Research Paper

Forensic Chip-Off Acquisition of NOR Flash Memory in Router's & DVR's

Dawle Aaditi[1], Ranjan Ashish[2*], Johari Tanushri[3], Mundirikkal Avani[4], Gupta Anurag[5]

[1]Masters in Science (Forensic Science), Oriental University, Indore, Madhya Pradesh, India
Email: aaditidawale@gmail.com
ORCID ID: 0009-0007-0590-9140

[2*]Assistant Professor, Department of Forensic Science, Oriental University, Indore, Madhya Pradesh, India
Email: ashishrajpoot9211@gmail.com
ORCID ID: 0009-0004-8127-6873

[3]Assistant Professor, Department of Forensic Science, Oriental University, Indore, Madhya Pradesh, India
Email: tanushrijohari24@gmail.com
ORCID ID: 0009-0007-3232-907X

[4]Masters in Science (Forensic Science), Oriental University, Indore, Madhya Pradesh, India
Email: avanimundirikkal@gmail.com
ORCID ID: 0009-0001-8217-333X

[5]PhD Scholar, Banaras Hindu University, India
Email: guptaanurag9026@gmail.com
ORCID ID: 0009-0009-9931-6868

Received: 15th Jul, 2026 | Revised: 25th Jul, 2026 | Accepted: 5th Aug, 2026 | Available Online: 12th Aug, 2026

ABSTRACT

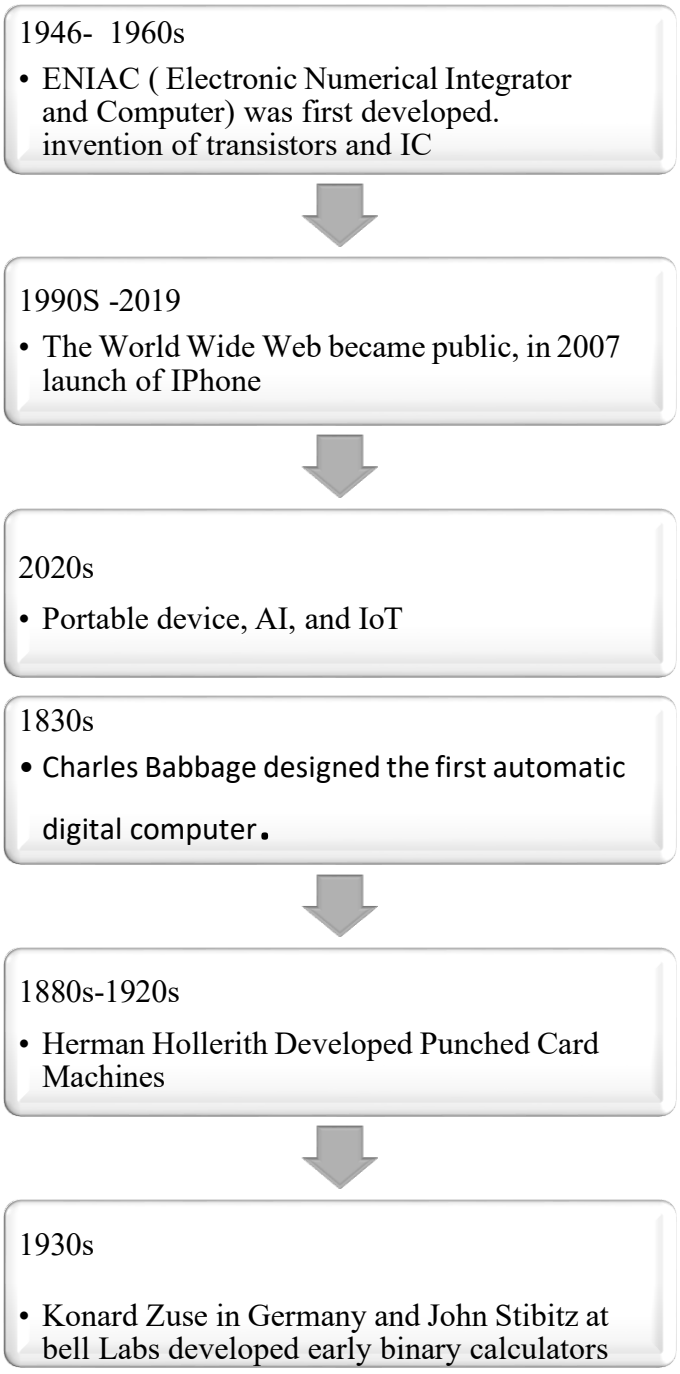
Chip-Off Acquisition offers great feasibility to the investigator, with such technique the data recovery has been made easy to extract from the devices, which are physically damaged, burned, encrypted or password protected. After a review of available literature, limited publications were found to be discuss on data recovery of NOR Flash Memory from Router's and DVR using Chip-Off Acquisition. This study presents a detailed application of Chip-Off technique for data recovery of NOR Flash Memory from Router's & DVR's. The process involves the physical removal of NOR chip from the device, followed by cleaning, chip reading, extracting and analyzing the data using Binwalk for Router's and Bulk Extractor for DVR's. Performing Wireshark to analyze the resolved address. The Chip Off method has some difficulties such as heat control, hot enough to melt the solder but not too much to damage the chip, chip reader, software for extracting the data etc. Our findings shows how data can be extracted from the devices using Chip-Off Acquisition along with the use of Software, Binwalk, Bulk Extractor, and Wireshark.

Keywords: Chip off Acquisition, Nor Flash Memory, Router's, DVR's

How to cite this article: Aaditi D, Ashish R, Tanushri J, Avani M, Anurag G., Forensic Chip-Off Acquisition of NOR Flash Memory in Router's & DVR's. Int J Drug Deliv Technol. 2026;16(76s): 1399-1445; DOI: 10.25258/ijddt.16.76s.125

INTRODUCTION

The evolution of digital devices from 1830s to 21st century has involved many advancements in technology (Muhammad Tuhin, 2025).



Digital devices such as laptop, smartphones, smartwatches, mobile phones, and internet based communication systems dominate everyday life (Shepherd, 2004). Digital devices are exploited by attacker involving in cybercrimes such as hacking, illegal surveillance tampering and network assaults (Pandey & Kapoor, 2025). Digital forensic plays a pivotal role in this area. It is the process involving the identification, preservation, acquisition, analysis, and presentation of digital evidences from digital devices. Data recovery from the encrypted, damages, broken digital devices makes it difficult to access through conventional methods, to resolve this issue Chip off Acquisition is used (Hargreaves et al., 2025).

Chip off Acquisition is a hardware level data extraction technique involving the process of removing of chip directly from circuit board, cleaning it, analyzing it into a chip reader and processing the extracted data into specialized software. Even though the device is in non- working condition the chip off mechanisms works really well (Avanoz & Akbal, 2025)

1.1 The Development of Chip off Forensic in India (kumar Akhlesh, 2021)

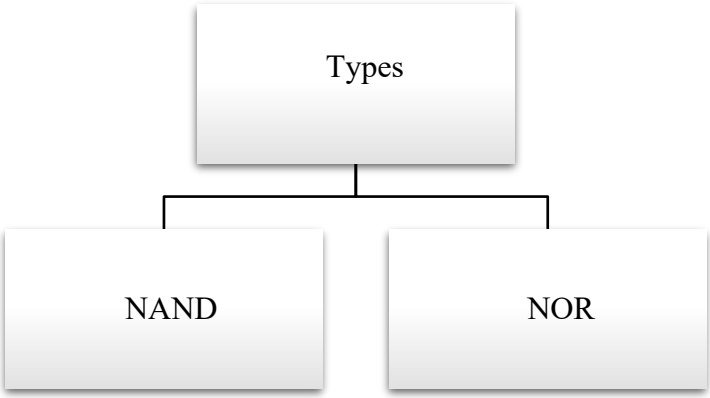
The technique developed by scientists Akhlesh Kumar, Bhushan Ghode and Khevna Maniar

At CFSL- 36, published with a case study in the International Journal of Engineering Science and Research Technology (IJESRT)

Using this technique, the data has been retrived from a smart cell phone which has been locked with the fingerprints of a person who had died by suicide

The technique was developed in the laboratory in December 2020.

It helps to store information and code in embedded devices. It can stores the data without power supply. Flash memory can be erased and reprogrammed electrically which is frequently used in SD cards and USB flash devices. Flash memory is the revolutionized form of EEPROM, the only difference is flash memory can read, write but can be erasable at block level only. It follows often 12C or SPI protocol, which helps to communicate between two devices or chips (jessica Hopkins, 2021).



1.1.1 NAND Flash Memory:

1. In 1987, scientist introduced NAND memory, in which only blocks of data could be streamed in or out. Cell designs are made in this way that NAND flash memory becomes denser than NOR.
2. It has cell in NAND flash memory was serially organized.
3. The memory is $4F^2$
4. The application that triggered the rise of NAND was digital photography and digital storage (Sanvido et al., 2008).
5. NAND Flash memory operation: The Flash forms a channel of columns and rows. Each channel contains transistor.

6. This procedure requires voltage (Stephen J. Bigelow and Margaret Jones, 2023).

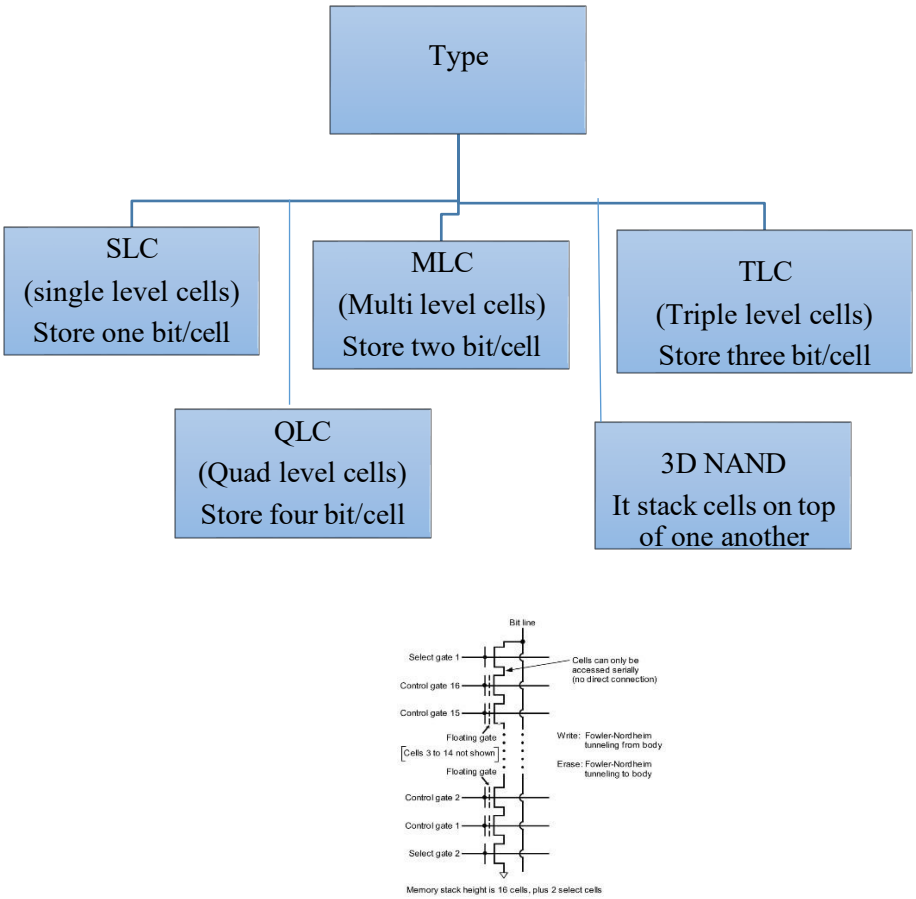


Fig. 1.1: Cell Architecture of NAND(Nguyen et al., 1999)

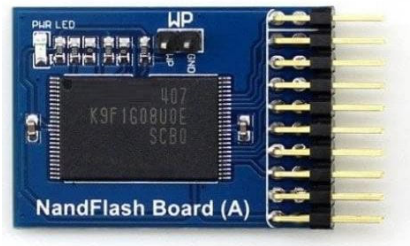


Fig. 1.2: NAND Flash Memory (Anagnostopoulos et al., 2022)

1.1.2 NOR Flash Memory:

1. Intel first developed NOR Flash Memory in 1988.
2. The storage density of NOR is low, so the cost of storing a byte is also higher.
3. Along with the high-density layout of 5G station, it will be long-term boon for NOR Flash Memory.
4. The reading speed of NOR is slightly faster than NAND (*NOR Flash: Working, Structure, and Applications* , 2021)

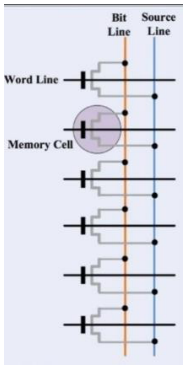


Fig. 1.3: Cell Architecture of NOR (Aleksandar Skendzic, n.d.)

Fig. 1.4: NOR Flash Memory(Skendzic et al., 2016)

1.2 Router:

The network which tends to connect network devices, focuses on roles i.e. traffic management of the network while forwarding data packets to the designated location and permit multiple network.

Types:

1. Wireless router- It uses wireless access point functions to connect networking devices. It do not establish LANs whereas they create WLANs which able to connect multiple devices using wireless communication.
2. Wired – It offering speed, security and stability.
3. Core router- core router transmit large amount of data packets within the network. This are used by large corporation and organization.
4. Virtual router: It is a software application that performs the same function as a standard hardware router (*What Is a Router?*, n.d.).

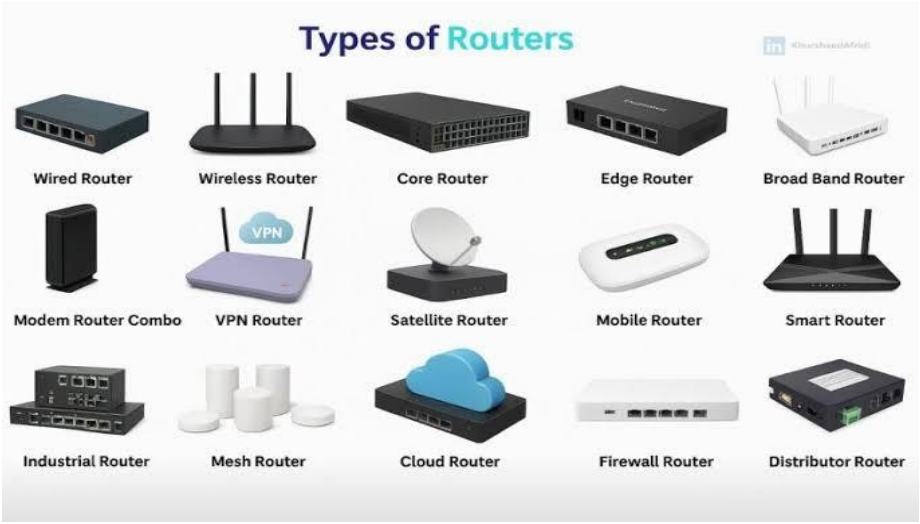


Fig. 1.5: Types of Router (Sedqatullah Yaqoubi, 2025)

1.3 DVR:

A Digital Video Recorder is a device that captures video from Security cameras in analog format, and converting it into digital formte, compressed it and storing it on a hard drive or other storage media for recording and playback purpose. For decades, DVRs have been the foundational base for security system, attaching multiple analog cameras to a single recording hub. DVR captures the analog signal through coaxial cables and converts it into digital format which is a rigorous process, compression to store it effectively, and recording to hard drive. Built –in compression using H.264 and H.265 codecs. Compression helps to store the weeks and months of data into modest drives.

It contains a microprocessor, video capture cards, hard drives, power supply, and motherboard.

Types:

1. Standalone DVRs- These are hardware devices which connects directly to analog cameras, monitors, and networks. Standalone DVRs has simple installation and have built-in back for preserving the evidence.
2. PC-based DVRs- These are install DVR software on users existing windows and Linux servers, it can create malware vulnerability if connected to the internet without proper security.
3. Hybrid DVRs- These is the combination of analog and IP camera, allowing rapid conversion of analog signals into digital formats (*What Is a Digital Video Recorder (DVR)?*, n.d.).

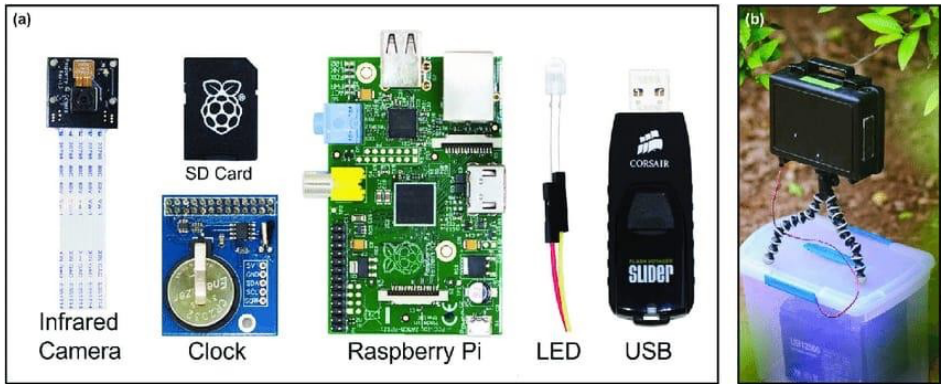


Fig. 1.6: DVR (Kistner et al., 2017)

REVIEW OF LITERATURE

2.1 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 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 drivers were grouped into three categories i.e. Category A (Minor issues) 6 drives, Category B (Mechanical failure) 4 drives, Category C (Severe damage) 5 drives. Each category is associated with different recovery method 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 (Zhasmin Kadyr, 2025).

2.2 T. Avanoz (2025) has perform the chip off acquisition on NAND for data recovery. The acquisition performed in 32 GB SanDisk Flash Drive, as it was defective in nature. The process involving the chip removal from the flash drive, cleaning it, using PC-3000 Flash platform to extract the data. The degree of heat is adjusted and decoding raw data describe systematic. During the extraction of data from the storage capacity of 16 GB, the data successfully retrieved and the unused space is 12.49 GB and 3.51 GB. After retrieving the recovered data from the device the data was successfully read by the software PC3000. This research signifies the use of Chip-Off Acquisition in recovery of data and provides a practical approach for lowering the risk of error during the procedure of data recovery (Avanoz & Akbal, 2025).

2.3 T. B. Serm et al. (2025) has investigated the working of NOR flash based on the functioning of electrical mechanisms. The measurement of the industrial 45nm NOR flash showcasing dominant degradation source as the NOR flash identifying loading effects. Researcher experimented on a test array of 64-call confirming the type, indicating the current attenuation of position dependent which exceeds 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 (Serm et al., 2025)

2.4 H. Huang et al. (2025) has offered an NF2FS a NOR flash- friendly file system to solve the problem of I/O amplification which further deteriorates as they are decoupled in existing NOR Flash file systems. The key insights is that the application running on NOR Flash usually have small file size, therefore block-based data organization can be converted to flat file layout and deterministic I/O patterns. The researchers implemented NF2FS in FreeRTOS using a range of techniques, including the all-logging layout, along with efficient layout management approaches. This paper proposes NF2FS, which relaxes data organization and WL to a coarse file granularity. The experimental results on a real embedded system show that NF2FS significantly outperforms existing work and can prevent quick NOR Flash wear-out under RAM-restricted MCU environments (H. Huang et al., 2025).

2.5 L. Rzayeva et al. (2025) has conducted a forensic recovery methodology of Hikvision and Dahua surveillance systems by utilizing three major innovations i.e., adaptive temporal sequencing, dual-signature validation and automatic manufacturer identification. The researcher

tested on 27 surveillance hard drives, which showed a recovery of 91.8, a temporal accuracy of 96.7% and a false positive rate of 2.4%. The proposed methodology offers the necessary algorithmic transparency to be court-admissible, and the automated MP4 conversion with metadata left intact. This study provided a scientifically validated approach to surveillance formats, which are practically useful to digital forensic investigations (Rzayeva et al., 2025).

2.6 T. Sutikno (2024) has showcased the capabilities of UFED in mobile device forensics. Advanced methods and algorithms allow cellebrite UFED to recover the data from erased or obscured embedded devices. It can pull data from call logs, texts, email, and social media, playing a pivotal role in investigations. It can decrypt encrypted data, recover deleted files, and extract data from multiple devices. The tools elaborate features both physical and logical extraction options, have equipped forensic specialists with the means to retrieve crucial information. The intuitive user interface speeds up data extraction and analysis, revealing crucial information. Legal considerations including access to data, protecting privacy, and adhering to chain of custody. Using cellebrite UFED researchers can navigate complex data on mobile devices more efficiently and precisely (Sutikno & Busthomi, 2024).

2.7 S. Shaikh et al. (2024) has directed a survey of forensic data carving techniques from non-functional Android mobile devices. Data extraction methods become limited when the phones are non-functional. This study aims to evaluate a chip-off data carving technique for extracting and analyzing data from non-functional devices using a four- step methodology, including disassembly, chip-off, image acquisition, and data carving as well as displaying the critical steps and precautions that must followed to ensure data carving. This study compares various tools used for data carving as well as highlight the challenges involved in the forensic analysis of mobile devices. Overall, this study contributes towards the growing body of experience in digital forensic and provide a valuable resource for investigators working with Android mobile devices in criminal investigations (Shaikh et al., 2024).

2.8 S. S. Kim et al. (2023) has summarized the current status and critical challenges of charge-trap based flash memory devices, with a focusing on the material, array-level circuit architecture (NOR Vs NAND), physical integration structure (2D Vs 3D) and cell level programming. The researcher states that NAND flash memory is readily available in the market as well as vertically integrated NAND flash memory is the main data storage in modern handled electronic devices, widening its share even in the data centers where installation and operational costs are high. Nonetheless, increasing the layers invoke several challenges such as film stress management and deep contact hole etching. Current efforts to improve fabrication processes and device performance using new material are also introduce. This review suggests directions for future storage devices based on the ionic mechanism, which may overcome the inherent problems of flash memory devices (Kim et al., 2023).

2.9 N. Tiwari et al. (2023) has executed a theoretical and methodological analysis of cyber and digital practices. The researcher explains that the advancement and upgradation of forensic software's are needed with each new versions of an operating system as well as in comparison to various other domains of forensic digital forensics has evolved faster as simple because technology changes rapidly. The researcher states that the goal of the investigators is to recover data and investigate artifacts found in digital evidences. This paper outlines that forensic scientist should have a great knowledge in this field and there must have different types of certifications available by many of the renowned organizations (Tiwari et al., 2023).

2.10M. Alshenaifi et al. (2023) has render a methodology how to implement the Embedded Universal Integrated Circuit Card (eUICC), also known as Embedded (eSIM) when merged with other IoT Devices as well as the ability to hack eUICC and get remote control of other Machine-to-Machine devices. This study discusses regular SIM cards from a digital forensic point of view as well as M2M. The proposed framework comes with the aim to provide a methodology complete with techniques that are widely accepted and are being use in the process of digital forensics and are capable of Potential Digital Evidence Analysis which are generally generated by IoT ecosystem devices. The researcher represented a flowchart i.e. MNO-SD, Supplementary Security Domains, Applets, and NAAs that will help digital forensic investigators towards the initial steps to start to investigate eSIM cards into two forensic method which are chip off and analyzing eSIM's profile (Alshenaifi et al., 2023).

2.11 Hadgkiss et al. (2022) has accomplished a methodology for chip off that examiners can follow, using an array of equipment. The method was develop to apply in the various digital investigation cases with devices that contain BGA Ic's. The method involve removing the chip from the circuit board using specialized tools and performing data extraction for analysis. The researcher demonstrated areas where the method was positively implement and areas where updates could improve the overall success of the methodology. The tools selected throughout testing the methodology were focus on equipment that can be easily procure at a low cost. Following the evaluation, a 6- stage process was formulate: deconstruction, identification, removal, and restoration, determine and perform. 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 (Hadgkiss et al., 2022).

2.12 M. L. Wei et al. (2022) has staged a novel analog CIM technique for GEMM using 3D NOR Flash devices to support general-purpose matrix multiplication. The analysis indicated that it's 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 of massive ALU and external DRAM. The researcher states that using ternary similarity search algorithm with positive and negative inputs can weigh to perform high dimension feature vector design. This study demonstrates the potential of NOR Flash memory beyond storage applications (Wei et al., 2022).

2.13Huang et al. (2022) has functioned a 3D NOR memory which 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, stack with multiple doped epitaxial Si layer was used, 3D NAND, bit-line planes, source line planes and vertical word-lines were utilize. 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 us 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 (W. Huang et al., 2022).

2.14B. 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 researcher analysis that as NOR flash memory has larger capacity then NAND or other flash memory it makes it highly suitable for long duration space mission 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 extrapolate based on single run result. The bit error distribution over the word bits, which is 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 device 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 shows that NOR flash selected devices showed to be highly resistant to SEU's and SEFIs under proton radiation (Tanios et al., 2021).

2.15W. 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 purpose. The methods of acquisition included direct data download pf 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 files format may provide quality that is equal to or greater than the proprietary file format (Bruehs & Stout, 2020).

2.16R. Gomm et al. (2020) has described a new forensic workflow for acquiring and analyzing artefacts from large amount data from CCTV devices of different models/manufactures, prior to presenting and analyzing three real world case studies. This study showcases the numerous challenges arise with the forensic acquisition and analysis of CCTV data. Such challenges are expanded when considerations is given to the volume of data due to different manufactures, data formats, file systems, volume storage methods etc. This study reviews on current approach on CCTV forensics in literature, and identifying challenges of CCTV forensic (Gomm et al., 2020).

2.17H. Al. Hosani et al. (2020) has awarded a guide with appropriate standards and procedure with which to approach SSDDs. This study shows that SSDDs commonly present at crime scene, 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 (Hosani et al., 2020).

2.18P. 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 cell and extracting physical property of flash memory cells through standard digital interfaces. The imprinting of watermarking into the NOR Flash memory is performed by chip manufactures. The watermark include 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-programed operations are perform 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 errors 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 (Poudel et al., 2020).

2.19N. R. Mistry et al. (2020) has regulated a methodology and guidelines for how to perform the

phase of digital forensic process on Smartphones devices using the Chip- Off technique. The researcher addresses the challenge of data extraction, especially when the phone is logically and physically damages. By using Chip-off removing the Flash memory, Chip and performing direct extraction and analysis. The researcher uses Apple iPhone, which are robust in nature, well locked and has API that can used to implement application level encryption performed Chip-Off on model A1203 that revealed vital forensic evidences (Mistry et al., 2020).

2.20M. Conti et al. (2018) has addressed the existing major security and forensic challenges within IoT networks. This study explains the fast pace of development and nature of IoT environments bring a variety of security and forensic challenges. The researcher briefly explains the major security challenge that exists in IoT environments i.e. Authentication (Key deployment and Key management is a challenge in IoT device authentication), Authentication and Access Control (Deployment and Management of a variety of authorization and access control mechanisms which are tailored to different nodes capabilities is a challenge in heterogeneous IoT network), Privacy (Privacy regulation mandates keeping users informed about how their private data is managed and administered), and Secure Architecture (Detection of malicious traffics rerouted over networks with different natures and hunting for malicious actor is a very challenging task) as well as forensic challenges i.e. Evidence Identification, Collection and Preservation, Evidence analysis and Correlation, and Attack or Deficit Attribution (Conti et al., 2018).

2.21J. Aweya (2018) has delves into the inner working of router and switch designs in comprehensive manner that is accessible to broad audience. The researcher compares centralized Vs distributed design of architecture. This study described the evolution of multilayer switch designs, the role of switch/router in a network, functional composition of switch/router, use of bus versus shared memory for communication within a design, also covers the Quality of Service mechanisms and configuration tools and highlights the major performance issues affecting each designs. It address the need to build faster multilayer switches and examines the architectural constrains imposed by the various multilayer switch designs. This study discuss design issues such as performance, implementation complexity and scalability to higher speeds. The researcher also summarize principle of operation and explores the most common installed routers (Aweya, 2018).

2.22H. Hidaka (2018) has led a comprehensive introduction to embedded Flash memory, history, status, and future projections for technology circuits and system applications. This study demonstrated a variety of embedded applications for automotive, smart-IC cards and low power. The researcher described a mature and stable Floating gate 1Tr cell technology imported from stand-alone Flash memory products that then introduced embedded-specific split-gate memory cell technologies based on floating-gate storage structure and charge-trapping SONOS technology and their eflash sub-system designs. It also explains detailed about history of embedded Flash memory technologies for micro-controller products (Hidaka, 2018).

2.23M. M. Alani (2017) has organized router management activities such as IOS upgrade, backup, restore and copy. The researcher demonstrates the important tips to consider before upgrading the router's IOS, different IOS file naming conventions, how to backup and restore configuration of the router, and Flash memory partitioning and explained the steps to upgrade/fix the IOS in multiple scenarios like router-to-router IOS copy, using TFTP server's and using the terminal emulation software (Alani, 2017).

2.24X. W. Shen et al. (2017) has processed a novel and efficient NoC router mechanism for dataflow

architecture. The researcher analyze and extract the features of data transfers in NoC's of dataflow architecture: multiple destinations, high injection rate, and performance sensitivity to delay. The proposed router supports multi-destination thus it can transfer data with multiple destinations in a single transfer. The researcher evaluates the proposed router with three typical parallel applications suitable for dataflow architecture in double-precision floating point: FFT, stencil and GEMM. The three test cases are examples to show the performance. They are very typical and popular in high performance computing especially in exa-scale scientific computing. The adopted mechanisms can reduce the possibility of congestion in routers and decrease the packet transfer delay in each router (Shen et al., 2017).

2.25MI. Mazdadi (2017) has explored how to do a forensics of Router OS based Mikrotik devices and developing a remote application to extract router data using API services. Mikrotik is a Linux based operating systems on a computer that functioned as a router. This study observed a problem that happen to live forensics is the modification of data or contamination of data, it because the acquisition process is done on the system itself. In the case of taking the log on the server, the servers also keep records on the log of acquisition activity. To overcome this problem, the researcher used API, which is a set of commands, functions, and protocols that can be use by programmers when building an OS, API allows programmers to use standard functions to interact with other OS. Extraction of Router's data with API gives us access to information on a wide variety of activities that are on the network (Muhammad Itqan Mazdadi, 2017).

2.26K. Paulsen (2017) has enact how the transition from linear recording to nonlinear recording and playback have become well-accepted 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 described how various subsystems that manage the physical storage medium that are applied to the drive configuration (Paulsen, 2017).

2.27Y. Chen et al. (2017) has functioned a Linux-base embedded DVR monitoring system. This study explains that the kernel driver of receiving chip is design for Hi3520D to control its receiving mode, so that the video data captured by the camera is transferred to data receiver, which carries, on the AD conversion and the data preprocessing via BT.656 interface. The researcher uses output interface and network transmission to complete playback operation. In order to implement the parallel operations of the multifunction module, the researcher achieved following functions, such as video data acquisition, flow configuration of video encoding and decoding. The video data is transmit via RTSP\RTP protocol to attain the goal of network video surveillance (Yi et al., 2017).

2.28O. Friard (2016) has purveyed an open source tool called BORIS for video/audio coding and live observations. This study addressee the challenge that researchers frequently face the need to code considerable quantities of video recording with relatively flexible software, often constrained by species-specific options or exact settings. To resolve this problem the researcher introduced an open-source and multiplatform standalone program that allows user-specific coding environmental to be set for a computer-based review pf previously recorded videos and live observations. The observation data can be export in many common formats (TSV, CSV, ODF, XLS, SQL, and JSON). The observed events can be plotted and exported in various graphic formats (PNG, TIFF and PDF) (Friard & Gamba, 2016).

2.29A. Biswas et al. (2015) has exhibited a security framework for Network-on-Chip system by analyzing routing and addressing attack on router tables. This study gives four countermeasures: Security using Run-time protector, Security using Restart-time protector, Security auditor and Non-volatile memory for source address authentication. In addition to detection and prevention, proposed protectors can locate a malicious router also. The researchers used Blue spec System Verilog for design and process, performing by updating the routing table with correct data for normal operations, using artificial traffic generators to generate traffic, stimulating attack on router by loading malicious routing table. The results shows that the area of Run-time protector and a Restart-time protector is only 6.6% and 2% of a conventional router area (Biswas et al., 2015) .

2.30D. Yadav et al. (2013) has unveiled the use of mobile devices in various activities and mobile forensic briefly. The researchers examines the challenges of mobile forensic investigations i.e. Operating System, Volatility of data, Hardware technology innovations, Forensic tools and admissibility of acquired mobile data as electronic evidence in Indian Jurisdiction. This paper highlighted the critical stages of mobile forensic and weakness in acquisition of digital evidences from mobile devices. This study contains a systematic guide in context of mobile forensic process model i.e. Stage 1 (Identification), Stage 2 (Evidence Acquisition), Stage 3 (Examination and Analysis) and Stage 4 (Reporting) and preservation of data from mobile devices and examination of those data with respect to the Indian Acts to admit those Digital evidences in Indian Courts (Yadav et al., 2013).

METHODOLOGY

3.1 Methodology Selection and Justification

Chip-Off Acquisition is an invasive and progressive methods. It accompanied when other Acquisition methods are failed to extract the data.

- Logical Extraction: It is fast and non-destructive process but when the condition of the device is non-working it unable to extract the data.
- JTAG Extraction: it is non- destructive process but it connects via access ports.
- Chip-Off Acquisition: it involves the physical removal of chip from the device followed by reading and analyzing the extracted data, it is destructive method but it overcomes the issue of other acquisitions.

3.1.1 Justification:

- Condition of Device: In a crime scence, the device will not be in a working condition the perpetrator would try to destroy it even if the device would be burned broken or encrypted with a code. By Chip-Off Acqusiton it will extract the data.
- Type of Data: Routers stores firmware, logs, username, password, and login credentials where as DVR stores domain.txt, url.txt, and exif.txt, domain.histogram.
- Bypassing encryption: Chip reading directly through the chip would help to access the data directly so it would bypass the encryption.

3.2 Choice of approach

The study entitled ‘Forensic Chip-Off Acquisition of NOR Flash Memory in Router’s and

DVR's' is mixed approach as-

3.2.1 Qualitative Data:

3.2.1.1 Steps of Procedure

- Physical removal of chip from the PCB
- Cleaning the chip
- Using chip reader to read and extract the binary data.
- Using specialized software to analysis the data.

3.2.1.2 Devices

- Router- it stores firmware, username, resolved address and log credentials
- DVR- it stores the domain list, web page lists, exif.txt and domain.histogram.

3.2.2 Quantitative Data:

➢ Router NOR Flash Memory

- Typical Storage: it stores 7-64 MB
- Quantity of Device: 5 Routers
- Time Required for the process: 2 hours per chip

➢ DVR NOR Flash Memory

- Typical Storage: it stores 15- 255 MB
- Quantity of Device: 5 DVR
- Time Required for the process: 2 hours per chip

3.3 Pros and Cons of Methodology

3.3.1 Pros of Methodology:

- Chip reader reading, the chip directly which helps in bypassing the encryption.
- It overcome the issues of other acquisition when other extraction method failed to acquire data.
- It works well for the non-working devices.

3.3.2 Cons of Methodology:

- It requires a lot of time and patience for the extraction of data.
- It requires specialized tools for analysis, if not then it would be difficult to analyze the data.
- Chip reader should be connected properly with the software to extract the binary.

Study Type:

- Condition of Controlled lab and Experimental procedures.
- Including both functional and non-functional devices from scrap market.

3.4.2 Independent Variable:

- Method of Extraction- Chip-Off, JTAG, ISP or logical extraction.
- Type of Device- DVR's and Router's with NOR Flash memory architecture.
- Condition of Device- Working, Non-working or Partially damaged.

- Software used- Binwalk, Hexeditor, Bulk Extractor and Wireshark.

3.4.3 Dependent Variable:

- Data integrity- Verified by hash values generated by file property of Wireshark.
- Required Time- Depends on every chip 1-2 hrs.
- Unsuccessfully extraction- The extraction of Hikvision DVR is unsuccessful might be the small file size, corrupt folder or software limitation.
- Completeness of extracted data- The data has been extracted partially and completely.

3.4 Ethical Consideration

- Destructive process- Chip-Off Acquisition permanently alters the device. It should be use as a last option for data extraction when other method fails.
- Documentation- Documenting each and every step to maintain the integrity of evidence.
- Transparency- The risks, methods, limitations and all the possibility should be disclosed in research to avoid misleading.

3.5 Data Protection

- Minimization of data- Extracting only necessary or forensic artifacts rather than full dump.
- Data Encryption- Securing the data with encrypted code with restricted access.
- Hashing checks- Using cryptography methods such as SHA-256 to all the files to ensuring no tampering happens during the procedure.
- Legal admissibility- Maintaining the chain of custody, using validated tools and software, photographing the each and every process to present in court of law.
- Accompany with GDRP- In case of extraction of personal data, the privacy regulations and rules should be maintained.

3.6 Research Design and Procedures

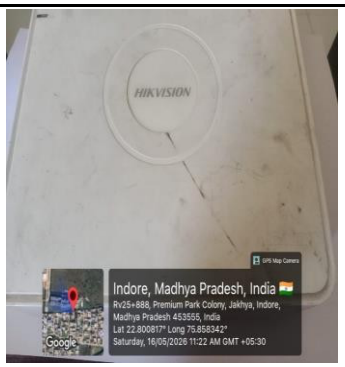
3.8.1 Collection of Sample

- The sample is collected from the scrap market through vendor 10 devices i.e. 5 Router's and 5 DVR's.
- Before handling the device, documentation must be performed which includes photographing the device and recording device information.
- In Sample Numbering and code, the OUI is considered as Oriental University Indore, R is considered as Router, D is considered as DVR and FS is considered as Forensic Science.

Table 1.1: Description of Devices

Sr. No	Sample Numbering	Device Model	Device Information	Image

1.	OUI/FS/AD/R/		SSID: DIR-615 MAC: 4086CB8142C7 MTCTE: 594300384	
2.	OUI/FS/AD/R/2	iball baton	IP: 192.168.1.1 S/N: 20205IB09944 MAC: 001EA60B9330 PIN: 56773842	
3.	OUI/FS/AD/R/3	ADSL+2	S/N: 06E16C013389 MAC: 00177C0B065 MODEL N0: GL.B-502T	
4.	OUI/FS/AD/R/4	Netgear	S/N: 2EB3227V02C61 MAC: 2CB05D49B8A0 PIN: 13033750	

5.	OUI/FS/AD/R/5	Tenda	IP: 192.168.0.1	
6.	OUI/FS/AD/D/1	Hikvision	S/N: D94847372 MODEL: DS-7A04HQHI-K1	
7.	OUI/FS/AD/D/2	Cametron	S/N: 2000001059	
8.	OUI/FS/AD/D/3	Secureye	S/N: 271506001575 MODEL: S-AHD-16C	

9.	OUI/FS/AD/D/4	Tejovat	S/N:8098807007 MODEL: AP-ZJ250J-AFE1	
10.	OUI/FS/AD/D/5	Tejovat	S/N: 2120306002 MODEL: AP-H42N-C116	

3.8.2 Instrumental Refinement

Table 1.2: Equipment & Experimental Setup

Sr. No	Equipment	Model Specification	Purpose
1.	Hoki 722 SMD Rework Station	Maximum power output of 280W and a temperature range of 100 to 480 degree C	Desoldering NOR chip from PCB. It includes adjustable knob to control air pressure and temperature
2.	Flux	Mechanic UV559 No-clean Soldering Flux paste	Facilitating solder melting and preventing pin damage
3.	Cleaner	Petrol	Cleaning chip surface after removal from PCB
4.	ENIT BIOS programmer	Handles 1.8V, 3.3V, and 5V SPI BIOS chips, as well as 8-pin and 16-pin chips	Used for reading chips via USB to system
5.	ENIT Software	Software tool	Displaying the binary data from chip
6.	Binwalk Software	Open-Source command-line Tool for analyzing binary files	Extracting the .bin files which is the firmware dump
7.	Wireshark Software	Open-Source Tool for network traffics	Analyzing and viewing network packets
8.	Bubble Plastic	Plastic Wrap	Protecting the device
9.	Cardboard Box	Box	Helps in Storing the device

3.8.3 Preservation of Sample

- Device will be kept in bubble plastic wrapped and stored in cardboard box to prevent it from further damage.

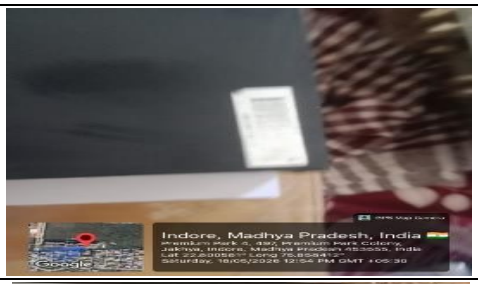
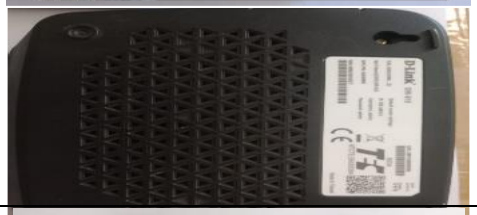
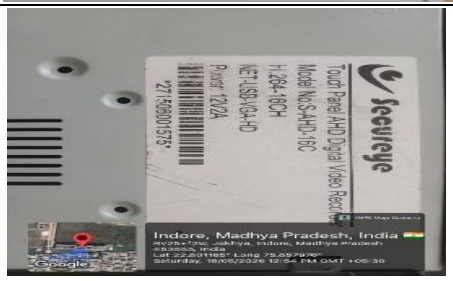
Table 1.3: Sample Preservation

3.8.4 Sample Analysis

Step 1- Identification

Identifying the device make and model. To aid in determining the type and location of the Flash memory chip, the information present on the back of the device such as SSID, MAC address, Default settings etc., will be recorded.

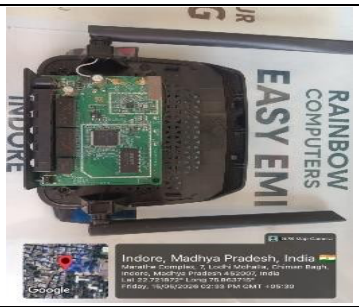
Table 1.4: Device Identification

Step 2- Preparation & Disassembly

The device was then dismantled, and PCB was removed

Table 1.5: Device Disassembly

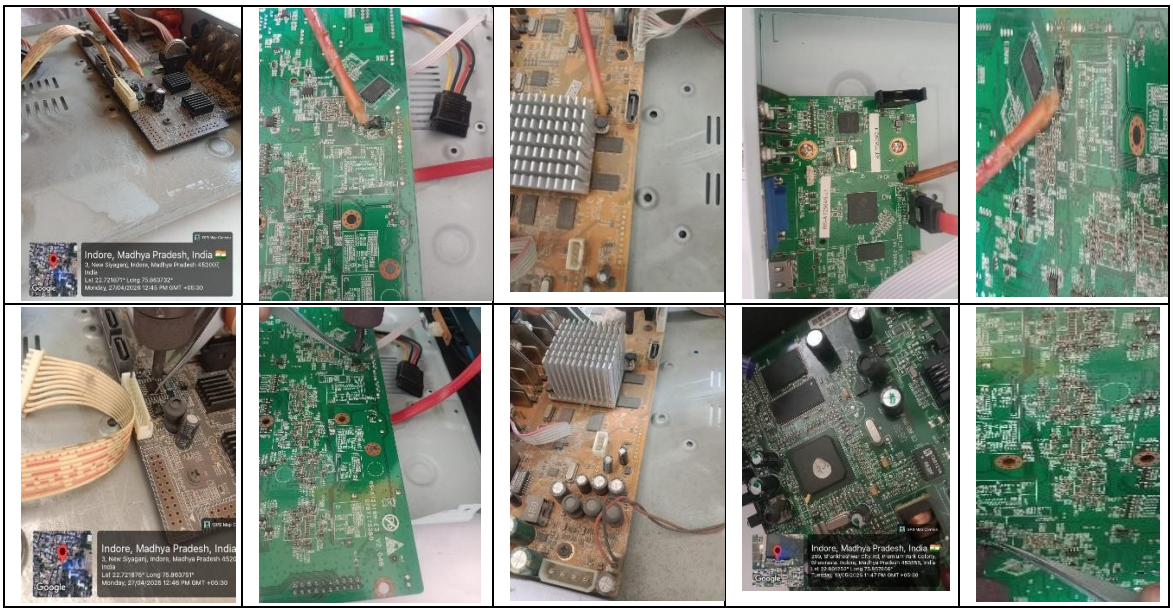
	
	
	
	
	

Step 3- Desoldering

After Dismantling, the flux was applied to all the solder joints, and HOKI 722 SMD heat gun was set to 400 degree C. Pins were evenly heated for approximately 25-30 seconds until the solder is liquefied. A tweezer is then used to gently lift chip from the board.

Table 1.6: Application of Flux

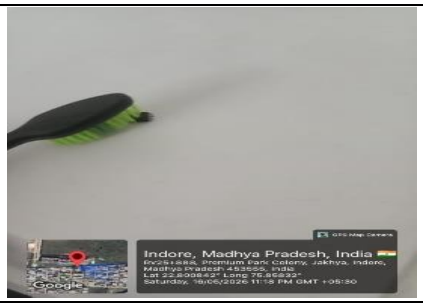
Table 1.7: Removal of Chip using Heat Gun



Step 4- Chip Cleaning

After removing, the chip it will be covered in adhesive and residual solder, which must be cleaned to fit correctly in a chip reader. The chip is cleaned with petrol or any other residue, which will be readily available.

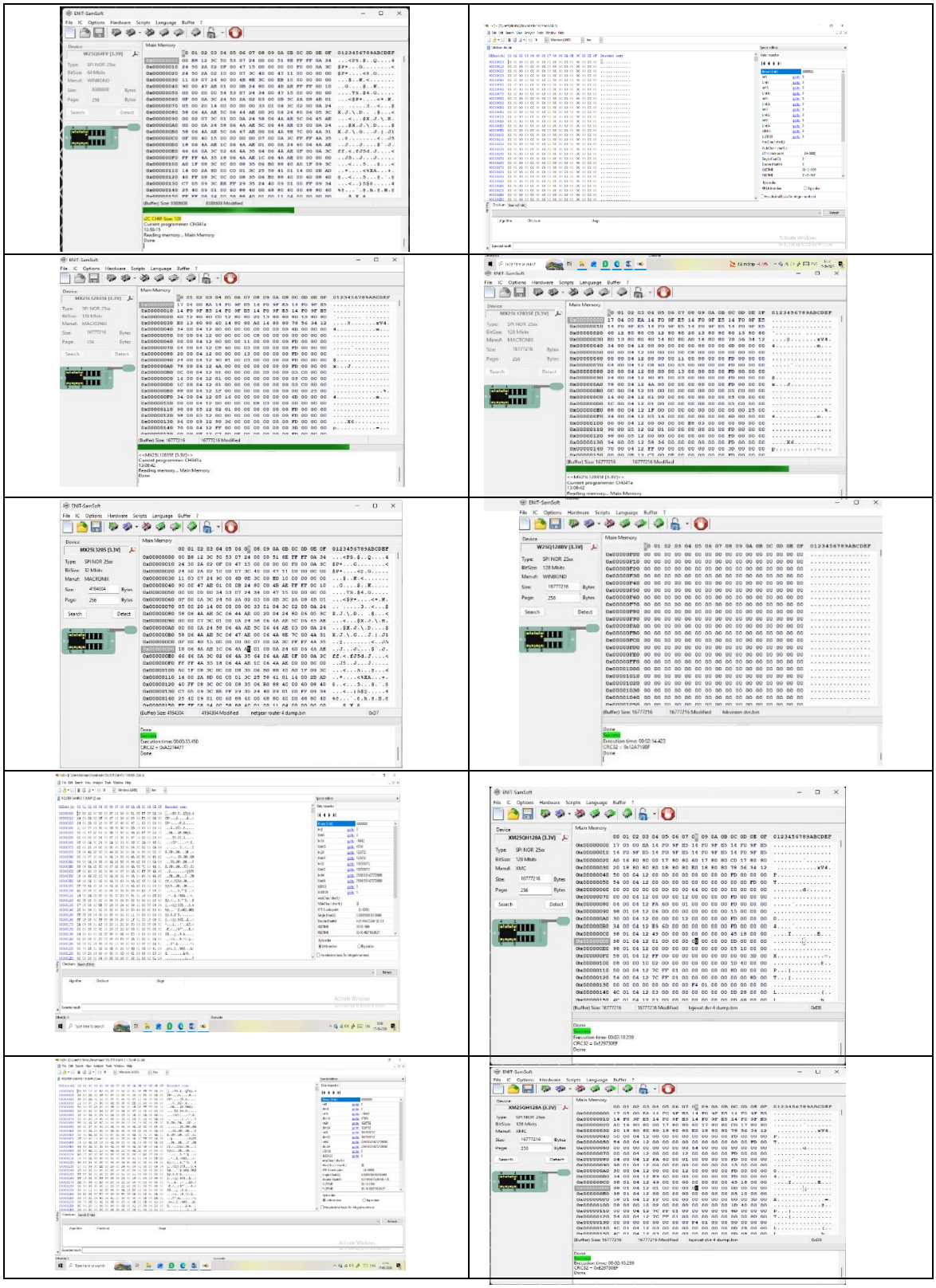
Table 1.8: Cleaning of Chip

Step 5- Chip Reading

Once cleaned, the chip is placed into a chip reader to create the raw image (dump) of the data.

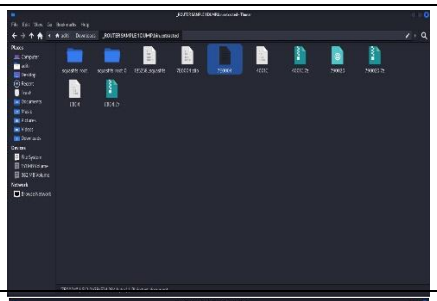
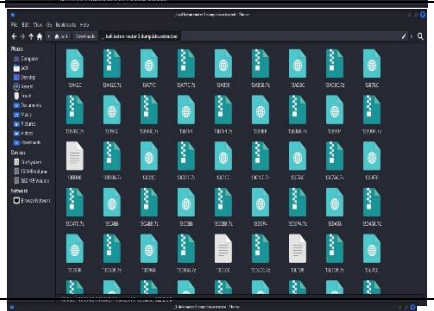
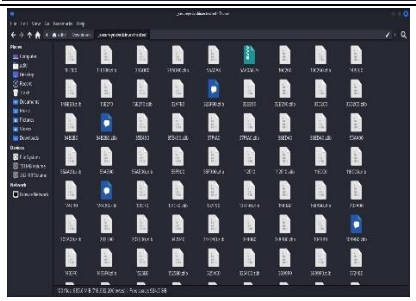
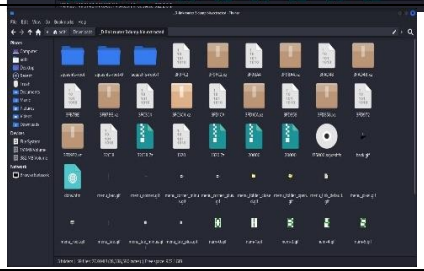
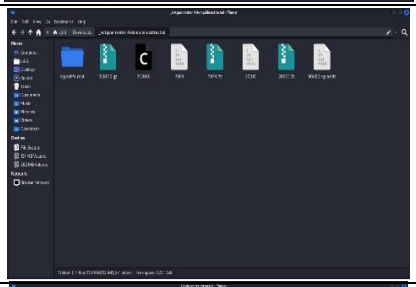
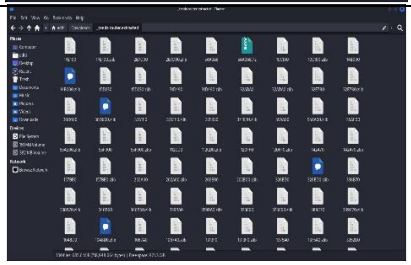
Table 1.9: Process of Chip reading



Step 6- Data Interpretation

The extracted raw dump is not directly readable as it is in binary form and must be processed. The data is extracted using specialized tool such as Binwalk.

Table 1.10: Interpretation of data

	
	
	
	
	No Data has been Extracted from Hikvision DVR

RESULT AND DISCUSSION

A chip-off procedure is performed on 10 Devices i.e., 5 Router's and 5 DVR's. Through the chip-off process, binary data contained in the flash memory is recovered. After Chip –off Acquisition, the .bin file has been analyze of all the devices. The software used in the analysis Binwalk and Bulk Extractor both are command line utility software, which is pre-installed in kali Linux. Binwalk is used to extract the data of Router's Devices whereas Bulk Extractor is used to extract the data of DVR's.

Table 1.11: Recovered Device information

Sample	Memory Type	Bit Size	Data
OUI/FS/AD/R/1	SPI NOR	64 Mbits	512.0 KiB
OUI/FS/AD/R/2	SPI NOR	16 Mbits	410 Files:140.3 MiB
OUI/FS/AD/R/3	SPI NOR	32 Mbits	3 Folders|27.0 MiB
OUI/FS/AD/R/4	SPI NOR	16 Mbits	7 Files: 11.9 MiB
OUI/FS/AD/R/5	SPI NOR	16 Mbits	100 Files: 685.6 MiB
OUI/FS/AD/D/1	SPI NOR	16 M	NIL
OUI/FS/AD/D/2	SPI NOR	128 Mbits	5 Folders| 1778 Files: 979.8 MiB
OUI/FS/AD/D/3	SPI NOR	128 Mbits	100 Files: 685.6 MiB
OUI/FS/AD/D/4	SPI NOR	128 Mbits	3 Folders| 3214 Files: 979.8 MiB
OUI/FS/ADD/5	SPI NOR	128 Mbits	5 Folders| 3291 Files: 1.1 GiB

4.1 Router

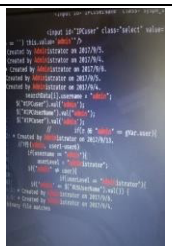
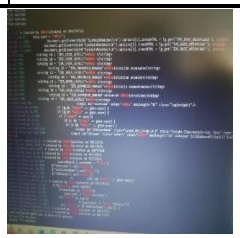
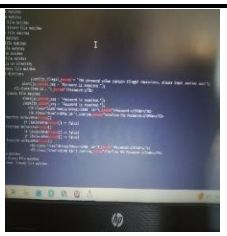
Using Binwalk Software to retrieve the data from the extracted .bin files. By giving command

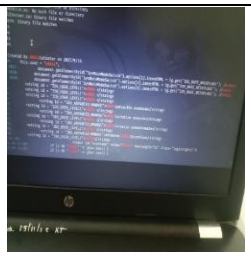
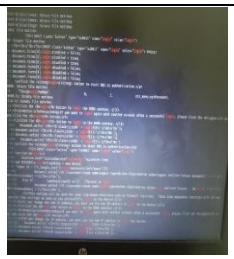
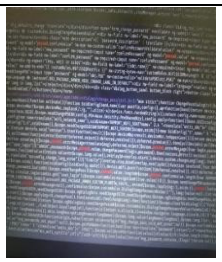
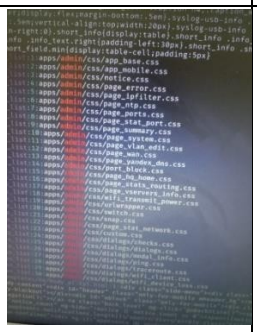
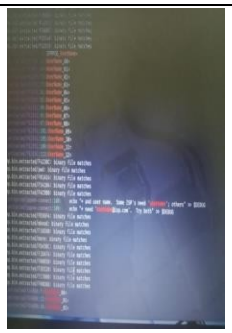
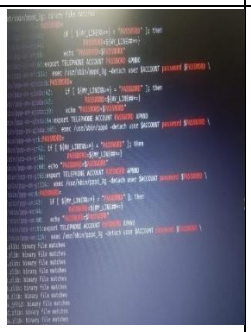
binwalk –e ‘Filename.bin’ e.g. binwalk –e ‘netgear.bin’ and giving specific command to get login, Username/admin, and password from each devices. Performing Wireshark on the extracted file by converting it into .pcap file to analysis Resolved Address, it helps in acknolowdeging MAC Address.

Data extracted from the Router’s:

The password, Login, Username/Admin is extracted through Binwalk using Command grep –Rni ‘login’ , grep –Rni ‘Username/admin’ and grep –Rni ‘‘passwd.

Table 1.12: Extracted data from Router using Binwalk

Sample	Username /Admin	Password	Login	Extracted Data
OUI/FS/AD/R/1	 Admin	 Admin	 The login command showing it resembles that the user has been logging into the accounts	  
OUI/FS/AD/R/2	 Admin	 #password	 Web login or settings page coded with JavaScript	

OUI/FS/AD/R/3	 Admin	 $scope	 Login System	Unsuccessful data extraction
OUI/FS/AD/R/4	 Admin	 12345	 Login System	
OUI/FS/AD/R/5	 Username_01	 MY_LINE*	 Login System	

NOTE:

The file contains low-level binary data. Showing uImage [Kernel image], LZMA [Bootloader image metadata], size value [file size], the image showing colors are highlighting the Syntax like purple is Signature of File system, Red is errors, Green showing metadata. The image showing raw data of binary file that can be machine code, structure of file system etc.

4.2 DVR

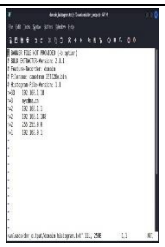
Using Bulk Extractor Software, to retrieve the data from the extracted .bin file. By giving command on bulk extractor –h 'Filename.bin' e.g. bulk extractor –h 'cametron 251128.bin' and giving specific command to get domain.txt, domain.histogram, exif.txt, url.txt and url.histogram. Except for Hikvision DVR, while analyzing in the bulk extractor the data is not extract the reason might be corrupted file or encrypted with code.

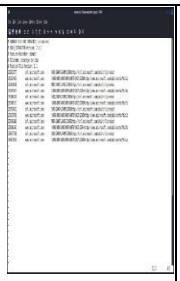
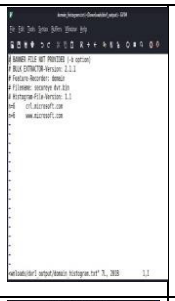
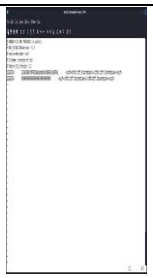
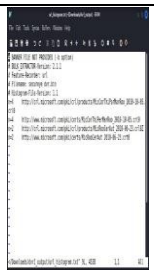
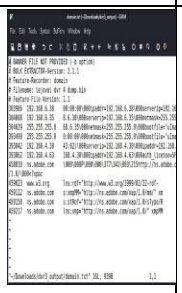
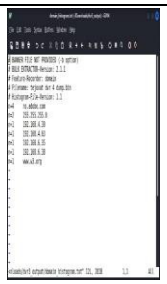
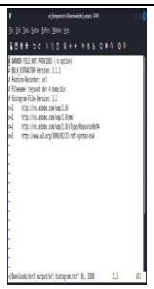
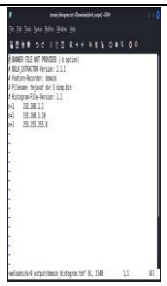
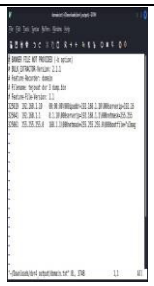
Table 1.13: Setting parameters

Parameters	**Description**
Domain.txt	List of Domains and hostnames
Domain.histogram	List of the extracted Domain
Exif.txt	Stores image and metadata
url.txt	List of web address
url.histogram	List of all extracted web address

Table 1.14: Extracted data from DVR using Bulk Extractor

Sr. no	**Sample**	**Domain. txt**	**Domain. histogram**	**Exif. txt**	**url.txt**	**url. histogram**
1.	**OUI/FS/AD/D/1**	**Unsuccessful extraction**	**Unsuccessful extraction**	**Unsuccessful extraction**	**Unsuccessful extraction**	**Unsuccessful extraction**

2.	**OUI/FS/AD/D/2**			**Unsuccessful extraction**	**Unsuccessful extraction**	**Unsuccessful extraction**

3	**OUI/FS/AD/D/3**					
4.	**OUI/FS/AD/D/4**			**Unsuccessful extraction**		
5.	**OUI/FS/AD/D/5**			**Unsuccessful extraction**	**Unsuccessful extraction**	**Unsuccessful extraction**

OUI/FS/AD/R/1	OUI/FS/AD/R/2	OUI/FS/AD/R/4	OUI/FS/AD/D/2	OUI/FS/AD/D/3	OUI/FS/AD/D/5

Resolved address

00:00:1c	Bell Technologies	00:01:02	3Com	00:60:3b	AMTEC spa	00:00:91	Anritsu Corporation	00:08:bf	Aptu Elek k AI
00:02:00	Net & Sys			:00:4e	Ampex Corporation	00:00:76	Abekas Video Systems	00:03:00	Barr a Netv s, In
00:00:44	Castelle Corporation	00:04:55	ANTARA.net	01:00:1d	Cabletron	00:30:00	Allwell Technology Corp.	08:00:33	Baus & L
00:84:1e	Cisco Meraki	00:01:c0	Compu Lab, Ltd.	01:13:80	Cisco Systems, Inc	00:00:b1	Alpha Micro	01:13:09	Ocea Broa nd Netv s.
00:01:00	Equip Trans	00:00:69	Concord Communications Inc	00:00:72	Miniware Technology	00:00:a4	Acron Computers Limited	00:00:de	Ceti
00:00:70	Hcl Limited	00:00:8d	Cryptek Inc,			00:00:d1	Adaptec Incorporated	00:60:3e	Cisc Syst Inc
00:11:1d	Hectrix Limited	00:03:f6	Allergo Networks.			00:00:4a	Adc Codenoll Technology Corp.	01:09:46	Clus Labs Gmb
			Dell EMC	41:a6:3d	SignalFire Telemetry	00:00:71	Adra Systems Inc.	00:01:00	Equi Tran
00:20:00	Lexmark Internati onal, Inc.	00:00:cc	Densan Co., Ltd.	00:00:02	Xerox Corporation	00:00:1a	Adavanced Micro Devices	08:00:14	Exce

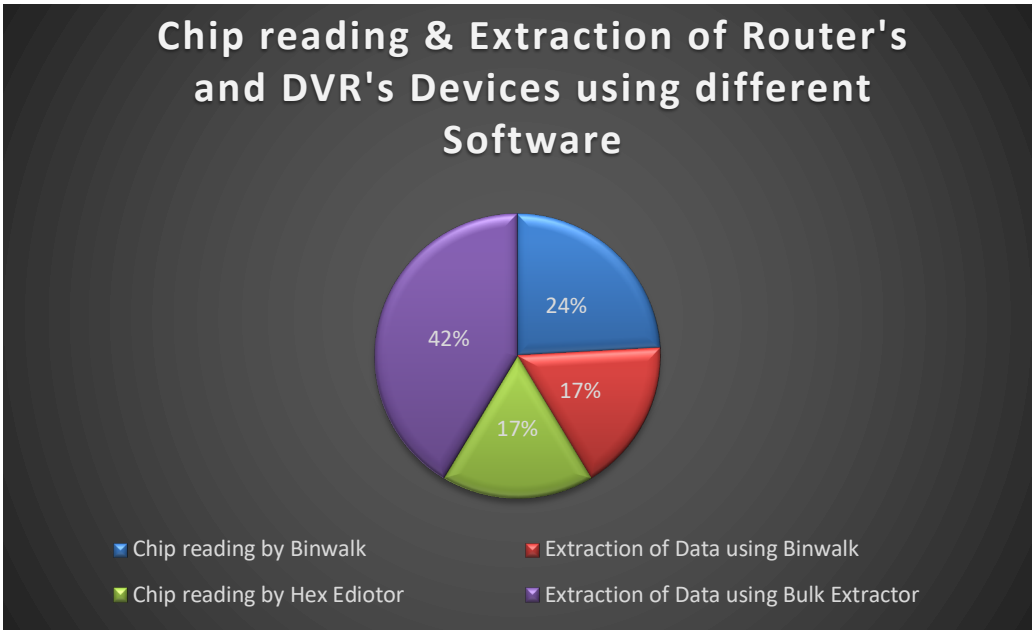
00:00:68	Rosemount Controls	00:00:56	Dr. B. Struck			00:01:aa	Airspan Communications	00:15:83	IVT corpon

Table 1.15: Chip reading and Extraction of data from Router's and DVR's Devices using Binwalk, Hexeditor and Bulk Extractor

The result shows that the completely extracted data is considered as 100%, Partially extracted data is considered as 50 %, and the data which is not extracted is considered as 0%.

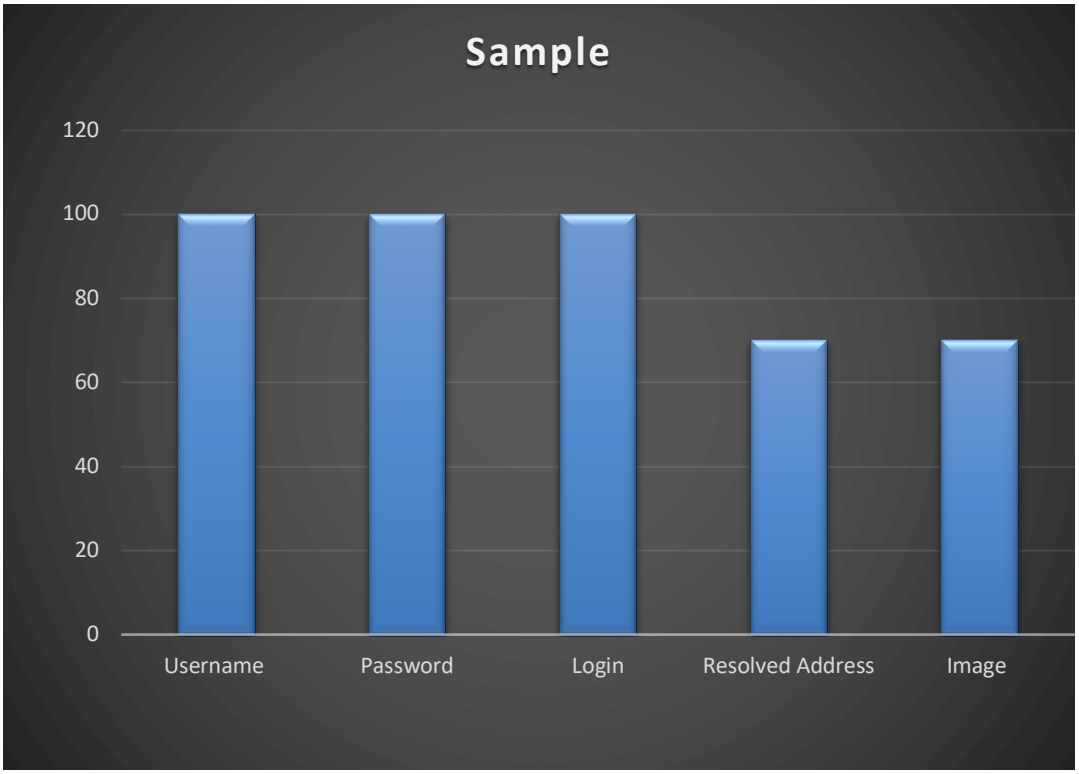
Sample	Chip reading by Binwalk Software [A]	Extraction of Data by Binwalk Software [B]	Chip reading by Hexeditor [C]	Extraction of data by Bulk Extractor Software [D]
OUI/FS/AD/R/1	□	□	×	×
OUI/FS/AD/R/2	□	□	×	×
OUI/FS/AD/R/3	□	□	×	×
OUI/FS/AD/R/4	×	□	□	×
OUI/FS/AD/R/5	×	□	□	×
OUI/FS/AD/D/1	×	×	□	□
OUI/FS/AD/D/2	□	×	×	□
OUI/FS/AD/D/3	□	×	×	□
OUI/FS/AD/D/4	□	×	×	□
OUI/FS/AD/D/5	□	×	×	□

□□□□□



□□□□

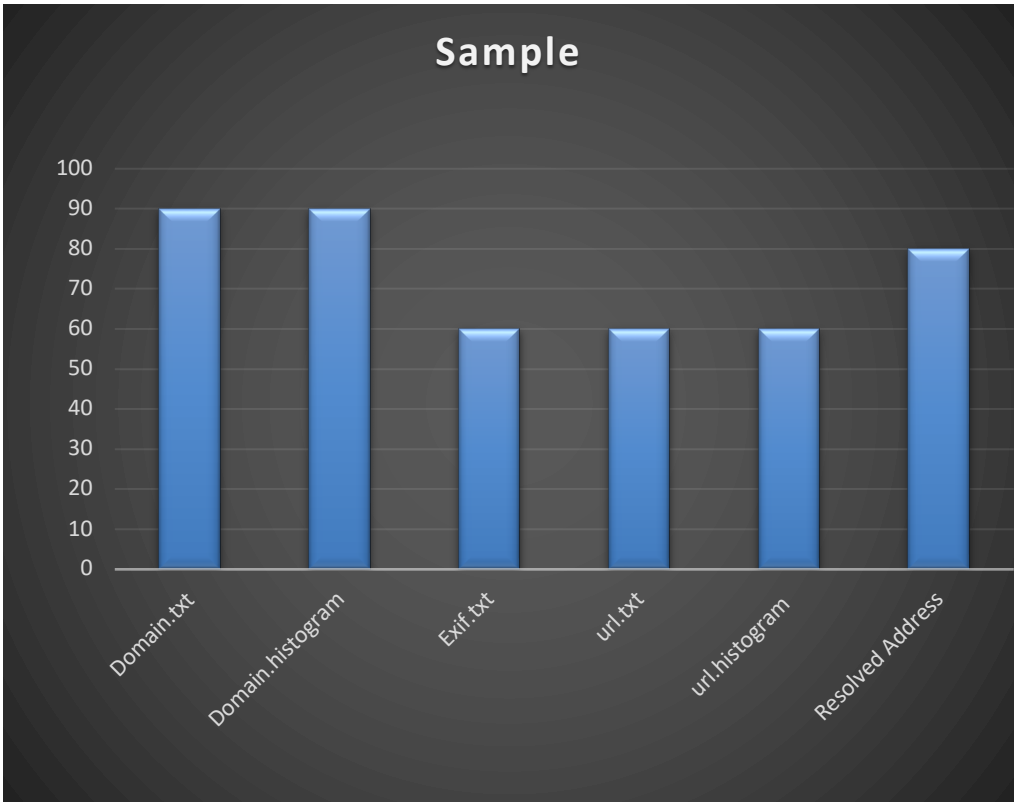
Pie chart 1.1: Chip reading and Extraction of Router's and DVR's Devices □



Histogram 1.1: Analyzing the data extracted from Router's Devices

Table 1.16: Analyzing the data extracted from Router's Deices

Sample	Username	Password	Login	Resolved Address	Image
OUI/FS/AD/R/1	□	□	□	□	□
OUI/FS/AD/R/2	□	□	□	□	□
OUI/FS/AD/R/3	□	□	□	□	×
OUI/FS/AD/R/4	□	□	□	×	□
OUI/FS/AD/R/5	□	□	□	×	×



Histogram 1.2: Analyzing the data extracted from DVR's Devices

Table 1.17: Analyzing the data extracted from DVR's Devices

Sample	Domain. txt	Domain. histogram	Exif. txt	url. txt	url. histogram	Resolve Address
OUI/FS/AD/D/1	×	×	×	×	×	×
OUI/FS/AD/D/2	□	□	×	×	×	□
OUI/FS/AD/D/3	□	□	□	□	□	□
OUI/FS/AD/D/4	□	□	×	□	×	×
OUI/FS/AD/D/5	□	□	×	×	×	□

DISCUSSION

The research shows that the data from Router's and DVR's would be very beneficial in an investigation. The data extracted can be helpful in knowing the username, password, login web page, resolved address, domain name, web pages and images. Our findings states that using Chip-off method as an Acquisition is systematic and progressive method that recover the data from the devices which are in non-working, conditions, password protected, encrypted, burned, and physically damaged. From the previous studies, the Chip-Off Acquisition has been used on Android phone which is password protected and the person has been deceased, so the only way to recover the data is by using Chip-Off method and it successfully retrieve the data. Comparably to NAND Flash Memory, NOR flash memory has been increasingly popular for RAM-restricted microcontrollers due to its small package and high reliability. The success rate of chip off acquisition of NAND Flash Memory has been observed successfully whereas in NOR Flash Memory the success rate has limited research.

The research has very limited focus in Chip-Off Acquisition. The fact that we found in our study, that the data can be easily recover from the device with minimum time. This study approaches in a systematic way that how to perform Chip-Off Acquisition in NOR Flash Memory in Router's and DVR's Devices. Router's and DVR's are seen in every place which can be your home, office, university, apartments etc. By using Chip-Off Acquisition, the extracted data will be very helpful in future aspects. The research on this field is very limited so, there is a growing need to develop researches that are more scientific on this area. Although every steps has some complexities namely, removal of the chip needs precise temperature, application of flux etc. Another goal is to analyze the data, which is an arduous process; we can say that the protagonist of this procedure is Software. It depends on the software how to work and what type of data should be extracted. Selecting Software is the foremost thing which every investigator should follow. Finally, the approach of this study would aid in investigation to collect the evidences from Router's and DVR's.

CONCLUSION

This research performed the extraction of data from Router's & DVR's Devices is helpful and evidentiary value in investigation. In case of physically damaged device, burned, locked or password protected data, recovery is particularly valuable because by which information can be analyzed. In this process, many challenges kept evolving. To solve this, the Chip-Off method is a hardware level data extraction process for extracting data by physically removing the chip and accessing the data directly through chip reader. The retrieved data is then processed and analyzed using specialized software. The tests are performed on 10 devices which shows that Chip-Off Acquisition is an invasive and distinctive process. The Open source software which has been utilized in the procedure is Binwalk, Hex editor, Bulk Extractor and Wireshark which are easily assessable and easy to use. The success of this Acquisition is based on the type of device examined, chip reader and software utilized which showed when combined Chip-off with software's such as Binwalk, Hex editor, Bulk Extractor and Wireshark showed 98% success.

Several challenging circumstances are observed, while performing the procedure such as incomplete or unsuccessful extraction of Hikvision DVR, due to the limitation of the software screenshot is unable to take, Complex nature of Chip-off process, and human error can still occur. From the previous literature, it is shown that NOR Flash Memory serve as a Non-Volatile Storage Medium and can store firmware, image, Bootloaders etc. The findings of this research demonstrates that data recovery from NOR Flash Memory through Chip-Off Acquisition is a delicate and technical process ensuring integrity of data and the utilization of software are all critical to successful extraction. Overall, this provides a comprehensive perspective that the chip off Acquisition can be conducted on NOR Flash Memory for the extraction of data from the embedded device.

REFERENCES

Muhammad Tuhin**.** (2025). The Evolution of Technology: From the Stone Age to Today. Available from: https://www.sciencenewstoday.org/the-evolution-of-technology-from-the-stone-age-to-today.

Shepherd, J. (2004). What is the Digital Era? In *Social and Economic Transformation in the Digital Era* (pp. 1–18). IGI Global. Available from: https://doi.org/10.4018/978-1-59140-158-2.ch001.

Pandey, P., & Kapoor, A. (2025). CYBERCRIME IN THE DIGITAL ERA: IMPACTS, AWARENESS, AND STRATEGIC SOLUTIONS FOR A SECURE FUTURE. *Sachetas*, *4*(1), 32–37. Available from: https://doi.org/10.55955/410004.

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

Avanoz, T., & Akbal, E. (2025). Data Recovery Application from NAND Flash Memories Using the Chip-Off Technique in Digital Forensics. *International Journal of Innovative Engineering Applications, 9(2), 232-242. Available from:*

https://doi.org/10.46460/ijiea.1797801.

Kumar Akhlesh, G. B. M. K. (2021). DATA EXTRACTION FROM PASSWORD PROTECTED MOBILE PHONE BY USING CHIP-OFF METHOD –A FORENSIC CASE STUDY. *International Journal of Engineering Sciences & Research Technology*, *10*(3), 28–37. Available from: https://doi.org/10.29121/ijesrt.v10.i3.2021.5.

Jessica Hopkins. (2021, October 27). *What is Flash Memory? Introduction, Types, Examples, and Applications.* Available from: https://www.totalphase.com/blog/2021/10/what-is-flash-memory-introduction-types-examples-applications/.

Sanvido, M., Chu, F. R., Kulkarni, A., & Selinger, R. (2008). nand Flash Memory and Its Role in Storage Architectures. *Proceedings of the IEEE*, *96*(11), 1864–1874. Available from: https://doi.org/10.1109/JPROC.2008.2004319.

Stephen J. Bigelow and Margaret Jones. (2023, May 12). *NAND flash memory. NOR Flash: Working, Structure, and Applications* . (2021, November 18). Available from: https://www.techtarget.com/searchstorage/definition/NAND-flash-memory.

What is a Digital Video Recorder(DVR)? (n.d.). Retrieved May 21, 2026. Available from: https://senstar.com/senstarpedia/what-is-dvr/.

What is a Router? (n.d.). Retrieved May 21, 2026, Available from: https://www.cloudflare.com/learning/network-layer/what-is-a-router/.

Zhasmin Kadyr, A. A. (2025). Intelligent chip off and imaging methods for extracting data from legacy HDDs. In Biloshchytsky Andrii, Zhakiyev Nurkhat, Abitova Gulnara, Yessenbek Sanida, & Baitulakov Anuar (Eds.), 1st international Scientific and Practical Conference(ICCSDFAI-25) (pp. 396–400). Decision of the Scientific and Technical Council of Astana IT University LLP dated 16.04.2025, protocolNo. Available from: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Intelligent+chip+off+and+imaging+methods+for+extracting+data+from+legacy+HDDs.&btnG=.

Avanoz, T., & Akbal, E. (2025). Data Recovery Application from NAND Flash Memories Using the Chip-Off Technique in Digital Forensics. *International of innovative Engineering Applications*, *9*(2),232–242. Available from: https://doi.org/10.46460/ijiea.1797801.

Serm, T.-B., Chen, T.-C., Wang, P.-K., Wu, Y.-D., Chan, T.-Y., Chiang, M.-H., & Ho, Y.- H. (2025). Experimental and modeled analysis of source-line loading effects in NOR flash compute-in-memory arrays. *Applied Physics Letters*, *127*(20). Available from: https://doi.org/10.1063/5.0304098.

Huang, H., Pan, Y., Xia, W., Zou, X., Yang, D., Shi, L., & Du, H. (2025). 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*, 1076–1090. Available from: https://doi.org/10.1145/3676641.3716272.

Rzayeva, L., Shayakhmetov, M., Atanbayev, Y., Budenov, R., & Mutaher, H. (2025). Automated Forensic Recovery Methodology for Video Evidence from Hikvision and Dahua DVR/NVR Systems. *Information*, *16*(11), 983. Available from: https://doi.org/10.3390/info16110983.

Sutikno, T., & Busthomi, I. (2024). Capabilities of cellebrite universal forensics extraction device in mobile device forensics. *Computer Science and Information Technologies*, *5*(3), 254–264. Available from: https://doi.org/10.11591/csit.v5i3.p254-264.

Shaikh, S., Deng, L., & Xu, W. (2024). A Practical Survey of Data Carving from Non-Functional

Android Phones Using Chip-Off Technique. In Shahram Latifi (Ed.), *ITNG 2024: 21st International Conference on Information Technology- New Generations (ITNG 2024)* (pp. 43–50). Springer, Cham. Available from: https://doi.org/10.1007/978-3-031-56599-1_6.

Kim, S. S., Yong, S. K., Kim, W., Kang, S., Park, H. W., Yoon, K. J., Sheen, D. S., Lee, S., & Hwang, C. S. (2023). Review of Semiconductor Flash MemoryDevices for Material and Process Issues (Adv. Mater. 43/2023). *Advanced Materials*, *35*(43). Available from: https://doi.org/10.1002/adma.202370310.

Tiwari, N., Baroniya, Y., Bharadwaj, V., Kumar, A., & Srivastava, A. (2023). Cyber and Digital Forensic. In Pankaj Shrivastava, Jose Antonio Lorente, Ankit Srivastava, Ashish Badiye, & Neeti Kapoor (Eds.), *Textbook of Forensic Science* (pp. 773–803). Springer Nature Singapore. Available from: https://doi.org/10.1007/978-981-99- 1377-0_25.

Alshenaifi, I. M., Qazi, E. U. H., & Almorjan, A. (2023). IoT Forensics: Machine to Machine Embedded with SIM Card. In Shahram Latifi (Ed.), *ITNG 2023 20th International Conference on Information Technology-New Generations (ITNG 2023)* (pp. 133–142). Springer, Cham. Available from: https://doi.org/10.1007/978-3-031- 28332-1_16

Aweya, James. (2018). *Switch/Router Architectures : Shared-Bus and Shared- Memory Based Systems*. Wiley-IEEE Press Available from: books.google.com.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78*, 544–546. Available from: https://doi.org/10.1016/j.future.2017.07.060.

Hadgkiss, M., Morris, S., Paget, S., Ventress, A., & Norris, K. (2022). Cheap as chips: An accessible chip off acquisition method for ball grid array (BGA) integrated circuits in digital investigations. *Forensic Science International: Digital Investigation*,*42–43*, 301481. Available from: https://doi.org/10.1016/j.fsidi.2022.301481.

Wei, M.-L., Lue, H.-T., Ho, S.-Y., Lin, Y.-P., Hsu, T.-H., Hsieh, C.-C., Li, Y.- C., Yeh, T.-H., Chen, S.-H., Jhu, Y.-H., Li, H.-P., Hu, H.-W., Hung, C.-H., Wang, K.-C., & Lu, C.-Y. (2022). 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 Device Meeting (IDEM),*33.3.1-33.3.4. Available from: https://doi.org/10.1109/IEDM45625.2022.10019495.

Huang, W., Zhu, H., Li, J., Yan, Z., Zhang, Y., Wang, Q., Ai, X., Xiao, Z., Kong, Z., Xiang, Zhao, J., Wu, Z., Li, J., Luo, J., Wang, W., & Ye, T. C. (2022). A Novel 3D NOR Flash With Single-Crystal Silicon Channel: Devices, Integration, and Architecture. *IEEE Electron Device Letters 43*(11), 1874–1877. Available from: https://doi.org/10.1109/LED.2022.3211174.

Tanios, B., Kaddour, M., Forgerit, B., Guerre, F. X., & Poivey, C. (2021). Single Event Effects Characterization of 55-65nm NOR Flash for Space Applications. *2021 21th European Conference on Radiation and Its Effects on Components andSystems (RADECS)*, 1–4 Available from: https://doi.org/10.1109/RADECS53308.2021.9954491.

Bruehs, W. E., & Stout, D. (2020). Quantifying and Ranking Quality for Acquired Recordings on Digital Video Recorders. *Journal of Forensic Sciences*, *65*(4), 1155–1168. Available from: https://doi.org/10.1111/1556-4029.14307.

Gomm, R., Brooks, R., Choo, K.-K. R., Le-Khac, N.-A., & Hew, K. W. (2020). CCTV Forensics in the Big Data Era: Challenges and Approaches. In Nhien-An Le-Khac & Kim-Kwang Raymond Choo (Eds.), *Studies in big data* (Vol. 74, pp. 109–139). Springer, Cham.

Available from: https://doi.org/10.1007/978-3-030-47131-6_6.

Hosani, H. Al, Yousef, M., Shouq, S. Al, & Iqbal, F. (2020). State of the Art in Digital Forensics for Small Scale Digital Devices. *2020 11th International Conference on Information and Communication Systems (ICICS)*, 072–078. Available from: https://doi.org/10.1109/ICICS49469.2020.239531.

Poudel, P., Ray, B., & Milenkovic, A. (2020). Flashmark: Watermarking of NOR Flash Memories for Counterfeit Detection. *2020 57th ACM/IEEE Design Automation Conference* 1-6 Available from: https://doi.org/10.1109/DAC18072.2020.9218521.

Mistry, N. R., Koshy, B., Dahiya, M., Chaudhary, C., Patel, H., Parekh, D., Kotak, J., Nayi, K., & Badva, P. (2020). iPhone Forensics. In *Digital Forensics and Forensic Investigations* (pp. 308–324). IGI Global. Available from: https://doi.org/10.4018/978-1-7998-3025-2.ch021.

Hidaka, H. (2018). *Embedded Flash Memory for Embedded Systems: Technology, Design for Sub-systems, and Innovations* (H. Hidaka, Ed.). Springer International Publishing. Available from: https://doi.org/10.1007/978-3-319-55306-1.

Alani, M. M. (2017). Cisco Router Management. In *Guide to Cisco Routers Configuration* (pp. 183–206). Springer International Publishing. Available from: https://doi.org/10.1007/978-3-319-54630-8_7

Shen, X.-W., Ye, X.-C., Tan, X., Wang, D., Zhang, L., Li, W.-M., Zhang, Z.-M.,Fan, D.-R., & Sun, N.-H. (2017). An Efficient Network-on-Chip Router for Dataflow Architecture. *Journal of Computer Science and Technology*, *32*(1), 11–25. Available from: https://doi.org/10.1007/s11390-017-1703-5.

Muhammad Itqan Mazdadi, I. R. A. L. (2017). Live Forensics on RouterOS using API Services to Investigate Network Attacks . *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(2), 406–410. Available from: https://sites.google.com/site/ijcsis/ ISSN 1947-5500.

Paulsen, K. (2017). Video Recording, Servers, and Storage. In *National Association of Broadcasters Engineering Handbook* (pp. 677–744). Routledge.
Available from: https://doi.org/10.4324/9781315680149-39.

Yi, Q., Shi, M., & Chen, Y. (2017). The Design of Surveillance System Based on Hi3520D. *2017 5th International Conference on Mechanical, Automotive and Materials Engineering (CMAME)*, 305–309 Available from: https://doi.org/10.1109/CMAME.2017.8540186.

Friard, O., & Gamba, M. (2016). BORIS : a free, versatile open-source event- logging software for video/audio coding and live observations. *Methods in Ecology and Evolution*, *7*(11), 1325–1330. Available from: https://doi.org/10.1111/2041- 210X.12584

Biswas, A. K., Nandy, S. K., & Narayan, R. (2015). 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)*, 1–6. Available from: https://doi.org/10.1109/CONECCT.2015.7383936.

Yadav, D., Mishra, M., & Prakash, S. (2013). Mobile Forensics Challenges and Admissibility of Electronic Evidences in India. *2013 5th International Conference on Computational Intelligence and Communication Networks*, 237–242. Available from: https://doi.org/10.1109/CICN.2013.57.