IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 5, 2022, accepted January 27, 2022, date of publication March 11, 2022, date of current version April 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3158958

New Diagnostic Forensic Protocol for Damaged Secure Digital Memory Cards

F. THOMAS-BRANS[1,2], T. HECKMANN[1,3], K. MARKANTONAKIS[4], AND D. SAUVERON[2]

[1]Centre de Recherche de la Gendarmerie Nationale (CREOGN), 77000 Melun, France
[2]Laboratoire Xlim UMR CNRS 7252, Université de Limoges, 87000 Limoges, France
[3]Ecole Normale Supérieure de Paris (ENS-Paris), 75005 Paris, France
[4]Information Security Group, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, U.K.

Corresponding author: F. Thomas-Brans (fabien.thomas-brans@gendarmerie.interieur.gouv.fr)

This work was supported by the National Research Agency under the Investments for the Future Program through Sigma-LIM under Grant ANR-10-LABX-0074-01.

ABSTRACT Over the past twenty years, Secure Digital memory cards have become the most popular digital storage media. Therefore, forensic experts need to develop forensic techniques to enable recovery of data, especially from cards severely damaged by accidents, air crashes, terrorist attacks or deliberate attempts by criminals to destroy evidence. The paper discusses the non-invasive and invasive diagnostics available to forensic experts, with descriptions of the necessary equipment, including binocular microscopes, X-Ray equipment, scanning acoustic microscopes, chemical benches, and, for the first time, infrared cameras. All of these techniques can be used to methodically determine the best treatment in order to repair damaged storage media and extract data from them. The main contributions of the paper include the development of an innovative systematic forensic protocol for diagnostics on damaged cards, which involves a decision-making diagram. Finally, a concrete case study is presented using the new forensic decision diagram-based protocol and the panel of techniques available to diagnose a card damage.

INDEX TERMS Decision making, digital storage, fault diagnosis, flash memories, forensics, infrared imaging, law enforcement, microscopy, tomography, X-rays.

I. INTRODUCTION

With the evolution of technology and lifestyles, many people now have one or more Internet of Things (IoT) devices [1]. These devices have become almost essential, which continues to support the drive for miniaturization. The widespread use of these electronic devices has resulted in an increased need for storage capacity. As a result, system manufacturers have gradually started to replace internal storage units [2] of considerable dimensional size, such as Hard Disc Drives (HDDs), with smaller ones that are faster and more efficient for data exchange, such as Solid-State Drives (SSDs).

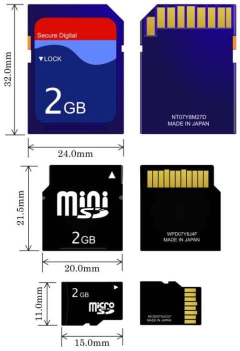


FIGURE 1. Standard form and size of SD cards (from top to bottom: SD, mini-SD and micro-SD cards).

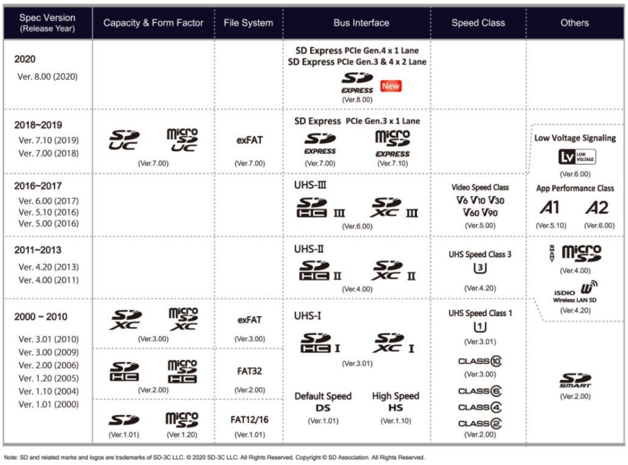
Due to users' needs for increasing storage capacity and because of the importance of cost for manufacturers to increase internal storage, the choice was quickly made to adopt a removable storage system, and Secure Digital (SD) cards fully meet this need [3]. Therefore, system manufacturers have integrated slots for Secure Digital (SD), mini-SD or micro-SD cards (Figure 1) to better adapt to the needs of users and to increase the storage capacity of the entire spectrum of electronic devices.

A user can adapt the storage capacity of a device at low cost, depending on their storage or reading/writing speed

The associate editor coordinating the review of this manuscript and approving it for publication was Gerard-Andre Capolino.

requirements. It is now possible to buy a micro-SD card with a capacity of 400 GB, using Secure Digital eXtended Capacity (SDXC) technology, for less than 100€ .

A user who does not need much storage may be satisfied with the internal storage offered by the manufacturer, while a user making a video in 4k high resolution will need a large storage capacity and a fast writing speed to avoid the phenomenon of latency [4]. SD card manufacturers have been able to adapt to such needs over the past twenty years (Figure 2), by offering more efficient media that are faster and have more storage capacity.



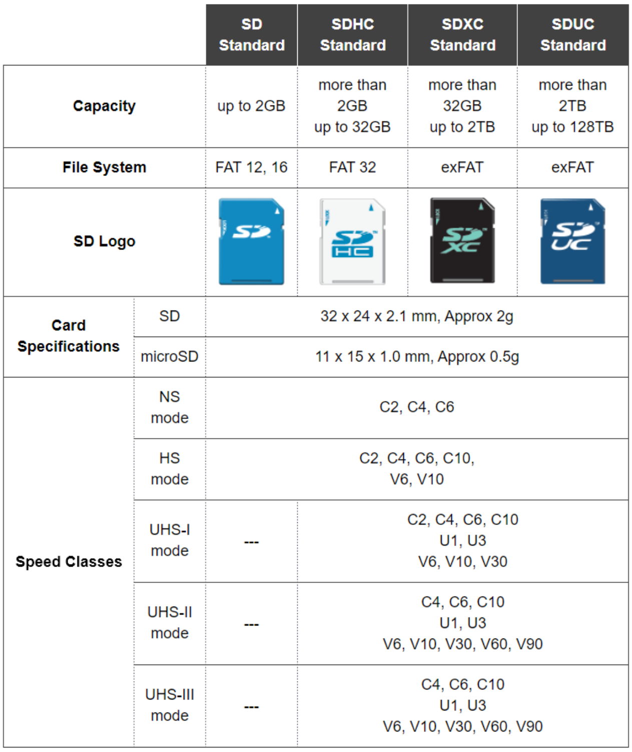
Spec Version (Release Year)	Capacity & Form Factor	File System	Bus Interface	Speed Class	Others
2020 Ver. 8.00 (2020)			SD Express PCIe Gen.4 x 1 Lane SD Express PCIe Gen.3 & 4 x 2 Lane SD EXPRESS New (Ver.8.00)		
2018~2019 Ver. 7.10 (2019) Ver. 7.00 (2018)	SD UC microSD UC (Ver.7.00)	exFAT (Ver.7.00)	SD Express PCIe Gen.3 x 1 Lane SD EXPRESS (Ver.7.00) microSD EXPRESS (Ver.7.10)		Low Voltage Signaling LV LOW VOLTAGE (Ver.6.00)
2016~2017 Ver. 6.00 (2017) Ver. 5.10 (2016) Ver. 5.00 (2016)			UHS-III SD HC III SD XC III (Ver.6.00)	Video Speed Class V6 V10 V30 V60 V90 (Ver.5.00)	App Performance Class A1 (Ver.5.10) A2 (Ver.6.00)
2011~2013 Ver. 4.20 (2013) Ver. 4.00 (2011)			UHS-II SD HC II SD XC II (Ver.4.00)	UHS Speed Class 3 U3 (Ver.4.20)	SMART microSD (Ver.4.00) iSDIO Wireless LAN SD (Ver.4.20)
2000 ~ 2010 Ver. 3.01 (2010) Ver. 3.00 (2009) Ver. 2.00 (2006) Ver. 1.20 (2005) Ver. 1.10 (2004) Ver. 1.01 (2000)	SD XC microSD XC (Ver.3.00)	exFAT (Ver.3.00)	UHS-I SD HC I SD XC I (Ver.3.01)	UHS Speed Class 1 U1 (Ver.3.01) CLASS 10 (Ver.3.00)	SD SMART (Ver.2.00)
	SD HC microSD HC (Ver.2.00)	FAT32 (Ver.2.00)			
	SD (Ver.1.01) microSD (Ver.1.20)	FAT12/16 (Ver.1.01)	Default Speed DS (Ver.1.01) High Speed HS (Ver.1.10)	CLASS 6 CLASS 4 CLASS 2 (Ver.2.00)	

Note: SD and related marks and logos are trademarks of SD-3C LLC. © 2020 SD-3C LLC. All Rights Reserved. Copyright © SD Association. All Rights Reserved.

FIGURE 2. **Evolution of SD card specifications in terms of capacity type, form factor, bus interface and speed class between 2000 and 2020 [5].**

Currently, there are four main types of SD card memory systems: Secure Digital Standard Capacity (SDSC, often referred as SD), Secure Digital High Capacity (SDHC), Secure Digital eXtended Capacity (SDXC) and Secure Digital Ultra Capacity (SDUC). These four types are ranked according to their capacity and recommended file system format (Figure 3). The standard chosen by users will offer a range of storage capacity suiting their requirements. By cross-referencing information from two sources, the evolution of capacity can be described as follows. In early 2000, an SD standard card had a capacity of less than 2 GB, to be supplanted in 2006 by the SDHC card with a capacity of up to 32 GB. This was exceeded by the SDXC standard, with a storage capacity increasing from 32 GB to 2 TB over the years between 2009 and 2017, while in 2018 the new standard SDUC was released, with a capacity ranging from 2 TB to 128 TB.

Forensic experts also had to adapt to this technological evolution [6]. The SD card became the object of tests [7] included in almost all judicial evidence [8] (including devices such as smartphones, cameras, automation tools, action-cams, game consoles, laptops, and connected vehicles). As these storage devices have become more and more efficient, they enable data to be secured through various options such as locking or encrypting [9]. Some manufacturers even use SD cards as key stores to encrypt the data for very high security smartphones, called darkphones, like No.1BC [10].



		SD Standard	SDHC Standard	SDXC Standard	SDUC Standard
Capacity		up to 2GB	more than 2GB up to 32GB	more than 32GB up to 2TB	more than 2TB up to 128TB
File System		FAT 12, 16	FAT 32	exFAT	exFAT
SD Logo		SD	SD HC	SD XC	SD UC
Card Specifications	SD	32 x 24 x 2.1 mm, Approx 2g			
	microSD	11 x 15 x 1.0 mm, Approx 0.5g			
Speed Classes	NS mode	C2, C4, C6			
	HS mode	C2, C4, C6, C10, V6, V10			
	UHS-I mode	---	C2, C4, C6, C10 U1, U3 V6, V10, V30		
	UHS-II mode	---	C4, C6, C10 U1, U3 V6, V10, V30, V60, V90		
	UHS-III mode	---	C4, C6, C10 U1, U3 V6, V10, V30, V60, V90		

FIGURE 3. **Evolution of storage capacity, file system and speed classes depending on the capacity type [5].**

Although cards have the advantage of being removable and easily transportable, they also have the disadvantage of being fragile (easily damaged by impact and accident) and easily concealable for illegal use (such as child pornography, terrorism, or drug trafficking). Frequently, individuals engaged in illicit activities try to destroy as much evidence as possible at the time of arrest by physically destroying their SD cards. For this reason, diagnostic processes for recovering information from SD cards are becoming standard practice for many forensic laboratories.

While there are several papers dealing with different stages of data recovery from SD cards, to the best of our knowledge there is no public diagnostic forensic protocol for damaged cards. The closest work is the decision diagram for damaged and undamaged mobile devices (i.e. smartphones) [11]. In [12], [13], the authors discuss how to adapt acquisition and analysis techniques to recover accurate and relevant data from flash memory chips; however, this is under the implicit assumption that they are not damaged. In [14], the authors explain that due to their block-based structure, flash memories are becoming forensics targets but they mainly propose an anti-forensic technique. Although present in most IoT devices, SD cards are rarely considered in recent surveys dealing with IoT forensics [15]–[17], further increasing the potential value of our contribution of a systematic diagnostic forensic protocol for damaged SD cards.

A. CONTRIBUTION

The main contribution of this paper is the proposal of a new forensic protocol for damaged SD cards, which aims at minimizing the risk of additional damage during the diagnostic process. This proposal relies on a decision-making diagram encompassing the main non-invasive and invasive techniques that forensic experts can use to identify issues while preserving the integrity of the evidence on the damaged card, and then make repairs to enable data extraction. Note that the data extraction step is not covered in this paper.

Our additional contributions are as follows:

- Surveying the available non-invasive and invasive techniques applicable to SD cards.
- Introducing a new diagnostic technique using an infrared camera to locate and characterize the damage on an SD card.
- Detailing the application of the proposed forensic protocol in a real case study.

B. STRUCTURE

Section II introduces the SD card from both hardware and software perspectives. Section III introduces the proposed forensic protocol for SD cards, which uses the developed decision-making diagram and presented diagnostic techniques to determine how to repair damage and conduct data extraction even in the most complex cases. Section IV illustrates the application of the proposed forensic protocol to a real case study and shows the extent to which the diagnostic technique using an infrared camera can minimize the risk of additional damage in forensic conditions. Section V discusses of subsequent data recovery steps not covered in this paper. Section VI concludes the paper.

II. FUNCTIONAL OVERVIEW OF AN SD CARD

The evolution of storage capacity requirements has resulted in a parallel evolution of storage technologies. The use of raw Not-AND (NAND) flash memory chips has been abandoned in favour of more complex memories. These systems, available in different form-factors, such as the Embedded Multi-Media Card (eMMC), Embedded Multi-Chip Package (eMCP) or SD card, consist of several stacked memory chips addressed by a microcontroller, which provides the host with an abstraction layer to manage the storage space via a standard communication interface.

A. HARDWARE DESIGN

The design of an SD card is similar to other managed data storage components. Indeed, as illustrated in Figure 4 and shown for a specific card in Figure 5, the micro-SD card, SD card and eMMC are composed of one or more flash memory dice [18] and a microcontroller [19] that acts as an interface between the memory and the card reader.

The memory dice and the microcontroller are standard and are produced by many manufacturers, including Samsung, Intel, Toshiba, Phison, Silicon Motion and SanDisk. Apart from the size of the card and the external interface, there are no rules for internal design (either in terms of location of components, or of their number); thus, it is one of the functions of the microcontroller to provide the abstraction for the storage space. For instance, a card with a 64 GB capacity can be composed of one, two, four or even eight memory dice.

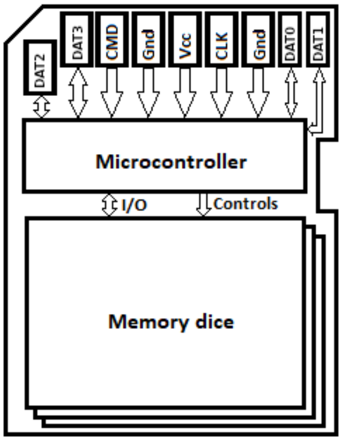


FIGURE 4. Internal composition of an SD card including communication signals and buses.

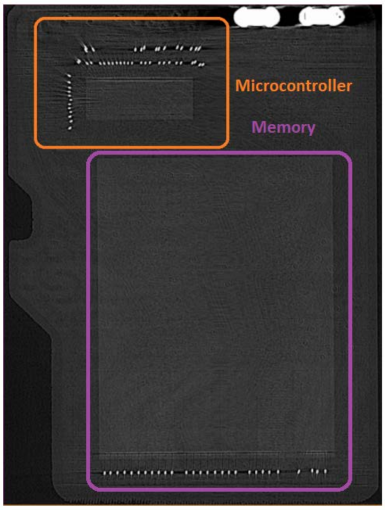
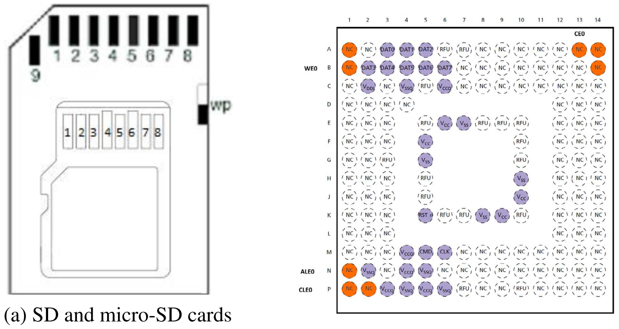


FIGURE 5. X-Ray view of a micro-SD card on which the microcontroller and the memory dice are highlighted.

As illustrated in Figure 4, the microcontroller has two communication buses: (a) one external bus with the card reader (i.e. with the host) which is standard[1] and defined by the SD Card Association [20] for interoperability purposes; and (b) one internal bus with the memory dice, for which there are several standards for communication signals (ONFI [21],

[1] However, there are different backward compatible pinout topologies offering different bus speed modes for data transfer, such as the Normal Speed, High Speed, and Ultra High Speed modes presented in Figure 3. It is important not to confuse the bus speed (UHS-I for instance, with a maximum speed of 104MB/s), which represents the maximum data transfer speed, with the card class (C10, for instance, standing for 10MB/s), which refers to the minimal speed at which data is sequentially written in memory.



(a) SD and micro-SD cards

(b) eMMC memory [24]

FIGURE 6. Pinout of different form factor samples.

JEDEC [22], Toggle NAND interface [23]) and no standards for pinout topologies (as illustrated in Figures 17 and 18, pinouts of memory dice with the microcontroller are card-model specific). The external pinouts of these managed systems also have similarities in signals, as shown in Figure 6b for SD and micro-SD cards and in Figure 6a for eMMC. The similarities and differences between pinouts for the different signals are illustrated in Table 1.

TABLE 1. Comparison of signals between SD card, micro-SD card, and eMMC memory.

Signal Function	Signal Name	SD Card Pinout	Micro-SD Card Pinout	eMMC Pinout
Power	Vcc	4	4	9 pins
	Gnd	3, 6	6	9 pins
Control	CMD	2	3	M5
	CLK	5	5	M6
	RST	✗	✗	K5
I/O	DAT0	7	7	A3
	DAT1	8	8	A4
	DAT2	9	1	A5
	DAT3	1	2	B2
	DAT4	✗	✗	B3
	DAT5	✗	✗	B4
	DAT6	✗	✗	B5
	DAT7	✗	✗	B6

✗: Do not exist

Though as illustrated in Figures 17 and 18, pinout patterns (sometimes called debug pads) are card-model specific, it is worth noting that accessing the internal bus can allow direct reading of the memory dice in order to perform complex data reconstruction tasks if, for instance, the microcontroller is malfunctioning.

While the function of a memory die is data storage, the roles of the microcontroller are multiple. The microcontroller performs arithmetic operations, manages data flow, and generates control signals in accordance with a sequence of instructions. Microcontrollers are dedicated to run one specific program. The program is usually stored in the microscontroller's own Read-Only Memory (ROM). All the functions of the SD-card microcontroller are shown schematically in Figure 4.

B. DATA ORGANISATION

As the microcontroller acts as an interface between raw NAND flash memory dice and the host to offer managed data storage, it is in charge of data organisation. It distributes data in the memory plan of the different dice to optimise reading/writing. It also excludes memory areas corrupted during writing or defective as a result of the manufacturing process. In addition, it allows correction of read errors and memory corruption using Error-Correcting Code (ECC).

The microcontroller manages the memory using a system of blocks and pages. The block is the smallest erasable unit. Each block is itself divided into pages, which are the smallest unit of writing and reading.

As illustrated in Figure 7, pages themselves are structured in one or more chunks, which contain usually two areas: the data area where user data are stored, and the spare area containing information about the page (like the page number) and ECCs related to user data. However, this structure varies according to the manufacturer of the microcontroller and the SD card model.

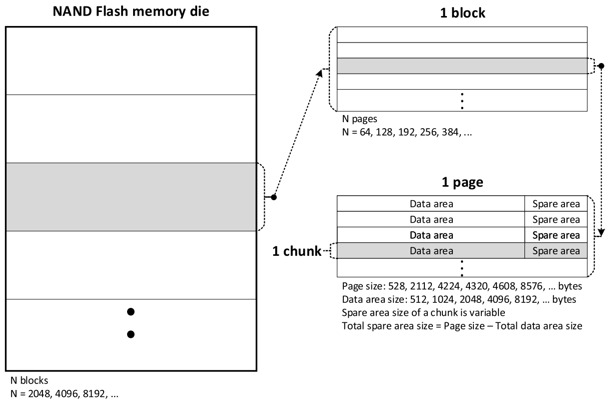

NAND Flash memory die
1 block
N pages
N = 64, 128, 192, 256, 384, ...
1 page
Data area
Spare area
Data area
Spare area
Data area
Spare area
Data area
Spare area
1 chunk
Page size: 528, 2112, 4224, 4320, 4608, 8576, ... bytes
Data area size: 512, 1024, 2048, 4096, 8192, ... bytes
Spare area size of a chunk is variable
Total spare area size = Page size – Total data area size
N blocks
N = 2048, 4096, 8192, ...

FIGURE 7. Elementary organisation of a NAND Flash memory with block and page structures.

ECCs are important for maintaining data integrity in SD memories. There are multiple sources of bit errors in NAND flash memories (including cell-to-cell interference, charge leakage, read disturbances, and bad transistor programming at writing). This control data allows the management of errors and their correction. These tasks of identification, control, and correction of errors are performed by the microcontroller. Each time a page is accessed, the microcontroller carries out ECC computations. When reading, in order to validate the read data and correct it if necessary,[2] the microcontroller uses the ECC value read, knowing that the read errors can be in the data read or in the ECC value read or in both.[3] Before

[2] Correction is done only if possible because depending on the size of the code used in the ECC and the type of code (Hamming, Bose-Chaudhuri-Hocquenghem, etc.) only a certain number of erroneous bits can be corrected.

[3] If the ECC correction process does not recover the data integrity, the microcontroller can potentially reread the page with other parameters (clock, etc.) in order to try to obtain the original data. The aim is that the memory medium appears error-free.

writing data to be stored, the microcontroller calculates the ECC value to write in the spare data.

To prolong the memory lifetime of an SD card, the microcontroller implements a wear leveling algorithm since NAND flash memory cells usually support around 5000 programming cycles. However, on modern devices using these memories, such as phones and GPS units, data changes are constant. As illustrated in Figure 8, the aim of the wear leveling mechanism is to erase as little as possible in each block, writing the new data in priority over the empty blocks that are least used. It is based on the number of erases in each block, using an incremented counter mechanism.

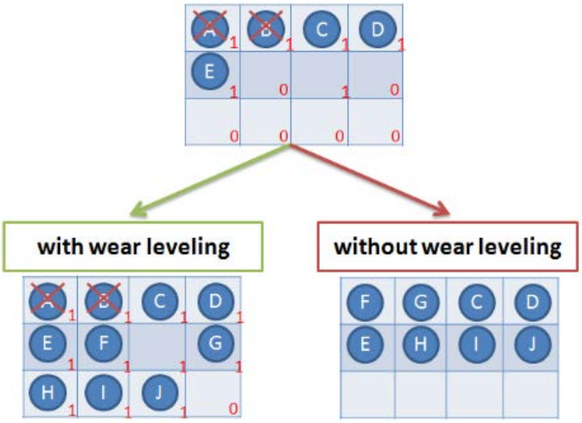


FIGURE 8. Example of new data writing with and without wear leveling in NAND flash memory [11].

In the example presented in Figure 8, five blocks are filled with data. Blocks A and B, which will be deleted, are marked as invalid by the system. The blocks are not systematically released in order to preserve the life of the flash memories. Without wear leveling, the new pages (F and G) are written in the first available blocks, in place of the old pages (A and B). But with wear leveling, the first two blocks are marked as having been used once already. Therefore, the new pages are written in the first blocks that have the lowest usage count. In the presence of wear leveling, when a block needs to be modified, the microcontroller copies it with the data modified elsewhere in the memory and connects this new physical address to the logical address; the previous block is marked as invalid. Using the standard external interface of the SD card the data storage is consistent and only the current state of a logical block is accessible. However, using the internal bus, it is possible to access each physical block and thus to access content of interest to forensic experts, such as the previous contents of a logical block (those whose physical blocks have not yet been released).

In addition to wear leveling in SD memory technology, the microcontroller can also implement a garbage collector mechanism [25], which is responsible for managing the free space. Its role is to determine which spaces can no longer be used and to then recover them. If blocks contain pages marked as invalid (i.e. no longer used), the algorithm moves the valid pages to another block, and then frees the initial blocks.

C. EXCHANGE PROTOCOLS AND BASIC OPERATIONS

Like other types of flash memory card, an SD card from any SD family is a block-addressable storage device, in which the host device can read or write fixed-size blocks by specifying their block number.

As illustrated in Table 1, the interface between the host and the SD card uses its own power, control and I/O signals. At power-up from the host (the so-called hardware reset), the microcontroller is in an idle state and waits to receive commands from among the 64 defined in [20]. The first is the `CMD0` command to define the bus mode: SD or SPI mode. At this stage, the bus is 1 bit in width and so only DAT0 is used for data transfers. However, the host can configure the device to use a wider data bus, DAT0-DAT3 or DAT0-DAT7, for data transfer in SD mode.

Commands sent by the host to the microcontroller can be `read` or `write` commands for single or multiple blocks as illustrated in Figures 9 and 10.

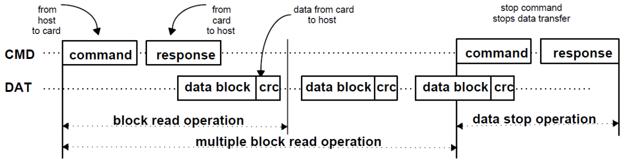


FIGURE 9. Protocol between the host and the microcontroller for read operation in SD mode [20].

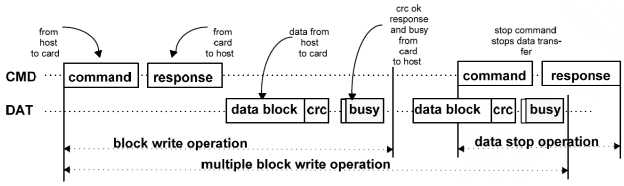


FIGURE 10. Protocol between the host and the microcontroller for write operation in SD mode [20].

Thus, when the microcontroller receives a command to read one or more blocks, it will use the appropriate protocol on the bus connecting it to the memory dice (mostly ONFI [21] – even if other standards exist, such as JEDEC [22], Toogle mode [23]), to read the data from the requested block(s) before sending them to the host after ECC corrections. Similarly, when receiving a write command and the data to be stored, the microcontroller will use the same bus and the appropriate protocol to write data to the memory dice after the calculation of the ECC correction data.

III. PROPOSED FORENSIC PROTOCOL USING DIAGNOSTIC TECHNIQUES

The SD card initial diagnostic is basically not different from a classic failure analysis [26], the main goal being to find the defect without accentuating it. The first step, when the sample is received, is to proceed with non-invasive handling before making tests electrically. Based on an analysis of several samples with different and unknown damage levels, the following global decision diagram is proposed (Figure 11).

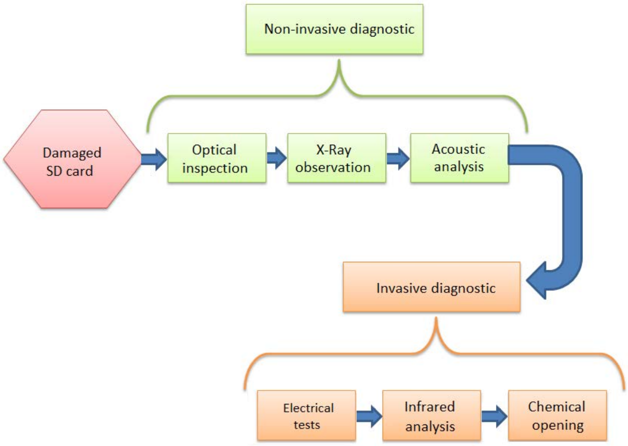


FIGURE 11. Overview of the proposed forensic decision diagram for damaged SD cards.

The proposed decision diagram can be developed in two sub-parts. The non-invasive part (Figure 12) is composed of steps that should not modify data contained in memories if the forensic expert proceeds appropriately. In contrast, the invasive part (Figure 13) can accentuate defects and lead to data loss. For this reason it is located in the second part of the decision diagram. This part of the diagram is only applied if the non-invasive part has been inconclusive. For each of the steps, the transition options are presented as well as the possible repairs, which are discussed later.

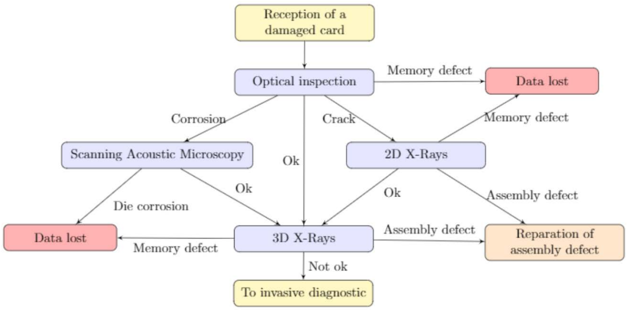


FIGURE 12. The steps in the non-invasive part of the decision diagram.

A. NON-INVASIVE DIAGNOSTICS

The main goal of the non-invasive analysis is to locate possible defects in the SD card package without accentuating them or causing further damage. Several techniques are used in the proposed forensic protocol:

- optical inspection;
- 2D and 3D X-Ray observations;
- scanning acoustic microscopy analysis.

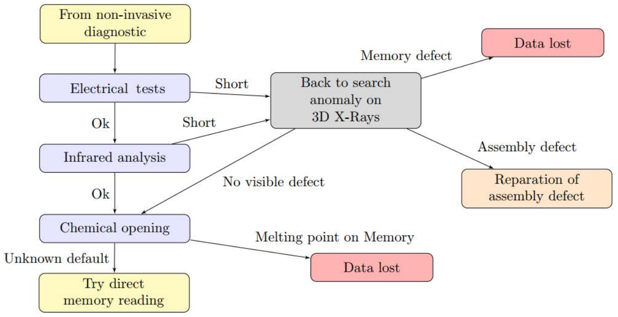
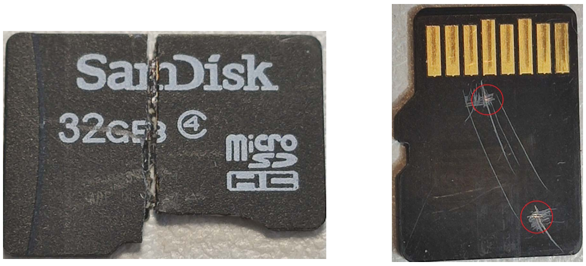


FIGURE 13. The steps in the invasive part of the decision diagram.

Each of these processes is detailed below.

1) OPTICAL INSPECTION

Using a binocular microscope, a forensic expert looks for cracks in the package (Figure 14a). Any abnormal curvature of the card is also searched since this can create important mechanical stresses on the chips. Inspection of the printed circuit boards (PCBs) is also performed in order to find cutting tracks, which could block internal communication between the microcontroller and the memory dice (Figure 14b). If defects are located, it is possible to characterize them to determine whether they are just superficial or whether they affect the integrity of the card.



(a) Crack on the package showing the silicon dice

(b) Scratch on the track side of the card

FIGURE 14. Optical view of micro-SD cards with different types of visible damage.

Another aspect looked for in optical inspection is the presence of corrosion. When such media have been in prolonged contact with water, the exposed metal elements are attacked. The areas of the SD card under the varnish or with a gold coating are protected. Thus, one objective of optical inspection is to find whether humidity is present and to investigate how it has entered the package. If the presence of humidity is suspected, the use of a Scanning Acoustic Microscope (SAM) can determine the propagation of corrosion in order to estimate the damage.

2) 2D AND 3D X-RAY OBSERVATIONS

Complementary to the optical inspection, X-Ray inspection allows further internal diagnosis. The realization of a 2D view from the top of the sample, then from the side, allows investigators to search for structural anomalies such as damaged or missing bondings at the chip level. However, this type of observation does not always make it possible to correctly differentiate the elements and their layers. It is thus preferable to carry out a 3D acquisition and reconstruction [27] to allow forensic experts to identify the levels between the PCB and the bondings, and thus to better locate possible defects [28]. Figures 15 and 16 show a break in the silicon through the active copper layer of the memory dice. This defect was not visible during the optical inspection step. However, with the X-Ray analysis, the forensic expert has additional information for repairing the sample.

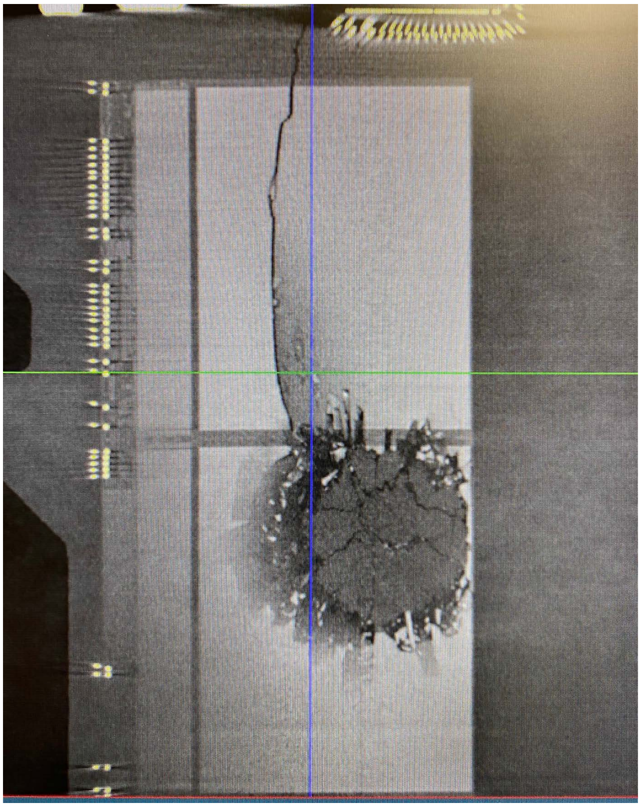


FIGURE 15. 2D X-Ray view: crack in the memory die.

A 3D image acquisition allows observation of the different slices of the sample on each axis. From the images obtained in 3D X-Rays, a forensic expert can reverse engineer the different signals by using the GIMP drawing tool to colorize the copper tracks: (a) those between the microcontroller and the external pins of the SD card (i.e. those that are in contact with the host's reader); and (b) those between the microcontroller and the memory dice (Figures 17 and 18).

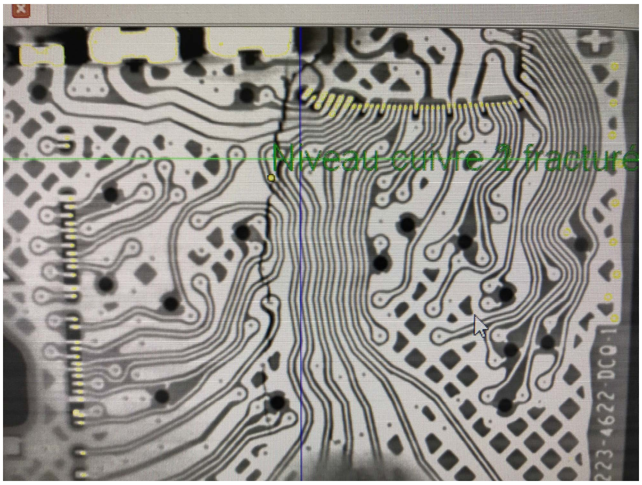
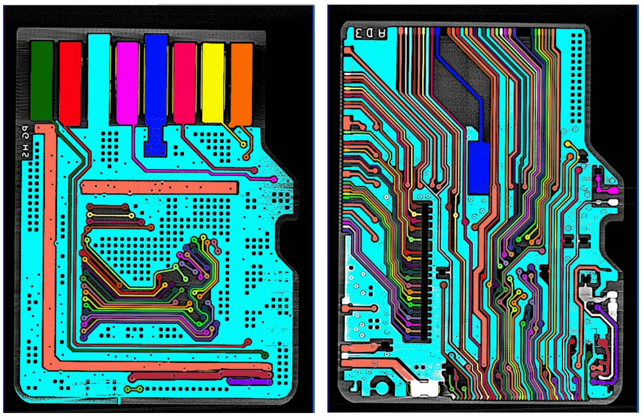


FIGURE 16. Layer of 3D X-Ray view: damage propagation on PCB and memory dice.



(a) Slice of SD pinout side

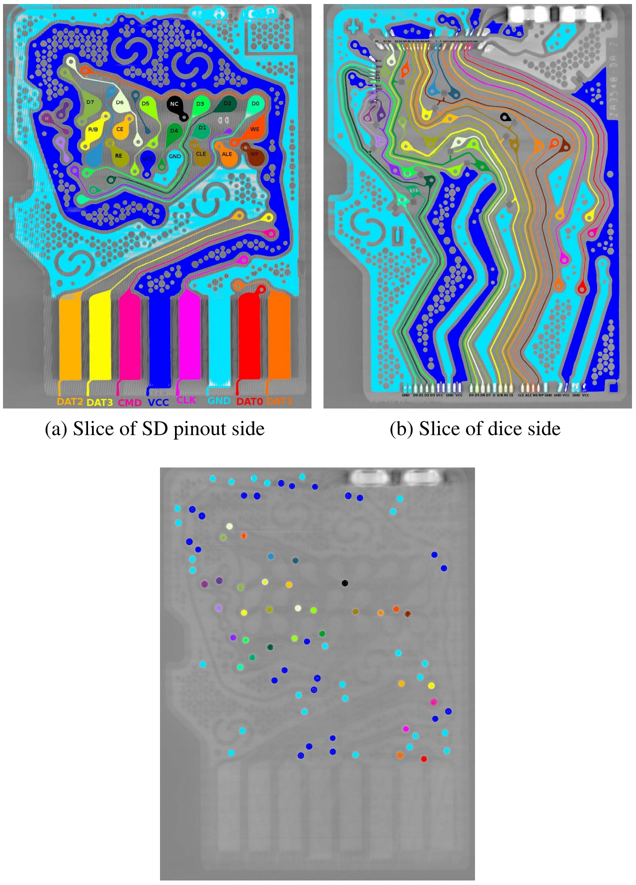
(b) Slice of dice side

FIGURE 17. 3D X-Ray slices from an SD card with identification of the tracks after a reverse engineering study.

The next step of the analysis is to assign a function for each color. With the aim of identifying signals, forensic experts can compare identified tracks with existing databases. For example, the "PC-3000 Flash" database [29] (from ACE Lab [30]) can help to make the identification and reverse engineering operations much faster by comparing the internal bus pinout topology with the existing database. This technique and the analysis of each layer make it possible to know which circuits correspond to the ground, through which the data are transferred, and which are the circuits through which the microcontroller receives commands and sends actions to be performed. However, identified tracks need to be physically verified by checking each output signal since similar internal bus pinout topologies may be used on different SD cards to route different signals.

In the example presented in Figure 18, a comparison of the copper level of an unknown card with the "PC-3000 Flash" database (Figure 19) allows the forensic expert to very quickly obtain a description of the pinout topology for the internal bus between the microcontroller and the memory dice (Figure 20).

When the pinout topology does not exist in the database, forensic experts can use a similar card (i.e. with identical internal components: sometimes, cards of the same model and brand can be externally identical but internally different).



(a) Slice of SD pinout side

(b) Slice of dice side

(c) Slice of vias

FIGURE 18. 3D X-Ray slices from another SD card after a reverse engineering study and identification of signal.

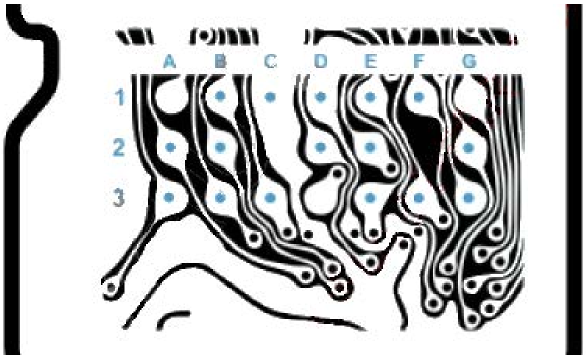
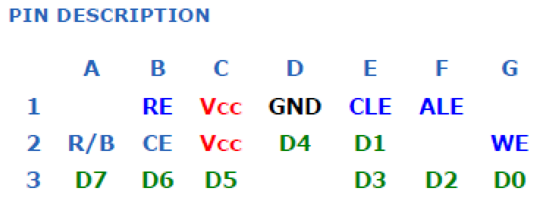


FIGURE 19. SD card pin identification from the "PC-3000 Flash" database [29].

A logic analyzer is connected to both the external and the internal buses in order to identify the signals on each track.

Having found a description of the pins connecting the microcontroller,[4] it is also possible to schematize it as illustrated in Figure 21 to assist in the diagnostic process.


PIN DESCRIPTION

	A	B	C	D	E	F	G
1		RE	Vcc	GND	CLE	ALE	
2	R/B	CE	Vcc	D4	D1		WE
3	D7	D6	D5		D3	D2	D0

FIGURE 20. Signal description for the pins identified in Figure 19.

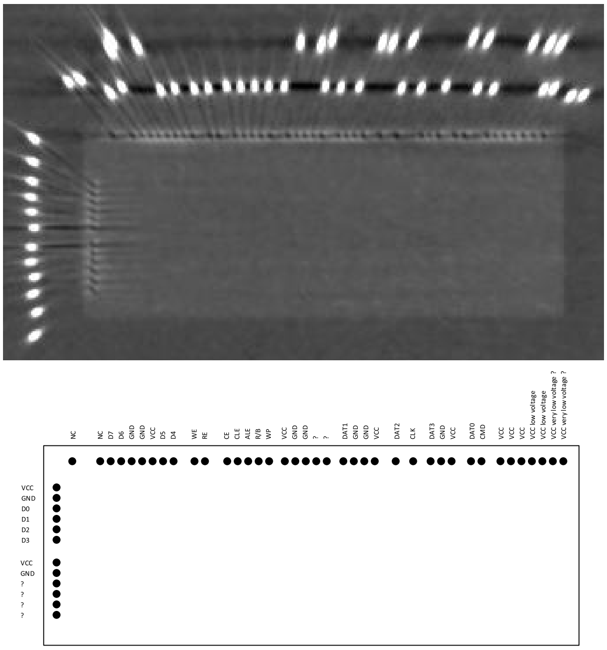


FIGURE 21. Signal identification (lower image) of the microcontroller bondings (upper image) after a reverse engineering study with 3D X-Ray slices.

To summarize, X-Ray observations, specifically 3D X-Ray tomography images, are very powerful when the card to be diagnosed is an unknown model since it is essential to be able to identify the card model during the diagnostic process. However, forensic experts should be aware of the possibility of introducing incorrigible bit errors [31] when using X-Rays on multilevel flash memories [32]. As with every method, forensic experts must carefully evaluate the pros and cons.

3) SCANNING ACOUSTIC MICROSCOPY ANALYSIS

Acoustic scanning is an observation technique that can determine the presence of air in a component package by using the propagation of an acoustic wave in water. The sample is immersed in water while a probe projects an acoustic wave in the order of 10 to 100 MHz. This wave will pass through several successive media: first the surrounding water, then the component package, and finally the chips. Without air in the package, the signal is returned with the same phase as the signal emitted. With the presence of air in the package, the signal is disturbed. By scanning the sample on three axes,

[4] This is the microcontroller for the card presented in Figures 5 and 18.

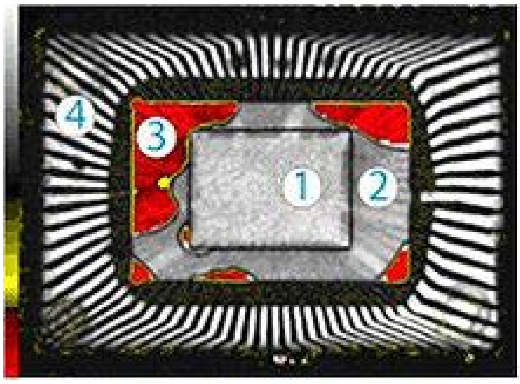


FIGURE 22. Example of delamination on a sample lead frame viewed with a SAM analysis [33].

the microscope will produce an image indicating the so-called delamination areas and the healthy areas (Figure 22). On Figure 22, the delamination area, highlighted in red, means that moisture is able to penetrate into the package in that region, causing a risk of corrosion.

This technique is widely used in failure analysis laboratories in the search for and diagnosis of several structural defects [34]. This is an extra way for non-invasive diagnosis to observe moisture propagation in the component. An SD card has a resin and varnish package, showing only the metal pins for communication with the host. These pins are coated with gold to protect them from degradation. The other metal parts are protected by the package. If a crack or a scratch appears in the resin or varnish, moisture can infiltrate and create an area of corrosion. If the die is corroded, data retrieval will not be possible. However, if corrosion is on a track, the signal could be cut, making the SD card non-functional. As illustrated in Figure 12, the decision-making diagram allows the subsequent use of 3D X-Ray observation to identify this type of defect, enabling repair of the assembly defect, which is not covered in this paper.

B. INVASIVE DIAGNOSTICS

Invasive diagnostics are not without risk to the sample. In the context of forensic expertise, it is important that the nature and traceability of the evidence are guaranteed. Specifically, in the context of a legal investigation, invasive diagnostics can only be used after having obtained authorization from a judge. Indeed, an invasive technique can alter or destroy information by accentuating or creating a defect. For this reason, an invasive technique should always be thoroughly practiced and mastered. Training and a good knowledge of the procedures are therefore very important before using the following techniques:

- basic electrical tests;
- infrared analysis;
- chemical sample opening.

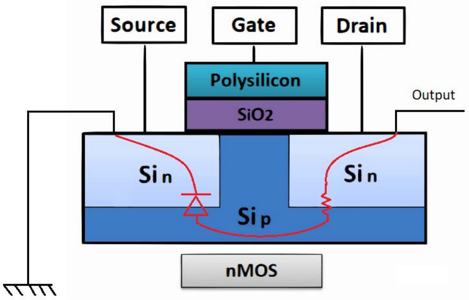


FIGURE 23. Electrical behaviour of inert nMOS transistor.

Each of these is detailed below.

1) BASIC ELECTRICAL TESTS

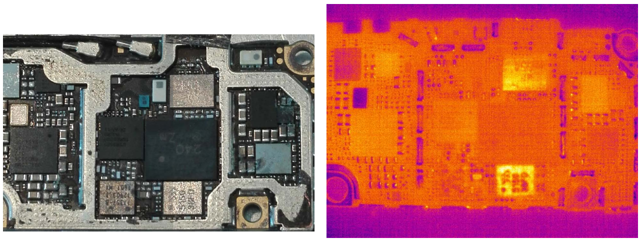
The purpose of this analysis is not to study the card during operation but to look for potential faults in the junctions at the level of the input/output signals. So-called active electronic circuits, such as memory dice or microcontrollers, are based on CMOS technology [35]. Therefore, they have protection diodes on the input, output or bidirectional signals; the direction of the diode varies depending on the nature of the signal. These diodes, induced by the transistors which drive the signals, are connected either to the power or to the ground (GND) of the component (Figure 23) and are easily observable with a multimeter [36]. By positioning probes between a signal and the ground, it is possible to observe either a functioning diode (meaning correct operation), or a short-circuit or an open circuit (meaning a failure of the signal).

By scanning each input/output of each component of the SD card in this way; i.e. the microcontroller and memory dice, the faulty element in the chain can be located. According to Figure 13, a forensic expert can check the die impacted by searching for anomalies with 3D X-Rays to decide what type of repair can be conducted.

2) INFRARED ANALYSIS

An infrared camera, also called a thermal camera, records the infrared radiation (also called heat waves) emitted from an object, which will vary according to the object's temperature (Planck's law [37]). On a theoretical level, infrared wavelengths cover the range from 780 nm to 1 µm, but the cameras used in electronics work on a range from 2 µm to 15 µm. Infrared cameras capture a matrix of thermal points, producing a color-scale image. This technique has the drawback of being ineffective on reflective areas. Consequently, areas with a mirror effect, such as the rear faces of silicon chips or raw metal shields, will appear on the images as heat sinks, distorting the statistical analysis of the image (Figures 24a and 24b). Despite this minor drawback, this technique makes it possible to identify anomalous areas of high heat (or abnormally low heat), and to highlight a defect.

In general, the study of a sample is carried out in comparison with a control sample (i.e. a similar functional product).



(a) Optical view of a part of a phone

(b) IR view of the same phone in operation

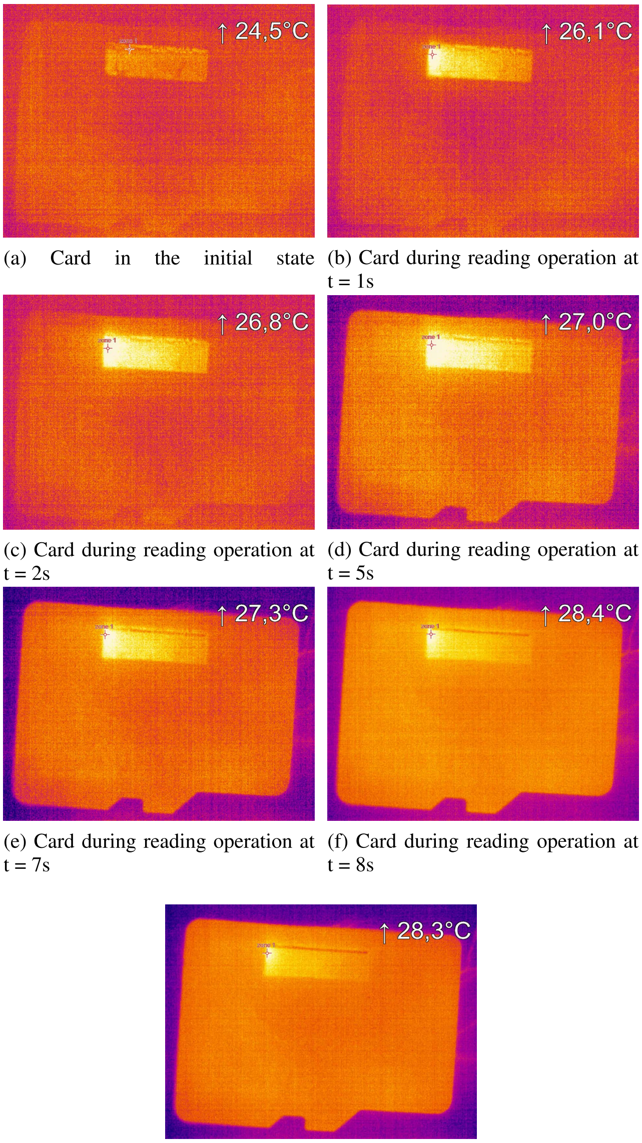
FIGURE 24. Example of identification of components and a view of their thermal emissions during operation.

This principle allows comparison of hot and cold spots to identify differences in behavior between the two samples. The thermal camera highlights transient effects, which are normally difficult to detect (Figure 25). According to Figure 13, identifying such issues enables a forensic expert to check relevant failures using 3D X-Ray images to then decide whether and how these failures can be repaired.

In this example of image acquisitions using an infrared camera, the micro-SD card is detected by the computer but the reading and writing processes are not possible. The computer offers only the possibility to format the card. In this initial state, the micro-SD card is powered on (Figure 25a), then the card is requested for reading by the host. As shown in Figures 25b, 25c and 25d, heat builds up very quickly in half of the microcontroller. In order to preserve the card, the forensic expert observing this phenomenon has to be ready to stop the experiment immediately. A difference in overall coloration of Figures 25a, 25b and 25c can be observed due to the auto-calibration of the camera. The difference in coloration between Figures 25c to 25g is due to heat propagation and dissipation in the micro-SD card package. With such analysis, it is difficult to accurately identify the starting point of the fault and the evolution of heat. It is possible that:

- The temperature will continue to increase until it reaches a threshold that is dangerous for the integrity of the chip materials. In this case, the forensic expert must be ready to stop the process to cool the controller. The experiment will have made it possible to identify the faulty chip but not the precise location. In this case, there is no stabilized state that could be qualified as a final state.
- The temperature will stop increasing, which allows the camera to adapt and therefore to provide a more precise image of the area where the fault is located. In this case, there is a stabilized state that can be called a final state. This is the moment when the system has reached a thermal equilibrium, allowing the expert to make a precise observation without risk of degradation of the sample.

When using an infrared camera, a challenge for the forensic expert is to determine whether the sample will reach a final state (and thus a stabilized state). The forensic expert will have to launch several image acquisitions to validate the assumption, each time on a slightly longer time base, until a stabilized state is reached.



(a) Card in the initial state

(b) Card during reading operation at t = 1s

(c) Card during reading operation at t = 2s

(d) Card during reading operation at t = 5s

(e) Card during reading operation at t = 7s

(f) Card during reading operation at t = 8s

(g) Card during reading operation: final state

FIGURE 25. IR acquisition on a micro-SD card during normal powering up and reading phases.

Returning to our example, the temperature of the micro-SD card stops increasing. The camera therefore succeeds in defining the intense heat zone, as shown in Figures 25e and 25f. In the final state (Figure 25g), the forensic expert can distinguish a warm-up point on the left of the map not far from the row of bondings. By comparing the timing of the acquisition and the operations carried out on the micro-SD card, it can be shown that the connection of the micro-SD card to the computer (and therefore the power-up) did not cause an operating fault. However, it establishes there is an internal fault in the transistors in the microcontroller, which prevents the forensic expert from accessing the data. As explained before and according to the decision diagram (Figure 13), the forensic expert must check, using 3D X-Ray analysis, whether the failure is visible in order to then decide to switch to either a reparation or to a chemical opening of the sample to search for the failure inside.

3) CHEMICAL SAMPLE OPENING

This is the most destructive technique that can be used to diagnose a fault [38] as it will remove the protective resin from the chips to expose them [39]. There are several chemical solutions that can achieve this, but the most common is to locally deposit drops of fuming nitric acid 100 % previously heated to 90 °C to carry out a localized attack on the chips [26]. There are several constraints on using this technique. First, the area of attack must be identified with an X-Ray view and then the concentrated acid must be applied at the right place. The attack must also be controlled to expose only the silicon without overexposing other elements, such as bonding, or copper PCB, which would be severely damaged. To avoid this problem, it is possible to change the process by modifying the attack temperature, the nature of the chemical, or the nature of a possible mixture. The most commonly used solution is a mixture of fuming nitric acid 100 % diluted to 60 % in sulfuric acid heated to only 40 °C [40]. This chemical attack, although it takes longer to set up, keeps the copper elements safe and therefore keeps the SD card functional [41]. An alternative to manual etching is to use a machine designed for the chemical opening of components (Figure 26). There are several brands of equipment on the market and the investment is worthwhile for batch processing or for repeatability requirements.

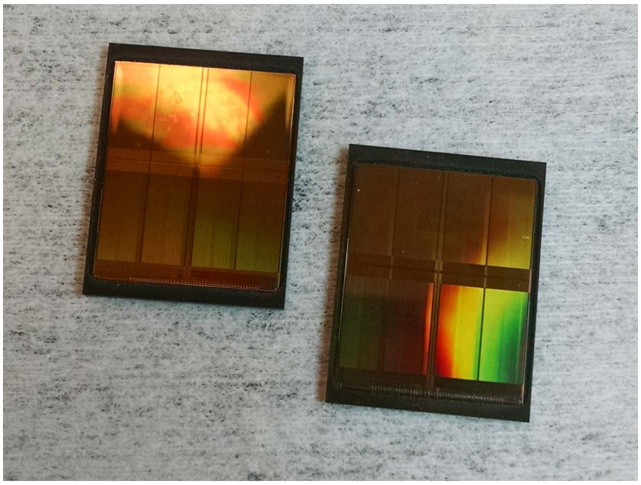


FIGURE 26. Example of sample opening with RKD Jet etcher Acid Decapsulator [42].

Another way to accelerate the chemical attack is by using laser ablation. Using a laser, the forensic expert can start by making a window in the resin at the location of the defect, removing much of the resin (Figure 27). The acid applied will be directed and centralized by laser ablation through the hole that has been created. The exposure time to acids will be considerably reduced, in order to increase the chances of success [43].

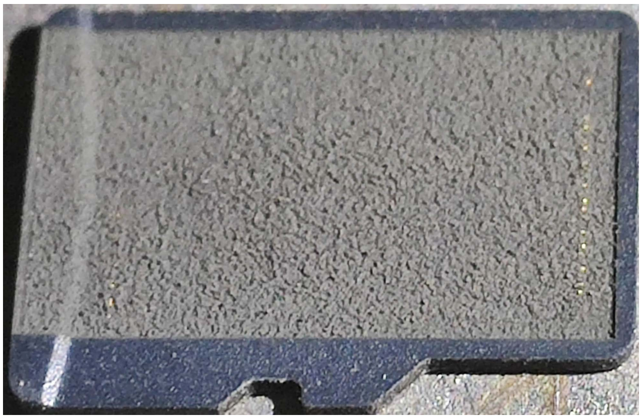


FIGURE 27. Example of a micro-SD card after laser preparation.

The purpose of implementing all of these techniques together is to determine the origin of the card malfunction, in order to identify which chip(s) is affected. As already introduced in part III, each chip has a function but the main objective was to be able to extract the data. The main focus is on the memory chips and a failure of this element definitively stops the study.

IV. CASE STUDY

The case study presented is related to a non-functional SD card. Before presenting the work performed on this media, it is important to specify the context and the rules that must be respected when receiving a sample.

A. CONTEXT

In France, as in many other countries, expertise is not centralized in a single laboratory. There are indeed several laboratories, each with forensic experts who have their own technical specializations. In addition to the state forensic laboratories, depending on the rules applied by law enforcement agencies, there are private laboratories that handle cases for a fee. Due to the plurality of actors, evidence arriving in a laboratory has a past. Although the forensic expert has the context of the origin of the evidence, he/she does not have direct access to the history of the actions carried out by other laboratories on it. Therefore, the reception state of the sample is considered as the original state. Any crack, scratch, or curvature of the sample must be considered as original and treated as such.

B. SAMPLE PRESENTATION

The sample in the case study is an SD card (Figure 28). First, it can be seen that the plastic package enveloping the dice and the PCB has been removed. No writing is visible on the PCB or on the resin. It is therefore not possible to directly obtain the manufacturer, model or memory size of the card. However, some information can be inferred. For

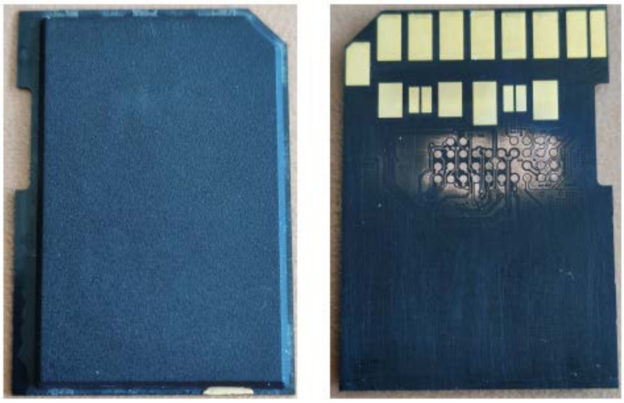


FIGURE 28. Optical view of the front and back sides of an SD card from a real case in the condition in which it was received.

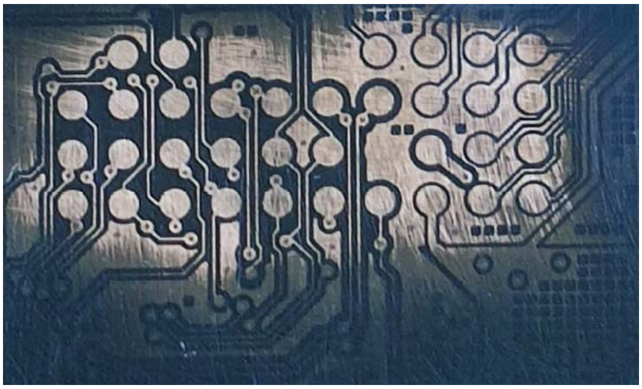


FIGURE 29. Initial diagnostic, using a binocular microscope, of a part of the studied SD card: no visible defect noted.

instance, the bus topology of the SD interface is that of a UHS-II card, which suggests a recent card designed for fast communication, with a huge memory size. It will be possible with a 2D X-Ray analysis to observe the design of the PCB tracks, which can sometimes suggest a manufacturer.

According to the information from the requester, the SD card is recognized when inserted in a reader, but requests formatting, and access to current data is not possible. The purpose of the expert analysis is to access the data contained in this SD card. To do so, the protocol described in Figure 11 is strictly applied to initiate the diagnostic phase and orient the expertise according to the results obtained. Then the necessary repair protocol will be applied to recover data.

C. NON-INVASIVE SAMPLE ANALYSIS

1) OPTICAL INSPECTION

According to the proposed forensic decision diagram, an optical inspection is performed (Figure 28). With regard to the resin, no crack, delamination or any other defect can be observed. Looking at the PCB, an abrasion has been carried out at the level of the memory debug pads (Figure 29). This polishing may have several origins, either accidental or deliberate by another laboratory during an attempt to perform a diagnosis. Given the shape and position of this polishing, the diagnostic hypothesis is prioritized. Moreover, it was correctly performed because no track was damaged.

As the optical inspection does not provide information about the defect in the card, the next step in the decision diagram (Figure 12) is performed. In the absence of visible delamination and without any indication of immersion, use of the SAM can be omitted to focus on the next stage: X-Ray observations.

2) X-RAYS OBSERVATIONS

Since no anomalies were observed during optical inspection, an X-Ray observation is performed. First, the observation is made in two dimensions, looking for identifiable defects. Due to the density of the elements constituting this SD card, some areas in the images appear difficult to interpret. Since the 2D analysis does not show any visible damage, a 3D examination is carried out to collect more information.

As mentioned previously, 3D tomography is the most effective way to locate a structural anomaly in a complex technological stack. For the case study, Figure 30 shows the layers of interest in the SD card. Two of them are the PCB layer on the chip side (Figure 30a) and the PCB layer on the debug pads side (Figure 30b), on which there are no cutting tracks. The other points of interest are the dice (Figure 30c) and their bondings (Figure 30d). However, the images show no defects and the X-Ray observation being the last non-invasive step in the decision diagram (Figure 12), the next phase is invasive diagnostics.

D. INVASIVE SAMPLE ANALYSIS

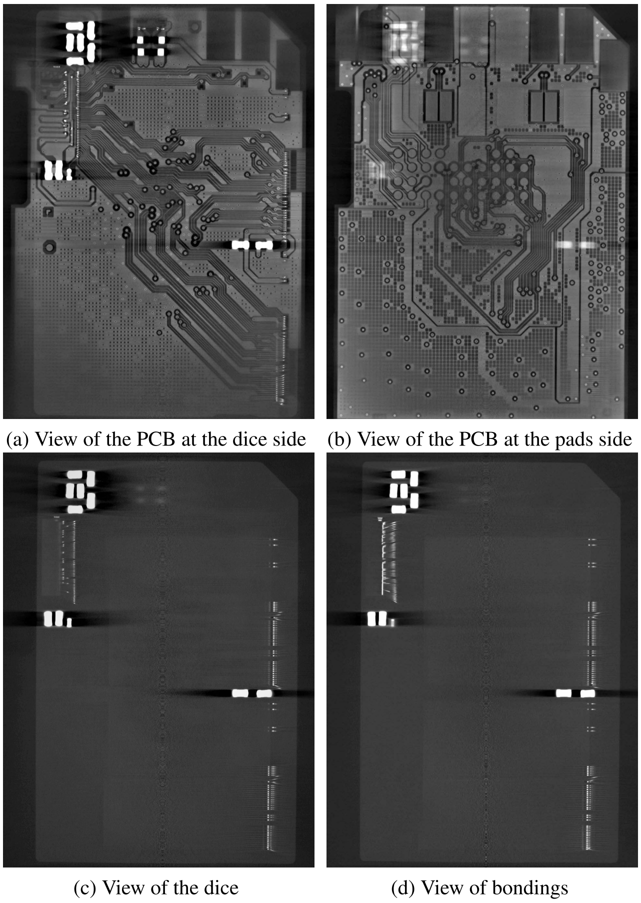
As described in Figure 13, the first step involves electrical tests.

1) ELECTRICAL TESTS

The behavior of the SD card described in section IV-B indicates a recognition by the host of the SD card but not of the file system. This information would indicate that the electrical behavior of the microcontroller is normal. To verify this, a diode test with a multimeter is performed on the external pads of the SD bus. This test being conclusive, a second analysis is performed at the level of the debug pads present between the memory and the microcontroller. This test also being conclusive, there is no shortcut between the signal and the power supply on the dice of the SD card. This conclusion allows the forensic investigator to move on to the next step in the decision diagram (Figure 11), i.e. infrared camera analysis.

2) INFRARED ANALYSIS

To evaluate potential defects as reflected by the temperatures measured using an infrared camera, a comparative thermal analysis is performed on the case study (Figure 32) and on a control sample (Figure 31). To execute the test, the SD card is connected to a host by a card reader controlled by


(a) View of the PCB at the dice side (b) View of the PCB at the pads side

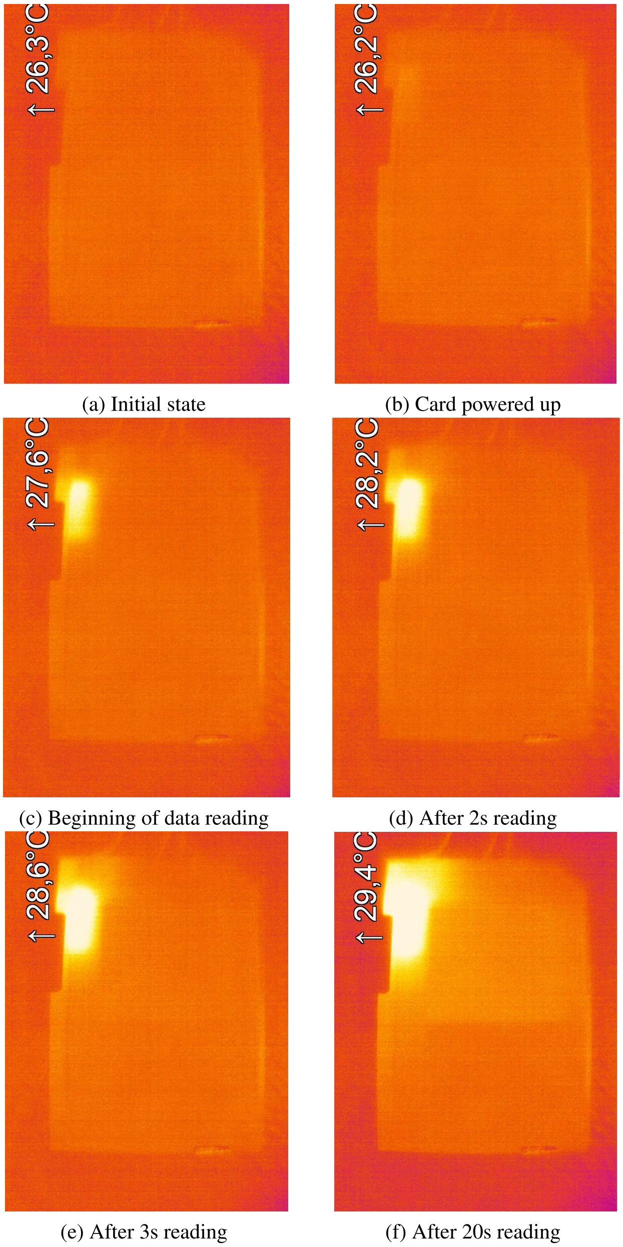
(c) View of the dice (d) View of bondings

FIGURE 30. 3D X-Ray view of the different layers of interest on the studied SD card: no defect detected.

a script, powering on the card and then reading 500MB of data at a random address. This piloting phase, taking a few seconds, is performed while the card is placed under the infrared camera.

In the initial state, the card has not been driven and it is at rest. The whole of the card has a homogeneous coloring and therefore a homogeneous temperature of 26°C (Figure 31a). As soon as the script is started, the host powers up the card. A minimal color change is observed in the top left corner (Figure 31b), corresponding to the position of the microcontroller die according to the X-Rays (Figure 30c). Then the host switches to data reading mode and executes multiple successive requests. This action has the effect of increasing the functioning of the microcontroller (Figure 31c). The temperature of the microcontroller changes to 27°C and continues to increase as shown in Figure 31 after 2 seconds (Figure 31d), 3 seconds (Figure 31e) and 20 seconds (Figure 31f). The reading is finished after 20 seconds, and on this sample, only the activity of the microcontroller is observable.

In contrast to the behavior of the sample control, the case study card shows an increase in temperature at the memory from the initialization phase (Figure 32b). This is the hot spot at the bottom right. When the script switches to the reading



(a) Initial state (b) Card powered up

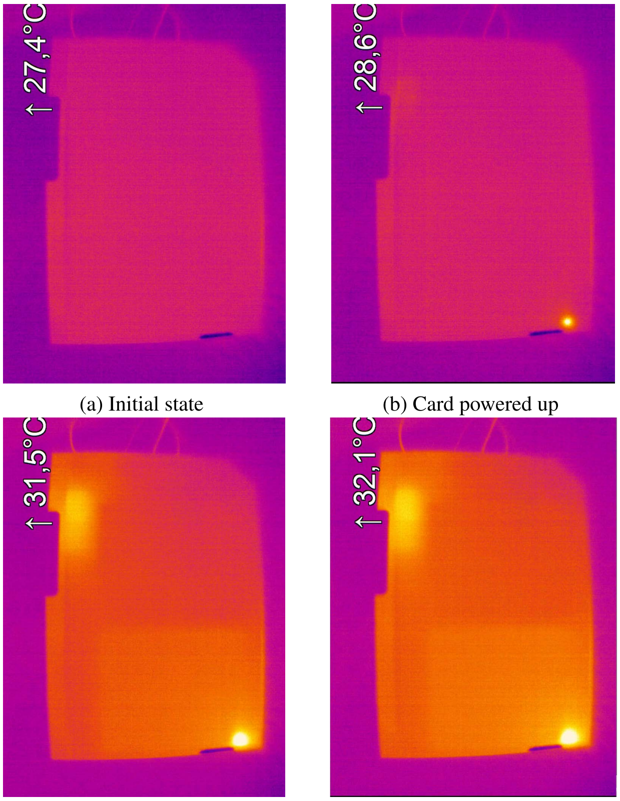
(c) Beginning of data reading (d) After 2s reading

(e) After 3s reading (f) After 20s reading

FIGURE 31. Infrared view of the control sample for the studied SD card during powering up and reading phases.

phase, the rise in temperature at the memory is even more noticeable (Figure 32c) and increases with time (Figure 31d). In view of the result, the analysis is stopped in order to avoid further damage to the card.

Analysis of the infrared camera images (Figure 32) and X-Ray images (Figure 30c) confirms the position of the fault in the memory, at the position of a series of bondings. Considering that the component is in a rigid package, it is normally not possible for the bondings to move and to touch each other. There are therefore two hypotheses that can explain the phenomenon. The defect may be in the bondings, and in this case the temperature has increased enough to melt the



(a) Initial state

(b) Card powered up

(c) Beginning of data reading

(d) After 3s reading

FIGURE 32. Infrared view of the studied SD card during powering up and reading phases: a defect is detected at the bottom right.

resin to allow the bondings to join. Alternatively, fusion of the circuitry has occurred internally in the die (i.e. fusion of the silicon, silicon oxides and tracks).

At this stage of the analysis, it was not possible to proceed because further investigation would require a chemical opening to observe the bondings and the surface of the dice. We did not have access to a chemical laboratory to continue investigations. However, the aim of this case study was not to perform all the steps of the proposed forensic decision diagram (Figure 11) but to illustrate its practicability for forensic experts in the choice of diagnostic techniques to be used, both to save time and to reduce the risk of creating additional damage in the sample.

V. DISCUSSION

This paper, to the best of our knowledge, has introduced for the first time the possibility of using an infrared camera as a diagnostic method in forensic protocols for digital devices. However, this method must be classified as an invasive method since the infrared diagnosis requires the SD card to be powered on, which increases the risk of accentuating or creating a fault not previously diagnosed.[5]

At the end of the diagnostic process using the decision-making diagram, providing a "data lost" state has not been reached, the next steps are first the reparation of the SD card, which is out of the scope of this paper (some examples can be found in [8], [11]) and then the reading of data either via the external interface or by interfacing directly with the memory dice,[6] for instance if the microcontroller is out of service. After the physical reading of data from the memory dice, the task faced by forensic experts is complex. To obtain exploitable data from the raw data, they have to reproduce all the operations of the microcontroller but without the same level of knowledge (e.g. how data are spread among the different dice and the ECC algorithm is often unknown). Among the different operations from the raw dump, forensic experts will have to remove manufacturing memory defects in the dice (called "bad columns"), to find page structures and to find the ECC type used to then correct the pages in the dump accordingly (and if ECC data are not sufficient, they will have to read corrupted areas again), to find the right XOR key (which can be dynamic) to get access to page contents and finally to reassemble all blocks and their pages in the right order to produce an image containing partitions and file systems. For these tasks, forensic experts can use software like PC-3000 Flash [44] or VNR (Visual Nand Reconstructor) [45].

VI. CONCLUSION

In the context of forensic investigations, experts are increasingly collecting evidence from removable memory devices, particularly the popular SD cards. These cards are used everywhere, including by criminals (from small-scale traffickers using them as data storage in their mobile phones to international mobs using them as key stores to encrypt data on high security smart phones). In addition, following air crashes, terrorist attacks or explosions, the judges in charge of investigations are now systematically requesting the extraction of digital data to understand the crime scene from videos that may have been filmed during the incidents. These two examples illustrate that forensic experts have more cases to handle and they need to adapt their protocols by developing new diagnostic techniques, which were until now very marginal.

Therefore, the main contribution of this study is the proposal of a new forensic protocol for damaged SD cards, which aims at minimizing the risk of creating additional damage during the diagnosis of existing damage. Since it relies on an effective decision-making diagram encompassing the main non-invasive and invasive techniques, it strengthens the ability of forensic experts to successfully handle more cases. In addition, for the first time, a new infrared diagnostic technique has been introduced to highlight transient effects that are potentially dangerous for data preservation and not visible by other conventional methods.

[5] For all invasive methods with a particularly high risk of damaging evidence, forensic experts must first obtain authorization from a judge before using them.

[6] Physical reading of memory dice is often preferred since it allows access to more artifacts that may be of interest.

In future work, the new infrared diagnostic technique will be studied further and innovative repair methods to obtain the raw data will be explored.

ACKNOWLEDGMENT

The authors would like to thank Graham Houghton for his support, proofreading, and contribution to this paper.

REFERENCES

[1] C. Shepherd, G. Arfaoui, I. Gurulian, R. P. Lee, K. Markantonakis, R. N. Akram, D. Sauveron, and E. Conchon, "Secure and trusted execution: Past, present, and future—A critical review in the context of the Internet of Things and cyber-physical systems," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 168–177.

[2] S. Willassen, "Forensic analysis of mobile phone internal memory," in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi, Eds. Boston, MA, USA: Springer, 2005, pp. 191–204.

[3] K. Seeger, *Semiconductor Physics*. Vienna, Austria: Springer, 2013, p. 504.

[4] SD Association, San Ramon, CA, USA. *SD Association Home Page*. Accessed: Feb. 13, 2022. [Online]. Available: https://www.sdcard.org/

[5] S. Association. *SD Association Home Page*. Accessed: Feb. 13, 2022. [Online]. Available: https://www.sdcard.org/

[6] M. Breeuwsma, M. De Jongh, C. Klaver, R. Van Der Knijff, and M. Roeloffs, "Forensic data recovery from flash memory," *Small Scale Digit. Device Forensics J.*, vol. 1, no. 1, pp. 1–17, 2007.

[7] R. Van Der Knijff, "Embedded systems analysis," in *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, E. Casey, Ed. St. Louis, MO, USA: Academic, 2001, ch. 11.

[8] T. Heckmann, T. Souvignet, D. Sauveron, and D. Naccache, "Medical equipment used for forensic data extraction: A low-cost solution for forensic laboratories not provided with expensive diagnostic or advanced repair equipment," *Forensic Sci. Int., Digit. Invest.*, vol. 36, Mar. 2021, Art. no. 301092.

[9] C. Maartmann-Moe, S. E. Thorkildsen, and A. Årnes, "The persistence of memory: Forensic identification and extraction of cryptographic keys," *Digit. Invest.*, vol. 6, pp. S132–S140, Sep. 2009.

[10] N. BC. *No.1 BC Home Page*. Accessed: Feb. 13, 2022. [Online]. Available: https://no1bc.com/

[11] T. Heckmann, "Reverse engineering secure systems using physical attacks," Ph.D. dissertation, Dept. Math., Ecole Normale Superieure de Paris, Univ. Paris Sci. et Lettres, Paris, France, 2018.

[12] J. P. van Zandwijk and A. Fukami, "NAND flash memory forensic analysis and the growing challenge of bit errors," *IEEE Secur. Privacy*, vol. 15, no. 6, pp. 82–87, Nov. 2017.

[13] A. Fukami, S. Ghose, Y. Luo, Y. Cai, and O. Mutlu, "Improving the reliability of chip-off forensic analysis of NAND flash memory devices," *Digit. Invest.*, vol. 20, pp. S1–S11, Mar. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287617300415

[14] N. Y. Ahn and D. H. Lee, "Forensics and anti-forensics of a NAND flash memory: From a copy-back program perspective," *IEEE Access*, vol. 9, pp. 14130–14137, 2021.

[15] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[16] J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 1–15, Jan. 2020.

[17] S. Amiroon and C. Fachkha, "Digital forensics and investigations of the Internet of Things: A short survey," in *Proc. 3rd Int. Conf. Signal Process. Inf. Secur. (ICSPIS)*, Nov. 2020, pp. 1–4.

[18] R. Bez, E. Camerlenghi, A. Modelli, and A. Visconti, "Introduction to flash memory," *Proc. IEEE*, vol. 91, no. 4, pp. 489–502, Apr. 2003.

[19] S. Fiorillo, "Theory and practice of flash memory mobile forensics," in *Proc. Austral. Digit. Forensics Conf.*, 2009, p. 37.

[20] (2010). SD Card Association. *Physical Layer Specification Version 3.01*. [Online]. Available: https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/imx-process% ors%40tkb/3706/1/Part_1_Physical_Layer_Specification_Ver3.01_Final_100218.pdf

[21] (2021). Open NAND Flash Interface Workgroup. *Open NAND Flash Interface Specification Revision 5.0*. [Online]. Available: https://media-www.micron.com/-/media/client/onfi/specs/onfi_5_0_gold.pd% f

[22] (2016). JEDEC SOLID STATE TECHNOLOGY ASSOCIATION. *NAND Flash Interface Interoperability—JESD230D*. [Online]. Available: https://media-www.micron.com/-/media/client/onfi/specs/jesd230d.pdf

[23] A. Aravindan. (2018). *Flash 101: The NAND Flash Electrical Interface*. [Online]. Available: https://www.embedded.com/flash-101-the-nand-flash-electrical-interface/

[24] C.-K. Hsieh, "Flash memory controller, SD card device, method used in flash memory controller, and host device coupled to sd card device," U.S. Patent 10 691 589, Jun. 23, 2020.

[25] M.-C. Yang, Y.-M. Chang, C.-W. Tsao, P.-C. Huang, Y.-H. Chang, and T.-W. Kuo, "Garbage collection and wear leveling for flash memory: Past and future," in *Proc. Int. Conf. Smart Comput.*, Nov. 2014, pp. 66–73.

[26] F. Kerisit, B. Domenges, and M. Obein, "Comparative study on decapsulation for copper and silver wire-bonded devices," in *Proc. Int. Symp. Test. Failure Anal.*, Nov. 2014, pp. 87–93.

[27] B. P. Flannery, H. W. Deckman, W. G. Roberge, and K. L. D'Amico, "Three-dimensional X-ray microtomography," *Science*, vol. 237, no. 4821, pp. 1439–1444, 1987.

[28] R. Gordon, R. Bender, and G. T. Herman, "Algebraic reconstruction techniques (ART) for three-dimensional electron microscopy and X-ray photography," *J. Theor. Biol.*, vol. 29, no. 3, pp. 471–481, 1970.

[29] (2021). ACE Lab. *PC-3000 Flash Solution Center*. [Online]. Available: http://www.pc3000flash.com/solbase/monochips.php?lang=eng

[30] (2021). *ACE Lab*. [Online]. Available: https://www.acelaboratory.com/

[31] S. Gerardin, M. Bagatin, A. Paccagnella, A. Visconti, S. Beltrami, M. Bertuccio, and L. T. Czeppel, "A study on the short-and long-term effects of X-ray exposure on NAND flash memories," in *Proc. Int. Rel. Phys. Symp.* IEEE, 2011, pp. EX.1.1–EX.1.5.

[32] M. J. Gadlage, M. J. Kay, J. D. Ingalls, A. R. Duncan, and S. A. Ashley, "Impact of X-ray exposure on a Triple-Level-Cell NAND flash," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 6, pp. 4533–4539, Dec. 2013.

[33] (2008). *SD Card Reader Using the M9S08JM60 Series*. [Online]. Available: https://www.nxp.com/docs/en/reference-manual/DRM104.pdf

[34] S. Atkins, L. Teems, W. Rowe, P. Selby, and R. Vaughters, "Use of C-SAM acoustical microscopy in package evaluations and failure analysis," *Microelectron. Rel.*, vol. 38, no. 5, pp. 773–785, May 1998. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0026271497002205

[35] M. Bushnell and V. Agrawal, *Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits*, vol. 17. Boston, MA, USA: Springer, 2004, p. 690.

[36] A. Terao, D. Flandre, E. Lora-Tamayo, and F. Van de Wiele, "Measurement of threshold voltages of thin-film accumulation-mode PMOS/SOI transistors," *IEEE Electron Device Lett.*, vol. 12, no. 12, pp. 682–684, Dec. 1991.

[37] S. N. Bose, "Planck's law and the light quantum hypothesis," *J. Astrophys. Astron.*, vol. 15, p. 3, Mar. 1994.

[38] T. Heckmann, J. P. McEvoy, K. Markantonakis, R. N. Akram, and D. Naccache, "Removing epoxy underfill between neighbouring components using acid for component chip-off," *Digit. Invest.*, vol. 29, pp. 198–209, Jun. 2019.

[39] G. H. Yen and N. K. Kay, "A sample preparation on decapsulation methodology for effective failure analysis on thin small leadless (TSLP) flip chip package with copper pillar (CuP) bump interconnect technology," in *Proc. Int. Symp. Test. Failure Anal.*, Nov. 2014, pp. 100–104.

[40] EDFAS Desk Reference Committee and Others, *Microelectronics Failure Analysis: Desk Reference*. Materials Park, OH, USA: ASM International, 2011.

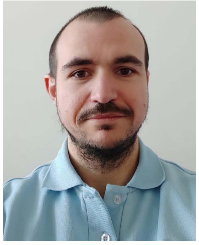
[41] H. B. Kor, Q. Liu, Y. W. Siah, and C. L. Gan, "Laser focus depth adaptation for decapsulation of copper wirebonded devices," in *Proc. Int. Symp. Test. Failure Anal.*, Nov. 2014, pp. 94–99.

[42] (2021). Wikipedia Contributors. *Acoustic Microscop—Wikipedia, the Free Encyclopedia*. Accessed: Jul. 30, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Acoustic_microscopy&oldid=10% 15333092

[43] M. J. Lefevre, F. Beauquis, J. Yang, M. Obein, P. Gounet, and S. Barberan, "New method for decapsulation of copper wire devices using laser and sub-ambient temperature chemical etch," in *Proc. IEEE 13th Electron. Packag. Technol. Conf.*, Dec. 2011, pp. 769–773.

[44] (2021). ACE Lab. *PC-3000 Flash*. [Online]. Available: https://www.acelaboratory.com/pc3000flash.php

[45] (2021). Rusolut. *Visual Nand Reconstructor*. [Online]. Available: https://rusolut.com/visual-nand-reconstructor/vnr-software/



F. THOMAS-BRANS is currently pursuing the Ph.D. degree in computer science with the University of Limoges under the supervision of Dean Damien Sauveron and Dr. Thibaut Heckmann. He is also an Engineer with qualifications in computer science, electronics and automation with ESIEA-Paris. Since 2020, he has been a Military Officer with the French Gendarmerie Laboratory, Digital Forensic Department (IRCGN), National Data Extraction Unit. He was for more than ten years a member of the French public administration, has presented papers at numerous international conferences relating to Law Enforcement Agencies, and has been involved in the production of several papers in collaboration with the Ecole Normale Supérieure of Paris of *Digital Investigation* and *Forensic Science International* journals.

T. HECKMANN received the M.Sc. degree in fundamental physics and the Ph.D. degree in mathematics from the Ecole Normale Supérieure of Paris (ENS-Paris). He is currently a Senior Military Officer with the French National Gendarmerie, an Associate Researcher with ENS, and a member of the National Gendarmerie Research Center (CREOGN). From 2015 to 2020, he was the Head of the French Gendarmerie Laboratory, Digital Forensic Department (IRCGN), National Data Extraction Unit. He was a Visiting Researcher with the Royal Holloway University of London, from 2017 to 2018. In 2018, he received the European Emerging Forensic Scientist Award from the European Academy of Forensic Science (EAFS), from 2018 to 2021, and the Cybersecurity Award from Cercle K2, in 2020.

K. MARKANTONAKIS received the B.Sc. degree (Hons.) in computer science from Lancaster University, in 1995, the M.Sc. degree in information security, in 1996, the Ph.D. degree in smart card security, in 2000, and the M.B.A. degree in international management from Royal Holloway University of London, in 2005. He became the Director of the Smart Card Centre, in January 2016. He is currently a Professor in information security with the Information Security Group, Royal Holloway University of London. He has published more than 140 papers in international conferences and journals. His research interests include smart card security and applications, secure cryptographic protocol design, key management, embedded system security and trusted execution environments, mobile phone operating systems/platform security, NFC/RFID/HCE security, grouping proofs, and electronic voting protocols. Since completing his Ph.D., he has worked as an Independent Consultant in a number of information security and smart card related projects. He continues to act as a Consultant on a variety of topics, including smart card security, key management, information security protocols, mobile devices, smart card migration program planning/project management for financial institutions, transport operators, and technology integrators.

D. SAUVERON received the M.Sc. and Ph.D. degrees in computer science from the University of Bordeaux, France. He was the Head of the Computer Science Department, Faculty of Science and Technology, University of Limoges, France, from 2016 to 2020, where he has been an Associate Professor (Habilitation) with the XLIM Laboratory, UMR CNRS 7252, since 2006. Since 2011, he has been a member of the CNU 27, the National Council of Universities, France. He has been the Chair of IFIP WG 11.2 Pervasive Systems Security, since 2014, having previously been appointed the Vice-Chair of the working group. He is currently the Dean of the Faculty of Science and Technology, University of Limoges. His research interests include smart card applications and security (at hardware and software level), RFID/NFC applications and security, mobile network applications and security (particularly UAV), sensor network applications and security, Internet of Things (IoT) security, cyber-physical systems security, and security certification processes. In December 2013, the General Assembly of International Federation for Information Processing (IFIP) awarded him the IFIP Silver Core Award for his work. He has been involved in more than 100 research events in a range of capacities (including the PC Chair, the General Chair, the Publicity Chair, an Editor/Guest Editor, a Steering Committee Member, and a Program Committee Member). He has served as an external reviewer for several Ph.D. thesis in foreign countries and France.