions; the drives were grouped into three categories i.e., Category A (Minor issues) 6 drives, Category B (Mechanical failure) 4 drives, and Category C (Severe damage) 5 drives. Each category is associated with different recovery methods such as Category A with imaging, Category B with HSA replacement, and Category C with chip-off technique. This study also displays the practical limitations of each technique and outlines a path toward future automation using AI-driven decision support systems in digital forensics [9].

Similarly, T. Avanoz (2025) has performed the Chip-off Acquisition on NAND for data recovery. The Acquisition was performed on 32 GB SanDisk flash drive, which was defective in nature. The process involved the Chip removal from the flash drive, cleaning it, and using PC-3000 Flash platform to extract the data. The degree of heat was adjusted and decoding raw data was performed systematically. During the extraction of data from the storage capacity of 16 GB storage capacity, the data was successfully retrieved and leaving the unused space at 12.49 GB and 3.51 GB. After retrieving the data from the device the data was successfully read by the software PC-3000. This research signifies the use of Chip-Off Acquisition in recovery of data and provides a practical approach for lowering the risk of errors during the procedure of data recovery [10].

Likewise, T. B. Serm et al. (2025) have investigated the workings of NOR flash based on the functioning of electrical mechanisms. The measurement of the industrial 45 nm NOR flash showcased dominant degradation source as the NOR flash identifying loading effects. The researcher experimented on a test array of 64-cells confirming the type, and indicating the current attenuation was position dependent, exceeding from 40% under conditions of high load. The outcomes directly linked device-level physics to array-level performance limits, offering quantitative design guidelines for optimizing interconnect resistance as well as device parameters and operating conditions in low power CIM architectures for embedded AI. [11]

Moreover, H. Huang et al. (2025) have offered an NF2FS, a NOR flash- friendly file system, to solve the problem of I/O amplification deteriorating and decoupled in existing NOR Flash file systems. A key insight is that NOR Flash in which the applications are running have small file sizes, therefore providing block-based data organization which helps to convert to flat file layout and deterministic I/O patterns. The researchers implemented the NF2FS technique in FreeRTOS with a wide variety of methods, including the all-logging layout and layout management approaches. This paper proposes NF2FS, which provides feasibility for data

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

organization and WL to a coarse file granularity. The experimental results on a real embedded system show that NF2FS can outperform outstanding existing work and quickly preventable to NOR Flash wear-out under RAM-restricted MCU environments [12].

In the same way, L. Rzayeva et al. (2025) have conducted a process of recovering from Hikvision and Dahua surveillance systems by utilizing three major innovations i.e., dual-signature validation, adaptive temporal sequencing and automatic manufacturer identification. The researchers collected a sample size of 27 of surveillance hard drives; the data recovery is shown is 91.8%, 96.7% of temporal accuracy and a 2.4% false positive rate. The proposed methodology offers the transparency in the process of recovery and the automated MP4 conversion, with metadata left intact which may support admissibility in court. This study provided an experimental process for surveillance formats, which are practically useful for digital forensic investigations [13].

3.2 Study related to recent developments in mobile device data extraction and analysis

T. Sutikno (2024) has showcased the capabilities of UFED in mobile device forensics. Using advanced techniques and algorithms that enable Cellebrite UFED to help recover the data from the embedded devices that have been erased or obscured. It can extract data from email, phone calls, texts, and social media playing a pivotal role in investigations. It can provide the functionality for cellebrite UFED to recover deleted files, decrypt encrypted data and extract data from multiple devices. It has two options to extract data logically or physically and is equipped with the tools to retrieve crucial information. The user interface speeds up the data extraction process, and its analysis helps to reveal crucial information. Legal considerations include data access, privacy protection and maintaining the chain of custody. The use of cellebrite UFED assists researchers in solving complex data on mobile devices more effectively [14].

In addition, S. Shaikh et al. (2024) conducted a survey contributes to the growing phase of experienceof Android mobile devices that are non-functional performing forensic data carving techniques. Extracting data from non-functional devices is difficult. This study uses 4 steps of data carving to extract and analyze the data from non-functional devices, including dismantling, chip-off, image acquisition, and data carving, as well as showcasing the important steps and precautions that must be followed to ensure data integrity. This research compares several tools used for data carving as well as highlighting the challenges faced in the forensic analysis of mobile devices. Furthermore, this study contributes to the growing body of knowledge in digital forensics and provides a valuable method for investigators to work with devices in criminal investigations [15].

3.3 Study related to integrated perspective on Flash memory, Digital Forensic and eSIM techniques

S. S. Kim et al. (2023) have summarized the current status and critical challenges of flash memory devices with charge-trap, with a focus on the nature, physical integration structure (2D vs 3D), architecture of array-level circuit (NOR vs NAND), and programming at cell level. The researchers state that NAND flash memory is available in the market and that vertically integrated NAND flash memory acts as the main data storage medium in modern handheld electronic devices, widening its share even in the data centers where installation and operational costs are high. Nonetheless, increasing the layers invokes several problems such as film stress management and hole etching. The researchers introduced current efforts to

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

improve fabrication processes and device performance using new materials. This study recommends directions for future storage mediums based on the ionic mechanism, which may resolve the inherent problems of flash memory devices [16].

Alternatively, N. Tiwari et al. (2023) have executed a theoretical and methodological analysis of cyber and digital practices. The researchers explain that the advancing nature and need for the upgrade of software with each new version of an operating system as well as in comparison to other domains of forensic science, has caused digital forensics to evolve rapidly. The researchers also state that the goal of the investigators is to recover data and investigate artifacts found in digital evidence. This paper outlines that forensic scientists should have a great knowledge of this field, and there are renowned organizations providing different types of certifications for skill development [17].

Besides, M. Alshenaifi et al. (2023) proposed a methodology for implementing the (eUICC), Embedded Universal Integrated Circuit Card, referred to as Embedded (eSIM) when combined with other IoT devices, enables the ability to hack eUICC and get remote control access to other Machine-to-Machine devices. This study discusses regular SIM cards from point of view of digital forensics as well as M2M. The proposed framework provides a procedure with techniques that are widely accepted and are being used in the process of digital forensics and are capable of Potential Digital Evidence Analysis which is generally generated by IoT ecosystem devices. The researchers present a flowchart i.e. MNO-SD, Supplementary Security Domains, Applets, and NAAs that will help digital forensic investigators towards taking the initial steps to start investigating eSIM cards into two forensic methods which are Chip-off and analysing eSIM's profiles [18].

3.4 Study related to emerging trends in Digital Evidence Extraction and NOR Flash Memory Applications

Hadgkiss et al. (2022) developed a method for Chip-off that investigators can follow, using an array of equipment. In various digital investigation cases involving devices that contain BGA ICs, this method was developed. The method involves taking out the Chip from the circuit board using specialized tools and performing data extraction for analysis. The researchers explained the areas where the method was efficiently implemented and areas where updates could improve the overall success of the methodology. The selection of the tools is mainly focused on low cost. Following the procedure, a 6 stage process was formulated: deconstruction, identification, removal, and restoration, determination and performance. However, even though this method proved successful with the performed case study testing, there will always be room for human error and scenarios where it cannot be utilized [19].

Distinctively, M. L. Wei et al. (2022) have staged a novel analog CIM technique for GEMM using 3D NOR Flash devices to support general-purpose matrix multiplication. The analysis indicated that it is very robust to use "billions" of memory cells with modest 4-level and large spacing analog Icell to produce good accuracy and reliability. The research estimated that a 2.7 Gb 3D NOR GEMM can provide a high performance image recognition interference of ResNet-50 on ImageNet dataset, using a simple flexible controller Chip with 1MB SRAM without the need for massive ALU and external DRAM. The researchers state that using ternary similarity search algorithm with positive and negative inputs can weigh to

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

perform high dimension feature vector design. This study demonstrates the potential of NOR Flash memory beyond storage applications [20].

Another study by Huang et al. (2022) investigated a 3D NOR memory that was investigated in terms of device structure, integration scheme, and circuit architecture. To obtain single-crystal silicon channel for 3D NOR vertical flash devices were presented, a stack with multiple doped epitaxial Si layers was used; 3D NAND, bit-line planes, source line planes and vertical word-lines were utilized. In this study, the device was programmed using band - to - band tunnel-induced hot electron injection. Through programming/erasing tests, the programming speed of 10 μs and erasing speed of 100 ms were obtained, which are comparable to that of the 2D NOR flash with single-crystal silicon channels. This study shows that the proposed method improves the architecture and performance of NOR flash memory [21].

CATEGORY B – INDIRECT BUT TECHNICALLY RELEVANT STUDIES

3.5 Study related to NOR Flash Technologies, CCTV Forensics, and Smartphone Chip-Off Analysis

B. Tanios et al. (2021) has delivered a comparative study of single event effects radiation sensitivity of two COTS 55-65nm NOR flash memories for space applications. The researchers analyzed that since NOR flash memory provides fast random access read capability, which makes it highly suitable for long duration space missions to store critical data such as boot code or configuration files. Test modes and their sequence used during proton SEE tests are similar to those of heavy ions. Both static and dynamic results can be extrapolated based on the result of a single run. The bit error distribution over the word bits, which are each bit of the 16 bits forming one word, has equal sensitivity. This is done by considering 10 blocks for dynamic behavior and the rest of the Chip for static behavior. Macronix devices offered higher LET threshold than Micron; these two selected parts of NOR flash memory offered similar results for heavy ions SEE tests in terms of saturated cross-section. The test results show that NOR flash selected devices showed to be highly resistant to SEUs and SEFIs under proton radiation [22].

Correspondingly, W. E. Bruehs (2020) has developed a test design to measure the quality and rank the quality of Acquisition methods used on live systems from DVRs typically used in digital CCTV systems. The purpose of the study was to determine guidelines for acquiring the best quality video for investigative purposes. The methods of Acquisition included direct data download of the proprietary file and open file format as well as recording the video playback from the DVR via the available display monitor connections. However, depending on the circumstances and as recording technology continues to evolve, options other than proprietary file formats may provide quality that is equal to or greater than the proprietary file format [23].

Not only that, R. Gomm et al. (2020) has described a new forensic workflow for acquiring and analyzing artifacts from large amounts of data from CCTV devices of different models/manufacturers, prior to presenting and analyzing three real world case studies. This study showcases the numerous challenges that arise with the forensic Acquisition and analysis of CCTV data. Such challenges are expanded when consideration is given to the volume of data due to different manufacturers, data formats, file systems, volume storage methods etc. This study reviews the current approach to CCTV forensics in literature, and identifies the challenges of CCTV forensics [24].

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

Uniformly, H. Al. Hosani et al. (2020) has awarded a guide with appropriate standards and procedures with which to approach SSDDs. This study shows that SSDDs commonly present at crime scenes, creating a need for the development of SSDDs forensic. The development of SSDDs is a less evolved field despite the excellent progress. This research presents the current state of the art in SSDDs including smartphones, drones, smart toys, wearable technologies, and gaming consoles. The purpose of this study is to develop a guide that provides forensic examiners with the required knowledge to develop appropriate standards and procedures with which to approach SSDDs within the investigative context [25].

Coupled with this, P. Poudel et al. (2020) has spearheaded a technique called Flashmark, for watermarking of NOR Flash memory for counterfeit detection. The proposed method relies on imprinting watermarks into the physical properties of Flash memory cells and extracting physical properties of flash memory cells through standard digital interfaces. The imprinting of watermarks into the NOR Flash memory is performed by Chip manufacturers. The watermark includes manufacturer identifier, die identifier, Chip speed grade, Chip testing status and other manufacturing related information. However, this information can be erased, forged, or fabricated by counterfeiters, so repeated erase-program operations are performed until there are sufficient differences in physical properties between the memory cells that never change their state. This study explores the metrics of interest such as bit error rates, the watermark imprint time, and the watermark extraction time as well as system integrators and end users will be able to detect counterfeit chips [26].

The study conducted by N. R. Mistry et al. (2020) has regulated a methodology and guidelines to perform the phase of digital forensic procedure using the Chip - Off technique on smartphone devices. The researchers address the challenge of extraction of data, especially when the device is logically or physically damaged. By using Chip-off removing the Flash memory from circuit board, provides the advantage of performing extraction and analysis. The researchers use a sample of Apple iPhone, which are robust in nature, well locked and have APIs that can be used to apply application level encryption performing Chip-Off technique on model A1203 that contained vital forensic evidence [27].

CATEGORY C – BACKGROUND LITERATURE

3.6 Study related to IoT Security, Network Routing Mechanisms, and Embedded Monitoring Systems

M. Conti et al. (2018) have addressed the ongoing major security and forensic issues within IoT networks. This study explains the nature of IoT environments and fast pace of development which brings a variety of security and forensic obstacles. The researchers briefly explain the main security challenges that exist in IoT i.e., Authentication (key management and key deployment are challenges in IoT device authentication), Authentication and Access Control (management and deployment of a variety of access control mechanisms and authorization which are tailored to different node capabilities are challenges in heterogeneous IoT network), Privacy (privacy regulation mandates to keep users informed about how their private data is administered and managed), and Secure Architecture (detection of various malicious traffics that is retransferred over networks with different natures in addition to hunting for malicious

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

actor is a very challenging task) as well as forensic hurdles i.e. Identification of evidence, Collection & Preservation, Analysis and Correlation of evidence, and Attack or Deficit Attribution [28].

Alternatively, J. Aweya (2018) has explained the internal functioning of router and switch designs in comprehensive manner that is accessible to every audience. The researcher compares centralized vs distributed design of architecture. This study describes the transformation of multilayer switch designs, the key role of switches/routers in a network, use of bus versus shared memory for communication within a design and functional composition of switches/routers, also covers the Quality of Service Mechanisms and configured tools and highlights the major performance problems that would affect each design. It displays the need to build proactive multilayer switches and examines the architectural constraints imposed due to the various multilayer switch designs. This study discusses design issues such as implementation, complexity, performance and scalability to higher speeds. The researcher also summarizes principles of operation and explores the most commonly installed routers [29].

In the same way, H. Hidaka (2018) provided an introduction to embedded Flash memory, status, its history, and future projections for technology circuits and system applications. This study explains a range of embedded features for automotive, low power and smart-IC cards. The researcher describes a stable and mature floating gate 1Tr cell technology imported from standalone Flash memory products as well as floating-gate storage structure, specific split-gate memory cell technologies introduced, and charge-trapping SONOS technology with their eflash sub-system designs. It also explains in detail the evolution of embedded Flash memory technologies for microcontroller products [30].

Concurrently, M. M. Alani (2017) has organized router management functions such as backup, IOS upgrade, restore and copy. The researcher provides useful considerations before upgrading the router's IOS, understand the different IOS file naming conventions, how to back up and restore configuration of the router, and displays the functioning of flash memory partitioning and explained the procedure to upgrade or fix the IOS in multiple scenarios like using TFTP servers, router-to-router IOS copy, and using the terminal emulation software [31].

Meanwhile, X. W. Shen et al. (2017) has proposed a novel and reliable NoC router feature for data flowing architecture. The researchers analyze and extract the features of data transfers in NoCs of data flowing architecture: high injection rate, multiple destinations and delay performance sensitivity. The proposed router supports the transfer of data with multiple destinations in a single transfer since it can be multi-destination. The researcher evaluates the proposed router with three typical parallel applications which are suitable for data flowing architecture in double-precision floating point: stencil, FFT and GEMM. To show the performance, these three test cases are examples. They are especially important and popular in exa-scale scientific computing in high-performance computing. In each router, the adopted mechanisms can reduce the possibility of congestion and decrease the packet transfer delay [32].

Additionally, MI. Mazdadi (2017) has explored how to do forensics on Router OS based on the functioning of Mikrotik devices by using API services to develop a remote application to extract router data. Mikrotik functions as a router which is a Linux based operating system on a computer. This study observed a problem that occurs in live forensics: the alteration of data or

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

tampering of data, due to the Acquisition process. The servers also keep records on the log of Acquisition activity, in the case of collecting the log on the server. To overcome this problem, the researcher used API, which is a guide of commands, functions, and protocols that can be used by programmers to help build an OS and interact with other OS APIs, allowing programmers to use standard functions. Router's data extraction with API gives us access to information on a wide range of activities that are running on the network [33].

Moreover, K. Paulsen (2017) has described how the transition from linear recording to nonlinear recording and playback has become well-established technologies, and in essence the new foundation for today's video recording, storage, and server systems. The researcher explains the variance available in devices that "serve video" for broadcast, non-broadcast and emerging applications. This study reviews the historical perspectives of the storage evolution, explains the three fundamental types of drive structure configuration, and describes how various subsystems that manage the physical storage medium that are applied to the drive configuration [34].

Uniformly, Y. Chen et al. (2017) have developed an embedded DVR monitoring system that is Linux-based. This study explains that the receiving Chip of kernel driver is designed for Hi3520D to control its receiving mode, so that the video data captured by the camera is transferred to the data receiver, which carries out the AD conversion and preprocessing of data via BT.656 interface. The researcher uses output interface and transmission of network to complete playback operation. Through the Parallel operations implementation of the multifunction module, the researcher achieved the following key benefits, such as the Acquisition of video data and flow configuration of video encoding and decoding. To attain the goal of network video surveillance the video data is transmitted via RTSP/RTP protocol [35].

3.7 Study related to Review of Network-on-Chip Protection Mechanisms and Mobile Evidence Acquisition Techniques

O. Friard (2016) has purveyed an open-source tool called BORIS for visual and acoustic coding as well as live observations. The study addresses challenges that investigators repeatedly see the need to code considerable quantities of visual recordings with moderately flexible software, often forced by species-specific options or exact settings. To resolve this problem the researcher introduced an open-source and multi-approach standalone program that allows user-specific coding environments to be set for a computer-based review of previously recorded videos and live observations. The common formats (TSV, CSV, ODF, XLS, SQL, and JSON) are used to export the observation data. Various graphic formats (PNG, TIFF and PDF) are used to export observed events which can be plotted [36].

On the other hand, A. Biswas et al. (2015) have exhibited a security framework for Network-on-Chip systems by analysing routing and addressing attacks on router tables. This study gives four countermeasures: security using a restart-time protector, run-time protector, non-volatile memory for source address authentication and a security auditor. In addition, the proposed protectors can locate a malicious router to avoid detection and prevention of attacks. The researchers used Bluespec SystemVerilog for design and process, performing by updates to the routing table with correct data for right operations, the use of artificial traffic generators to generate traffic, stimulating attack on router by loading malicious routing table. The results

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

show that the area of run-time protector is 6.6% and that of a restart-time protector is only and 2% of a conventional router area [37] .

Simultaneously, D. Yadav et al. (2013) have unveiled the utilization of mobile devices in multiple accomplishments and mobile forensic concisely. The researchers undermine the difficulties of mobile forensic investigations i.e., operating systems, volatility of data, hardware technology innovations, forensic tools and acceptability in Indian jurisdiction of acquired mobile data and electronic evidence. The research highlighted the detailed levels of mobile forensics and weaknesses in Acquisition of digital evidence. This study contains a systematic guide in context of mobile forensic process model i.e. Level 1 (Identification), Level 2 (Evidence Acquisition), Level 3 (Examination and Analysis) and Level 4 (Reporting) as well as preservation of data and examination of extracted data with respect to the laws and Acts for the admissibility of those Digital evidences in Indian courts [38].

3.8 Research gap

Although related work has established the value of chip-off Acquisition for recovering data in embedded devices, there is still a gap in the application of NOR flash memory. Most literature either remains conceptual, focusing on flash memory architecture and firmware analysis, with fewer works on NAND Flash Memory and isolated case studies.

This gap is important because devices such as routers, DVRs and IoT controllers are increasingly encountered in investigations. These devices include hardware designs, encrypted firmware, complex interfaces, making conventional methods inadequate. To overcome such issues, chip-off Acquisition is used which becomes efficient for recovering data or firmware, system logs, credentials and other forensically sound evidence.

The current review addresses this research gap by examining chip-off Acquisition of NOR Flash Memory. By integrating findings from multiple studies, this review provides a comprehensive understanding of Chip-off acquisition.

4. Review Methodology

4.1 Review Design

This study was conducted using a systematic literature review methodology for identification, evaluation, and synthesis of present research on Forensic Chip-off Acquisition of NOR Flash memory in embedded devices. The review adhered to PRISMA guidelines to ensure reproducibility, clarity, and methodological soundness. The review methodology comprises formulation of review objectives, review questions, search plan, search keywords, search strings, inclusion and exclusion criteria, PRISMA Workflow, Quality Assessment, experimental strategy, including challenges and future directions.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

4.2 Review Objective

- The objectives of the review are:
- Identifying Acquisition and the tools reported in the literature.
- Identifying research gaps and limitations which require further investigation.
- Examining challenges encountered during the procedure.

4.3 Formulation of Review Questions

- Why is Chip-off Acquisition used for recovering data?
- What tools are used in data extraction and analysis?
- What challenges are faced during acquisition?
- What research gaps remain in the literature?

By addressing these review questions, this provides a structured basis for extracting data from the devices when the condition of the devices is burned, physically damaged or encrypted over another descriptive literature on known challenges.

4.4 Developing Search plan

Table 1.2: Search plan development

Selection platform	Science Direct, IEEE Xplore, Google Scholar, Shodh Ganga, Scopus, ACM Library, Springer, IGI Global, Wiley – IEEE Press.
Time period	2004 - 2026
Medium	English Language
Document Type	Conference paper, Handbook, Research paper, Review article.

4.5 Selecting Search Strings

- “NOR Flash” OR “NOR Flash Memory”
- “Chip-off Acquisition” OR “Forensic Acquisition”
- “Digital Investigation” OR “ Hardware Forensic”

4.6 Selecting Search Keywords

- Chip-off Acquisition
- NOR Flash Memory
- Embedded Devices having NOR Flash Memory
- Router Device
- DVR System
- Extraction of Firmware

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

4.7 Inclusion and Exclusion Criteria

Table 1.3: Criteria for Inclusion and Exclusion

Key aspect	Inclusion Criteria	Exclusion Criteria
Time period	Published between 2004 - 2026	Research papers outside the time period
Medium	English Language	Non-English Language
Embedded Device	Router, DVR, IoT Devices, flash memory or NOR flash architecture	Studies not related to devices
Flash Memory	NOR and NAND	Unrelated to flash memory
Acquisition technique	Chip-Off Acquisition	Traditional Methods
Availability of data	Research papers available in full text	Publications without full text
Tools can be used	Binwalk, Hexeditor and bulk extractor and paid tools	Where the tool is used for the purpose unrelated to acquisition
Article Type	Original Article, Conference paper, Handbook, Research paper.	Duplicate publication

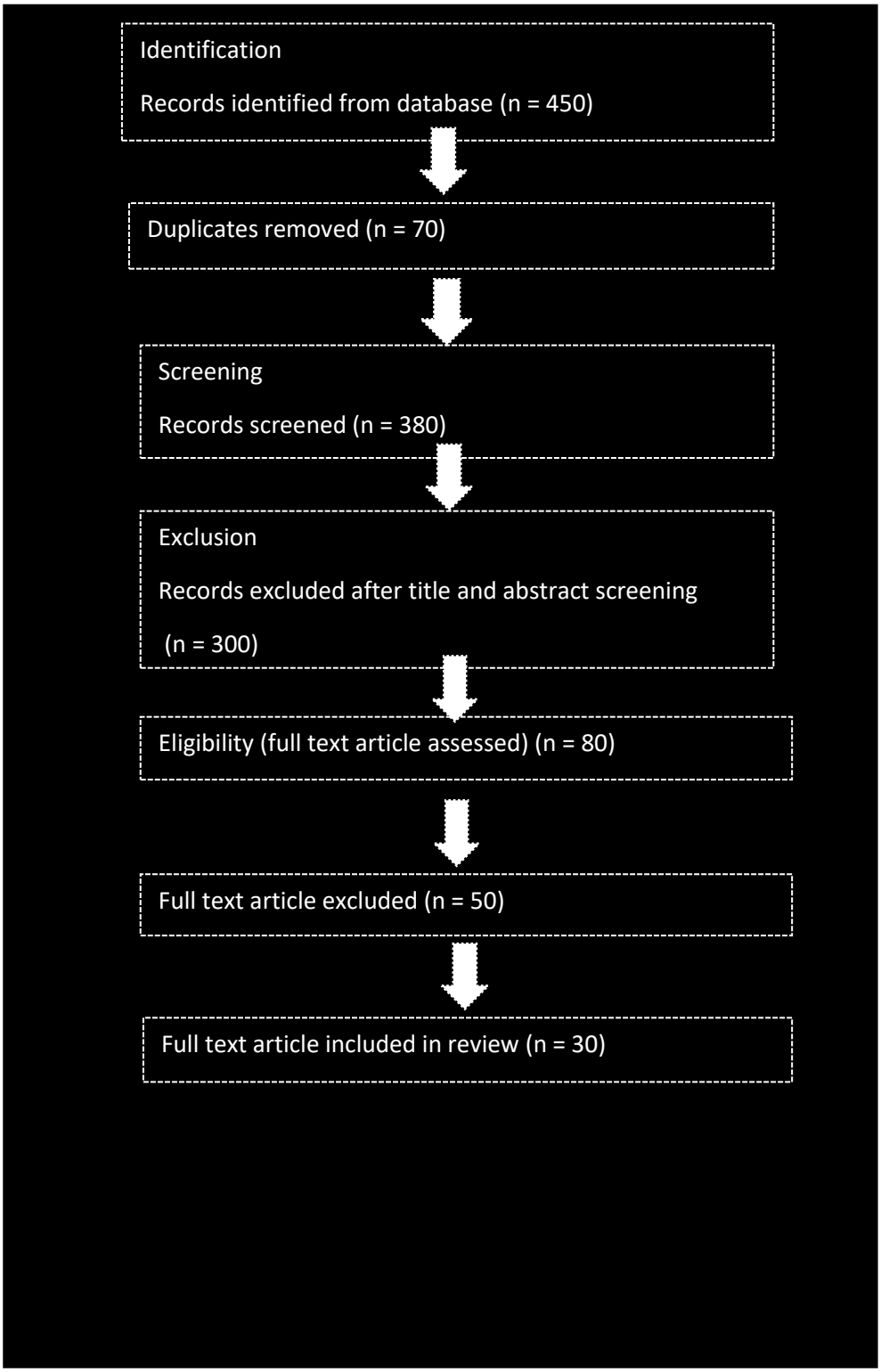
4.8 PRISMA Workflow

The Preferred Reporting Items for Systematic Review and Meta-Analysis consist of the identification records, duplicates removed, screening & eligibility criteria and abstracts according to the inclusion criteria, and finally selecting studies relevant to chip-off Acquisition and NOR flash memory.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

Fig 1.3: PRISMA Workflow



© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

Table 1.4: Reason for the exclusion of title, abstract and text article

Reason for the exclusion of tittle, abstract, and Text article	Number
Not related to embedded devices and flash memory	60
Not related to digital Acquisition and forensic	70
Not related to computer architecture only	50
Not related to domain	60
Other screening issues and duplicates	60

4.9 Quality Assessment

This study was evaluated using six categories- Methodology, Validation, Device Information, Success of Acquisition, Reliability & Limitations.

Scoring System:

- 1 = Partially demonstrated
- 2 = Clearly demonstrated

Maximum = 12 points per study

Table 1.5: Evaluation of each study based on the criteria

Criteria	Clear Methodology	Validation through experimental	Device Information	Success of Acquisition	Reliability of Tool	Limitation Discussed	Score out of 12
Z. Kadyr (2025)	2	2	1	2	2	1	10/12
T. Avanoz (2025)	2	1	2	2	1	2	10/12
T. B. Serm et al. (2025)	1	2	2	2	2	1	10/12
H. Huang et al. (2025)	2	2	2	2	2	1	11/12
L. Rzayeva et al. (2025)	2	1	2	2	2	2	11/12
T. Sutikno (2024)	1	1	2	1	2	2	9/12
S. Shaikh et al. (2024)	2	2	2	2	2	2	12/12
S. S. Kim et al. (2023)	1	2	1	2	2	1	9/12
N. Tiwari et al. (2023)	2	2	2	2	2	2	12/12
M. Alshenaifi et al. (2023)	2	1	1	2	2	1	9/12
Hadgkiss et al. (2022)	1	1	2	1	1	2	8/12
M. L. Wei et al. (2022)	2	2	2	2	1	2	11/12
Huang et al.	2	1	2	2	2	1	10/12

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

(2022)							
B. Tanios et al. (2021)	2	2	2	2	2	2	12/12
W. E. Bruehs (2020)	2	2	2	2	2	1	11/12
R. Gomm et al. (2020)	1	1	2	2	2	2	10/12
H. Al. Hosani et al. (2020)	2	2	2	2	2	2	12/12
P. Poudel et al. (2020)	1	2	2	2	2	2	11/12
N. R. Mistry et al. (2020)	2	1	1	2	2	2	10/12
M. Conti et al. (2018)	2	2	2	2	2	1	11/12
J. Aweya (2018)	2	2	2	2	2	2	12/12
H. Hidaka (2018)	1	1	2	2	2	2	10/12
M. M. Alani (2017)	2	2	1	2	2	1	10/12
X. W. Shen et al. (2017)	2	1	1	2	1	2	9/12
MI. Mazdadi (2017)	2	2	2	2	2	2	12/12
K. Paulsen (2017)	2	2	2	2	2	1	11/12
Y. Chen et al. (2017)	1	2	2	2	2	2	11/12
O. Friard (2016)	2	1	2	2	1	2	10/12
Biswas et al. (2015)	2	2	1	1	2	1	9/12
D. Yadav et al. (2013)	1	2	2	2	2	2	11/12

4.10 Chip-off Acquisition Workflow

The workflow is adapted from the literature review and presented as a framework. The equipment used, tools, temperature, application of flux vary according to device.

- Identification (Identifying the make and model of device to determine the location of flash memory)
- Preparation and Disassembly (Dismantling the device and removing PCB)
- Desoldering (After dismantling, desolder the devices by applying flux to all the solder joints using a heat gun. After that, the pins were evenly heated until

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

the solder liquefied and with the help of tweezers the Chip was gently lifted from the board)

- Chip Cleaning (After removal, the Chip will be covered in adhesive and residual solder, which must be cleaned so it fits correctly in a Chip reader)
- Chip Reading (Once cleaned, the Chip is placed into a Chip reader to create the raw image (dump) of the data)
- Data Interpretation (The extracted raw dump is not directly readable because it is in binary form and must be processed. The data is extracted using specialized tools such as Binwalk)

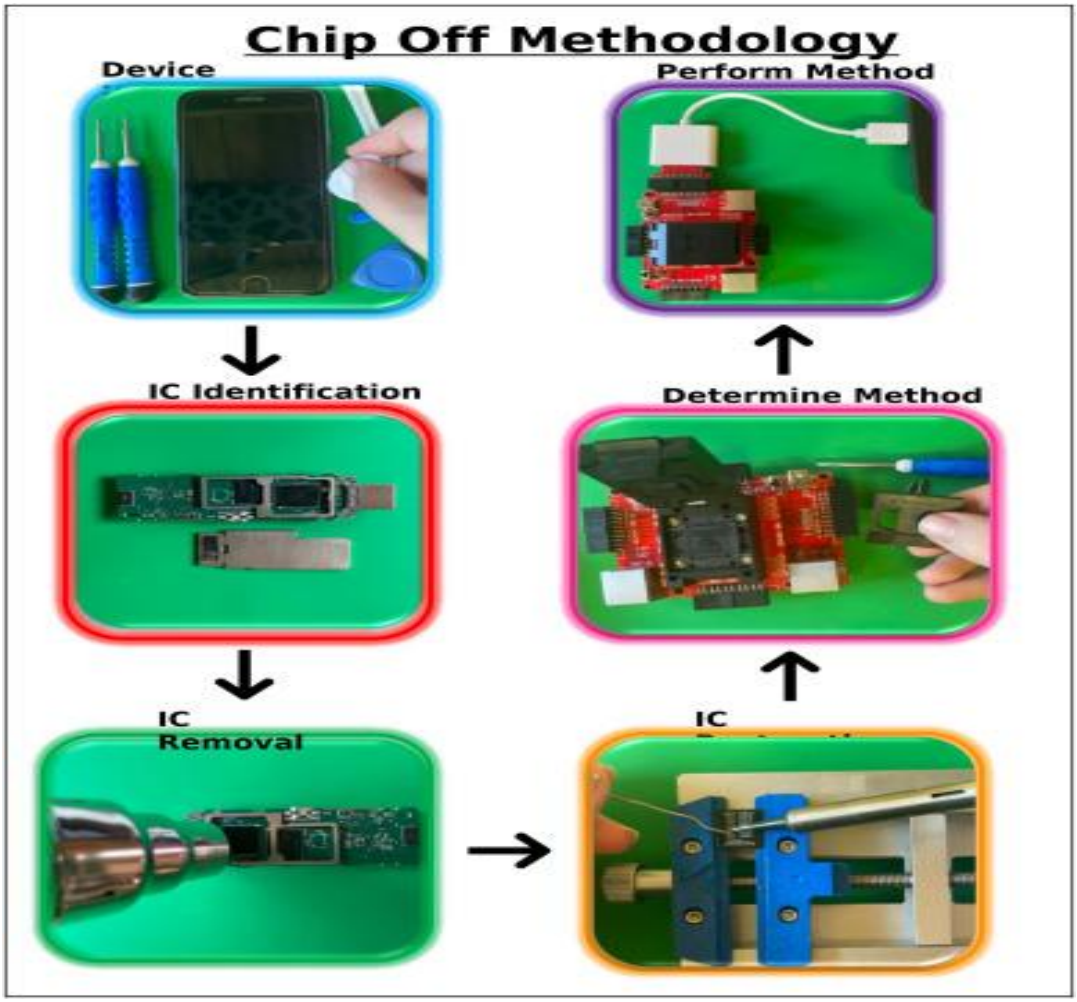


Fig 1.4: M. Hadgkiss, S. Morris, S. Paget, A. Ventress, K. Norris. Cheap as Chips: An accessible Chip-off Acquisition method for ball grid array (BGA) integrated circuits in digital investigations. 11 Nov 2022

4.11 Challenges, their impact on forensic investigation and possible solutions

Table 1.6: Illustrating the forensic Challenges, impacts and their solution

Forensic Challenges	Impact	Solution

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

Heat damage	Physically damage to Flash Memory leading to complete or partial data loss	Using controlled rework station with temperature adjustment
Encryption of Firmware	Preventing data extraction	Documenting encryption status, analysis using cryptography, and in some cases with legal permission obtaining decryption key
Degradation of memory	Incomplete recovery of data due to the mechanism of memory	Using error correction techniques, validating extracted data and performing multiple memory dumps
Evidence Integrity	Chances of alteration during removal of Chip reducing integrity of evidence	Using Cryptographic hash values to ensure the integrating of the evidence
Chain of Custody	Due to poor documentation it compromises the admissibility of digital evidence in court	Documenting every step and preserving chain of custody

4.12 Future Directions

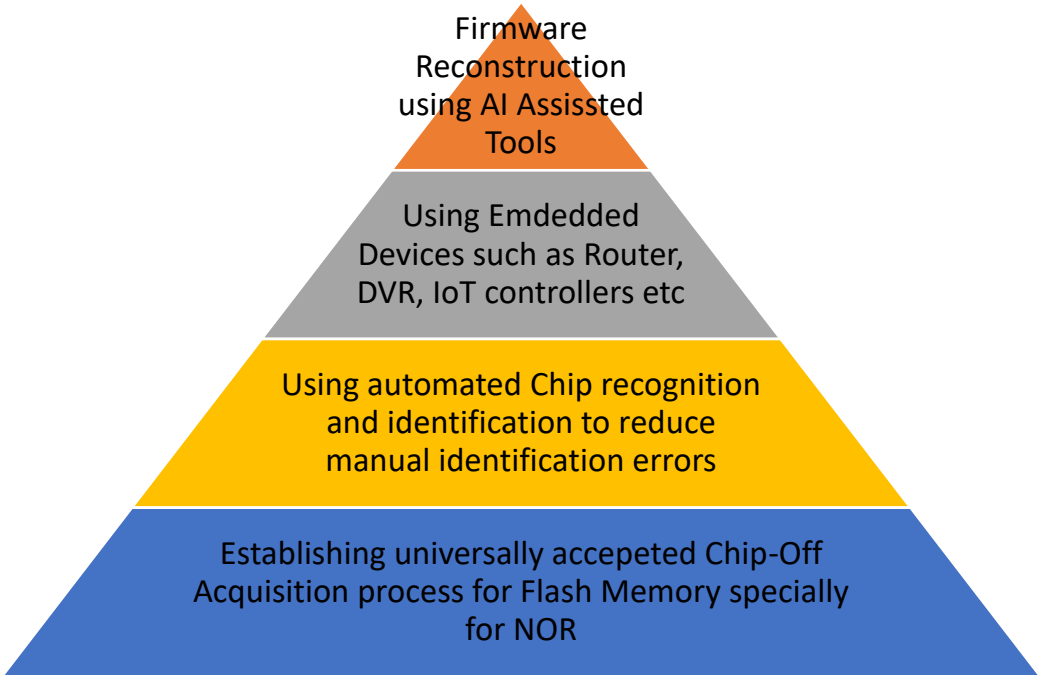


Fig 1.5: Future directions in the study

5. DISCUSSION

This review displays the importance of Chip-off Acquisition as a productive procedure for recovery of data and extraction of evidentiary data from embedded devices containing NOR Flash Memory. The review illustrates that Chip-off Acquisition is a data extraction process, which is an advanced yet complex technique.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/20szkv62

Apart from traditional methods, this Chip-off technique eases direct access to the data even when the condition of the device is broken, locked, non-working or encrypted. With the expansion of embedded devices such as routers, IoT systems and DVRs in both industrial and household environments, they function to store, process, and generate data, which can be further utilized in the investigations. The need for a systematic procedure for the NOR flash memory has become critical.

The findings show that the application of Chip-off Acquisition to NAND Flash Memory and mobile devices is more practical than NOR Flash memory in Routers, DVRs and other embedded systems. It further exhibits that successful chip-off acquisition of NAND flash memory has been demonstrated, whereas the literature on NOR flash memory remains limited. Previous studies in this field proposed that in spite of many pros, this technique has manifold difficulties such as removal of flash from circuit board, processing of data needs specialized software and temperature control and other procedural factors. The challenges may include possible Chip damage due to heat, high encryption, tools and techniques. The reviewed literature proposes that the Chip-off technique can contribute to the recovery of data, analysis of devices, and investigating cybercrime.

Overall, this review explains that Chip-off Acquisition of NOR flash memory is valuable yet underexplored in this field. Future research should focus on making the acquisition process systematic, using specialized tools, and noticing challenges that can alter the process of recovery of data.

6. CONCLUSION

This review proposes the application of Chip-off Acquisition to NOR Flash Memory in Embedded Devices. NOR Flash Memory stores Boot Code/Firmware, Application Code, Configuration Data, and Boot Blocks etc. However, the direct forensic evidence concerning NOR flash memory remains limited compared with the literature on NAND flash.

This review also demonstrates that the rate of success in Chip-off technique depends on the care at every stage of extraction such as removal of chip, data reading and analysis of interpreted data. The procedure requires standardized software and skilled expertise. However, the process is highly valuable but still possesses complexity such as possibility of Chip damage, reading glitches, and limitation of the software used.

The findings of this review demonstrate that the application of Chip-off Acquisition is applied to NAND Flash memory whereas to NOR Flash Memory it remains limited. Overall, this provides a broader view that chip-off acquisition should be further investigated for NOR flash memory. for the extraction of data from the embedded devices. Future research should further investigate the application of Chip-off Acquisition in embedded devices such as routers, DVRs, IoT Devices, and Driver Assistance Systems etc.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

ACKNOWLEDGEMENT

The authors declare that no financial or institutional support was received for this research.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Muhammad Tuhin. The Evolution of Technology: From the Stone Age to Today 2025

[2] Shepherd J. What is the Digital Era? Social and Economic Transformation in the Digital Era, IGI Global; 2004, p. 1–18. https://doi.org/10.4018/978-1-59140-158-2.ch001

[3] Pandey P, Kapoor A. CYBERCRIME IN THE DIGITAL ERA: IMPACTS, AWARENESS, AND STRATEGIC SOLUTIONS FOR A SECURE FUTURE. Sachetas 2025;4:32–7. https://doi.org/10.55955/410004

[4] Hargreaves C, van Beek H, Casey E. SOLVE-IT: A proposed digital forensic knowledge base inspired by MITRE ATT & amp; CK. Forensic Science International: Digital Investigation 2025;52:301864. https://doi.org/10.1016/j.fsidi.2025.301864

[5] Avanoz T, Akbal E. Data Recovery Application from NAND Flash Memories Using the Chip-Off Technique in Digital Forensics. International Journal of Innovative Engineering Applications 2025;9:232–42. https://doi.org/10.46460/ijiea.1797801

[6] Jessica Hopkins. What is Flash Memory? Introduction, Types, Examples, and Applications. 2021

[7] Sanvido M, Chu FR, Kulkarni A, et al. Nand Flash Memory and Its Role in Storage Architectures. Proceedings of the IEEE 2008;96:1864–74. https://doi.org/10.1109/JPROC.2008.2004319

[8] Stephen J. Bigelow, Margaret Jones. Stephen J. Bigelow and Margaret Jones. (2023, May 12). NAND flash memory. NOR Flash: Working, Structure, and Applications. (2021, November 18). 202

[9] Zhasmin Kadyr AA. Intelligent Chip-off and imaging methods for extracting data from legacy HDDs. In: Biloshchytsky Andrii, Zhakiyev Nurkhat, Abitova Gulnara, et al., editors. 1st international Scientific and Practical Conference (ICCSDFAI-25), Astana, Kazakhstan : Decision of the Scientific and Technical

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

Council of Astana IT University LLP dated 16.04.2025, protocol No.5; 2025, p. 396–400

[10] Avanoz T, Akbal E. Data Recovery Application from NAND Flash Memories Using the Chip-Off Technique in Digital Forensics. International Journal of Innovative Engineering Applications 2025;9:232–42. https://doi.org/10.46460/ijiea.1797801

[11] Serm T-B, Chen T-C, Wang P-K, et al. Experimental and modeled analysis of source-line loading effects in NOR flash compute-in-memory arrays. Applied Physics Lett 2025;127. https://doi.org/10.1063/5.0304098

[12] Huang H, Pan Y, Xia W, et al. Simplifying and Accelerating NOR Flash I/O Stack for RAM-Restricted Microcontrollers. Proceedings of the 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2, New York, NY, USA: ACM; 2025, p. 1076–90. https://doi.org/10.1145/3676641.3716272

[13] Rzayeva L, Shayakhmetov M, Atanbayev Y, et al. Automated Forensic Recovery Methodology for Video Evidence from Hikvision and Dahua DVR/NVR Systems. Information 2025;16:983. https://doi.org/10.3390/info16110983

[14] Sutikno T, Busthomi I. Capabilities of cellebrite universal forensics extraction device in mobile device forensics. Computer Science and Information Technologies 2024;5:254–64. https://doi.org/10.11591/csit.v5i3.p254-264

[15] Shaikh S, Deng L, Xu W. A Practical Survey of Data Carving from Non-Functional Android Phones Using Chip-Off Technique. In: Shahram Latifi, editor. ITNG 2024: 21st International Conference on Information Technology-New Generations (ITNG 2024), Baltimore, MD, USA: Springer, Cham; 2024, p. 43–50. https://doi.org/10.1007/978-3-031-56599-1_6

[16] Kim SS, Yong SK, Kim W, et al. Review of Semiconductor Flash Memory Devices for Material and Process Issues (Adv. Mater. 43/2023). Advanced Materials 2023;35. https://doi.org/10.1002/adma.20237031

[17] Tiwari N, Baroniya Y, Bharadwaj V, et al. Cyber and Digital Forensic. In: Pankaj Shrivastava, Jose Antonio Lorente, Ankit Srivastava, et al., editors. Textbook of Forensic Science, Singapore: Springer Nature Singapore; 2023, p. 773–803. https://doi.org/10.1007/978-981-99-1377-0_25

[18] Alshenaifi IM, Qazi EUH, Almorjan A. IoT Forensics: Machine to Machine Embedded with SIM Card. In: Shahram Latifi, editor. ITNG 2023 20th International Conference on Information Technology-New Generations (ITNG 2023), Springer, Cham; 2023, p. 133–42. https://doi.org/10.1007/978-3-031-28332-1_16

[19] Hadgkiss M, Morris S, Paget S, et al. Cheap as chips: An accessible Chip-off Acquisition method for ball grid array (BGA) integrated circuits in digital

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

investigations. Forensic Science International: Digital Investigation 2022;42–43:301481. https://doi.org/10.1016/j.fsidi.2022.301481

[20] Wei M-L, Lue H-T, Ho S-Y, et al. Analog Computing in Memory (CIM) Technique for General Matrix Multiplication (GEMM) to Support Deep Neural Network (DNN) and Cosine Similarity Search Computing using 3D AND-type NOR Flash Devices. 2022 International Electron Devices Meeting (IEDM), IEEE; 2022, p. 33.3.1-33.3.4. https://doi.org/10.1109/IEDM45625.2022.10019495

[21] Huang W, Zhu H, Li J, et al. A Novel 3D NOR Flash With Single-Crystal Silicon Channel: Devices, Integration, and Architecture. IEEE Electron Device Letters 2022;43:1874–7. https://doi.org/10.1109/LED.2022.3211174

[22] Tanios B, Kaddour M, Forgerit B, et al. Single Event Effects Characterization of 55-65nm NOR Flash for Space Applications. 2021 21th European Conference on Radiation and Its Effects on Components and Systems (RADECS), IEEE; 2021, p. 1–4. https://doi.org/10.1109/RADECS53308.2021.9954491

[23] Bruehs WE, Stout D. Quantifying and Ranking Quality for Acquired Recordings on Digital Video Recorders. J Forensic Sci 2020;65:1155–68. https://doi.org/10.1111/1556-4029.14307

[24] Gomm R, Brooks R, Choo K-KR, et al. CCTV Forensics in the Big Data Era: Challenges and Approaches. In: Nhien-An Le-Khac, Kim-Kwang Raymond Choo, editors. Studies in big data, vol. 74, Springer, Cham; 2020, p. 109–39. https://doi.org/10.1007/978-3-030-47131-6_6

[25] Hosani H Al, Yousef M, Shouq S Al, et al. State of the Art in Digital Forensics for Small Scale Digital Devices. 2020 11th International Conference on Information and Communication Systems (ICICS), IEEE; 2020, p. 072–8. https://doi.org/10.1109/ICICS49469.2020.239531

[26] Poudel P, Ray B, Milenkovic A. Flashmark: Watermarking of NOR Flash Memories for Counterfeit Detection. 2020 57th ACM/IEEE Design Automation Conference (DAC), IEEE; 2020, p. 1–6. https://doi.org/10.1109/DAC18072.2020.921852

[27] Mistry NR, Koshy B, Dahiya M, et al. iPhone Forensics. Digital Forensics and Forensic Investigations, IGI Global; 2020, p. 308–24. https://doi.org/10.4018/978-1-7998-3025-2.ch021

[28] Conti M, Dehghantanha A, Franke K, et al. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems 2018;78:544–6. https://doi.org/10.1016/j.future.2017.07.060

[29] Aweya James. Switch/Router Architectures : Shared-Bus and Shared-Memory Based Systems. Wiley-IEEE Press; 2018.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

[30] Hidaka H. Embedded Flash Memory for Embedded Systems: Technology, Design for Sub-systems, and Innovations. Cham: Springer International Publishing; 2018. https://doi.org/10.1007/978-3-319-55306-1

[31] Alani MM. Cisco Router Management. Guide to Cisco Routers Configuration, Cham: Springer International Publishing; 2017, p. 183–206. https://doi.org/10.1007/978-3-319-54630-8_7

[32] Shen X-W, Ye X-C, Tan X, et al. An Efficient Network-on-Chip Router for Dataflow Architecture. J Computer Science Technology 2017;32:11–25. https://doi.org/10.1007/s11390-017-1703-5

[33] Muhammad Itqan Mazdadi IRAL. Live Forensics on RouterOS using API Services to Investigate Network Attacks . International Journal of Computer Science and Information Security (IJCSIS) 2017;15:406–10

[34] Paulsen K. Video Recording, Servers, and Storage. National Association of Broadcasters Engineering Handbook, Routledge; 2017, p. 677–744. https://doi.org/10.4324/9781315680149-39

[35] Yi Q, Shi M, Chen Y. The Design of Surveillance System Based on Hi3520D. 2017 5th International Conference on Mechanical, Automotive and Materials Engineering (CMAME), IEEE; 2017, p. 305–9. https://doi.org/10.1109/CMAME.2017.8540186

[36] Friard O, Gamba M. BORIS : a free, versatile open-source event-logging software for video/audio coding and live observations. Methods Ecology and Evolution 2016;7:1325–30. https://doi.org/10.1111/2041-210X.12584

[37] Biswas AK, Nandy SK, Narayan R. Network-on-Chip router attacks and their prevention in MP-SoCs with multiple Trusted Execution Environments. 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), IEEE; 2015, p. 1–6. https://doi.org/10.1109/CONECCT.2015.7383936

[38] Yadav D, Mishra M, Prakash S. Mobile Forensics Challenges and Admissibility of Electronic Evidences in India. 2013 5th International Conference on Computational Intelligence and Communication Networks, IEEE; 2013, p. 237–42. https://doi.org/10.1109/CICN.2013.57

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)