International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 10, Issue 06, ISSN No. 2455-2143, Pages 15-19
Published Online October 2025 in IJEAST (http://www.ijeast.com)

DIGITAL FORENSIC TECHNIQUES FOR DAMAGED DIGITAL DEVICES: A COMPREHENSIVE REVIEW AND PRACTICAL APPROACH

Mr. Kapil B. Morey
Directorate of Forensic Science Laboratories,
Home Department Government of Maharashtra,
Mumbai, India

Mr. Vishal S. Pawade
Directorate of Forensic Science Laboratories,
Home Department Government of Maharashtra,
Mumbai, India

Dr. Vijay J. Thakare
Directorate of Forensic Science Laboratories,
Home Department Government of Maharashtra,
Mumbai, India.

Abstract—**Digital forensic investigations often confront scenarios involving damaged digital devices due to physical destruction, environmental exposure, or intentional tampering. Digital devices play a critical role in modern investigations, serving as vital sources of evidence. However, in many cases, these devices are intentionally or unintentionally damaged, complicating the forensic recovery process. This paper explores digital forensic techniques tailored to recovering data from physically and logically damaged devices. It categorizes types of damage, evaluates existing tools and recovery methodologies, and demonstrates a low-cost recovery implementation toolkit for forensic recovery. The paper also includes diagrams and tables for deeper understanding and provides future directions for advancing this essential field of digital forensics.**

Keywords—**digital forensics, damaged digital devices, forensic techniques, data recovery, forensic toolkits.**

I. INTRODUCTION

Digital devices are ubiquitous and are often the primary sources of evidence in criminal, civil, and corporate investigations. However, suspects often destroy or damage devices to eliminate incriminating data. This research addresses the challenges posed by damaged digital devices and investigates practical forensic techniques that can be employed to recover data. This study aims to: (1) classify damage types, (2) review forensic recovery methods, (3)forensic techniques for damaged devices, (3) evaluate tools, (4) some case studies of damaged devices and (5) proposes a toolkit for forensic recovery.

II. RELATED WORK

Several prior studies have addressed challenges in recovering data from compromised digital storage. Casey [1] provides a foundation for forensic principles applicable to both functional and damaged systems. Al-Dhaqm et al. [2] categorize forensic strategies according to device damage severity. Garfinkel [3] discusses future trends including the recovery of partially damaged metadata, and Quick and Choo [10] propose data mining frameworks optimized for forensic recovery. These studies underscore the need for structured, adaptable methodologies that can respond to both physical and logical disruptions.

III. CLASSIFICATION OF DAMAGE

Table-1 Types of Damage and Corresponding Forensic Challenges

Type of Damage	**Examples**	**Forensic Challenges**
Physical	**Crushed, shattered, burned**	**Mechanical access, media integrity**

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 10, Issue 06, ISSN No. 2455-2143, Pages 15-19
Published Online October 2025 in IJEAST (http://www.ijeast.com)

Chemical	**Water, acid, corrosive exposure**	**Circuit degradation, oxidation**
Electrical	**Power surge, short circuit**	**Firmware corruption, unreadable storage**
Logical	**Deleted files, partition loss**	**File system corruption, metadata loss**
Intentional	**Encryption, disk wiping**	**Obfuscation, key management**

IV. RECOVERY TECHNIQUES

The process of recovering data from damaged devices varies by the type and extent of damage. These recovery techniques provide the necessary groundwork upon which forensic techniques are applied. Recovery techniques aim to first stabilize and access damaged media so that forensic analysis and extraction can proceed. Thus, they serve as preparatory or enabling stages for advanced forensic procedures.

A. Hard Disk Drives (HDDs)

1) Imaging Tools: Tools like FTK Imager and ddrescue clone readable sectors while skipping damaged areas [5].
2) Platter Swapping: Used when heads are misaligned or scratched. Clean room access is critical [6].
3) Printed Circuit Board (PCB) Replacement: Involves replacing the controller board with a donor from an identical model [6].

B. USB Flash Drives

1) Connector Repair: Damaged USB pins can often be resoldered using micro soldering techniques [1].
2) Disk Imaging: Sector-level cloning through Linux's dd tool preserve's structure [5].
3) File Carving: Tools such as photorec can recover deleted or lost files from raw images [10].

C. Solid State Drives (SSDs)

1) TRIM and Garbage Collection Handling: Imaging tools must be used before power cycling, as TRIM command may permanently erase deleted blocks [2]. TRIM command tells the SSD which data blocks are no longer in use [13].
2) Firmware Access: Some forensic platforms (e.g., PC-3000) interface directly with firmware to bypass controller logic [6], [13].

D. Mobile Devices

1) Logical and Physical Acquisition: Solutions like Cellebrite UFED extract app and OS data without damaging hardware [8].
2) Chip-Off & JTAG: Employed when devices are non-responsive or encrypted [2], [6], [11].

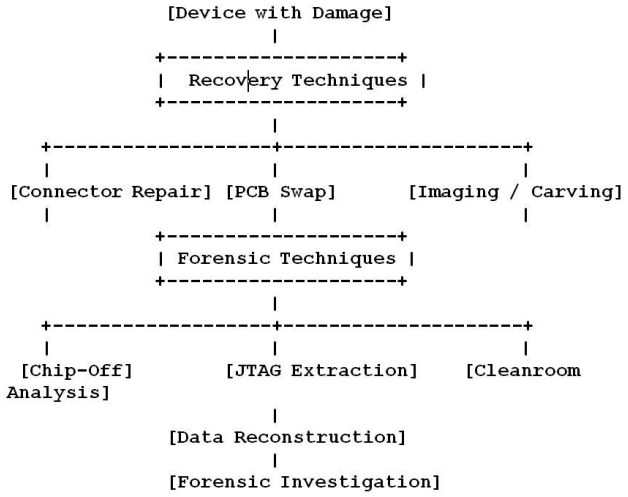

Fig. 1.Workflow Linking Recovery and Forensic Techniques

V. FORENSIC TECHNIQUES FOR DAMAGED DEVICES

Successful data recovery from damaged devices requires tailoring forensic methods to specific damage types and device architectures. Each technique has strengths, limitations, and operational environments that determine its applicability [1], [5], [6]. Following are few forensic methods for damaged devices.

A. Chip-Off technique

Chip-off forensics entails the physical removal of NAND flash memory chips from the printed circuit board. Analysts clean and heat the chip area to de-solder components without damaging internal structures [11]. Specialized NAND readers then extract raw binary dumps for analysis. This technique is particularly useful for non-functional smart-phones, USB drives, and tablets [1], [6].

B. JTAG Extraction

JTAG (Joint Test Action Group) forensics allows memory extraction via test access ports on the board. It is a non-invasive technique relying on documented pinouts and debugging protocols to dump memory content without physically removing components [2], [8], [14].

C. Use of Clean Rooms

Forensic labs utilize clean rooms to conduct recovery operations on magnetic hard drives where dust particles can cause irreversible platter damage. Common procedures include head replacement, platter extraction, and Printed Circuit Board (PCB) swaps [6].

D. Micro Read Technique

In extreme cases, where chips are physically scorched or chemically corroded, experts use scanning electron

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 10, Issue 06, ISSN No. 2455-2143, Pages 15-19
Published Online October 2025 in IJEAST (http://www.ijeast.com)

microscopes to read memory cells bit by bit. This process reconstructs the original binary data manually [3].
Together, these forensic techniques rely on recovery methods to prepare the device for deeper analysis. Recovery stabilizes and accesses the device; forensic techniques then extract, reconstruct, and interpret the data for evidentiary use.

VI. CASE STUDIES

A. Burnt Mobile Phone
A criminal suspect's phone was retrieved from a fire site. The outer casing was melted, and the internal PCB was charred [11]. Using chip-off techniques in a clean room, investigators removed the NAND flash, reconstructed partitions, and recovered timestamps and deleted SMS records, which supported the timeline of the criminal act [9].

B. Water-Damaged Laptop
A laptop belonging to a corporate whistleblower was found in a submerged vehicle. The hard drive exhibited corrosion and unreadable sectors. Forensic experts treated it with isopropyl baths and replaced the PCB using a donor drive. Disk imaging yielded over 85% of the original data, including email communications and spreadsheets vital to a fraud case [6], [10].

C. Short-Circuited IoT Device
An environmental monitoring sensor in a power plant experienced a voltage surge. Investigators identified JTAG ports and used them to extract system logs and sensor readings, enabling root cause analysis of the incident and proving tampering was not involved [2], [3], [14].

D. Bent USB Flash Drive
A physically bent flash drive containing academic data was restored by re-soldering its connector. Imaging with Linux tools followed by carving with photorec allowed full recovery of PDFs and Word documents [1], [5].

VII. PROPOSED TOOLKIT: RECOVERY STATION

A key contribution of this study is the design of a low-cost, practical recovery station that allows investigators to conduct initial recovery steps on damaged digital devices without relying on expensive proprietary lab setups. This toolkit is designed to support forensic practitioners working in the field or on a limited budget, such as law enforcement in remote areas, academic researchers, or internal investigators within corporations.

A. Components and Functionality
Table -2 Components for Budget Forensic Workbench

Component	**Functionality**
Raspberry Pi 4	**Disk imaging station**
USB to SATA Adapter	**HDD/SSD interface**
Soldering Kit	**Repair broken connectors**
Open-source tools	**dd, ddrescue, photorec, testdisk**

B. Capabilities
1) Disk Imaging: Ability to create forensic images of USBs, HDDs, and SSDs using tools like dd or dc3dd.
2) File Carving: Run photorec or scalpel for reconstructing deleted or corrupted files.
3) Live Forensics: Useful for field imaging before powering down suspect devices to preserve volatile evidence.
4) Supports modular upgrades such as General Purpose Input/Output (GPIO)-based automation or thermal sensors.

C. Benefits
1) Extremely low cost.
2) Highly portable for on-site digital forensic operations.
3) Compatible with open-source Linux distributions.
4) Used in conjunction with soldering tools to bring damaged connectors back online.

D. Limitations
1) Cannot replace clean room recovery for heavily damaged drives cost.
2) Limited processing power for large-scale recovery tasks.
3) Requires trained personnel to use soldering tools and Command Line Interface (CLI) utilities.

VIII. TOOLSETS AND SOFTWARE

A wide variety of forensic software and hardware toolsets are essential for conducting successful investigations on damaged digital devices. These tools support different phases of the forensic process, including device stabilization, data recovery, file carving, imaging, and post-recovery analysis. The selection of appropriate tools depends on the type of device, the extent and nature of the damage, and the forensic objective.

A. Imaging and Recovery Tools
1) FTK Imager: A widely used tool for creating forensic images and previewing data without altering the source drive. It supports various file systems and allows logical and physical image acquisition [5], [8].
2) dd / ddrescue / dc3dd: Command-line utilities for sector-by-sector imaging. ddrescue is especially useful for handling bad sectors or unstable media, while dc3dd extends dd with forensic features [5], [10].

3) TestDisk and PhotoRec: Open-source tools for partition repair and file carving. TestDisk reconstructs lost partitions, whereas PhotoRec recovers lost files from formatted or damaged storage devices [5], [10].

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 10, Issue 06, ISSN No. 2455-2143, Pages 15-19
Published Online October 2025 in IJEAST (http://www.ijeast.com)

B. Mobile Forensics Tools

1) Cellebrite UFED: Industry-leading solution for mobile phone forensic extraction. It supports logical, physical, and file system extractions and includes tools for bypassing screen locks and encrypted app data [1], [8].

2) XRY: An alternative to UFED, supporting a wide range of mobile devices with capabilities for live acquisition, deleted data recovery, and secure reporting [4], [15].

C. Storage Device Analysis Tools

1) PC-3000: A professional-grade suite for analyzing and repairing hard drives and SSDs at the firmware level. Useful for cases involving PCB failure, firmware corruption, or advanced recovery from mechanically damaged drives [6], [7].

2) X-Ways Forensics: An advanced data analysis platform known for its efficiency and detailed forensic reporting. It supports complex file systems and forensic image formats, and is often used in conjunction with imaging tools [7].

D. Chip-Level and Embedded Systems Tools

1) JTAG Debuggers: Tools used to connect to microcontrollers and extract raw data from memory through standard debugging interfaces. Requires device-specific pinout mapping and supported protocols [2], [9], [14].

2) NAND Flash Readers: Specialized programmers and sockets used in chip-off forensics to read binary dumps from physically removed flash memory chips. Common tools include the RT809H and UP828P [2], [6],[11].

E. Open-Source Platforms and Operating Systems

1) CAINE (Computer Aided Investigative Environment): A Linux-based forensic distribution bundled with dozens of forensic tools, including Autopsy, Bulk Extractor, and Sleuth Kit [10].

2) Kali Linux: Another powerful distribution used for both penetration testing and digital forensics. It includes utilities for imaging, carving, reverse engineering, and live response [10].

These tools, when integrated effectively, form the backbone of a forensic analyst's toolkit and significantly influence the success of digital investigations involving damaged devices. A proper understanding of their capabilities and constraints allows practitioners to adapt quickly to evolving forensic challenges.

Table -3 Forensic Tools for Damaged Devices

Tool	Function	Use Case
XRY	**Alternative mobile forensics suite, deleted data recovery**	**Damaged smartphones**
FTK Imager	**Imaging and data carving**	**Partially readable HDDs**
X-Ways Forensics	**Analysis and recovery**	**Complex file system recovery**
PC-3000	**HDD and other storage device repair and imaging**	**Mechanically damaged drives**
JTAG Debuggers	**Chip-Level and Embedded Tool**	**Non-invasive memory extraction through debug ports**
NAND Flash Readers	**allows users to read data from NAND flash memory chips**	**Direct binary read from de-soldered flash chips**

IX. LEGAL AND ETHICAL CONSIDERATIONS

Data recovery from damaged devices may involve bypassing encryption or security features, raising legal issues. Strict adherence to forensic protocols, documentation, and chain of custody is vital to ensure admissibility in court [3], [7], [12].

X. FUTURE DIRECTIONS

Future efforts may focus on AI-driven recovery, deeper integration of chip-level interfaces, and universal forensic platforms for handling damaged digital media. Nano-scale and firmware-layer techniques are also promising research areas [10].

XI. CONCLUSION

Digital forensic techniques for damaged devices form a vital aspect of modern cyber investigations, particularly where adversaries attempt to destroy digital traces. This paper has presented an in-depth exploration of forensic approaches—from high-cost clean room interventions to affordable open-source recovery methods. Through the analysis of real-world case studies and technical procedures, it is evident that the combination of hardware repair skills and software analysis tools enables significant recovery even from severely damaged media. As data volumes and device complexity continue to grow, developing adaptable, efficient, and legally compliant recovery methods will remain a priority in the digital forensic field [1], [2], [3].

XII. ACKNOWLEDGMENT

We are thankful to The Director General (Legal and Technical), Home Department, Govt. of Maharashtra for his guidance, encouragement and constant support.

XIII. REFERENCES

[1]. Casey Eoghan, (2011). Digital Evidence and Computer Crime, Academic Press.

[2]. Al-Dhaqm Ahmed, et al., (2022). Digital forensic techniques for damaged devices: A structured analysis, Forensic Science International.

[3]. Garfinkel Simson L., (2013). Digital forensics research: The next 10 years, Digital Investigation, Vol. 7, (Pg S64–S73).
[4]. National Institute of Standards and Technology (NIST), (2006). Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86.
[5]. Carrier Brian, (2005). File System Forensic Analysis, Addison-Wesley.
[6]. Sammes Tony and Jenkinson, Brian, (2007). Forensic Computing: A Practitioner's Guide, Springer.
[7]. Rogers Marcus, (2006). A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study, Digital Investigation.
[8]. Nelson Bill; Phillips Amelia; and Steuart Christopher, (2018). Guide to Computer Forensics and Investigations, Cengage Learning.
[9]. Choo Kim-Kwang Raymond, (2011). Cloud computing: challenges and future directions, Trends & Issues in Crime and Criminal Justice.
[10]. Quick Darren and Choo Kim-Kwang Raymond, (2013). Data reduction and data mining framework for digital forensic evidence, Journal of Network and Computer Applications, Vol. 36, (Pg.1–9).
[11]. Kessler Gary C., (2013). The Use of Chip-Off Techniques in Mobile Device Forensics, Journal of Digital Forensics, Security and Law, Vol. 8, No. 3, (Pg 25–34).
[12]. Nardone Raymond E. and Forcht Karen A., (2011). Legal Considerations of Digital Forensic Evidence in Court, Journal of Information Privacy and Security, Vol. 7, No. 4, (Pg 3–14).
[13]. Zubair Ahmad; Malik Adeel; and Khan Rizwan, (2021). Forensic Data Recovery from Solid-State Drives: Challenges and Solutions, Forensic Science International: Digital Investigation, Vol. 36. https://doi.org/10.1016/j.fsidi.2021.301114
[14]. Sun Bo; Yu Jian; and Wang Xiaohong, (2018). Advanced Techniques in JTAG and Boundary Scan for Digital Forensics, in Proc. IEEE CyberC: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, (Pg 1–7).
[15]. Dardick Amanda G., (2015). Recovering Evidence from Damaged Mobile Devices: Comparative Analysis of Forensic Tools, Digital Investigation, Vol. 14, (Pg S91–S99).