






## A Digital Forensics Approach for Lost Secondary Partition Analysis using Master Boot Record Structured Hard Disk Drives

 Erhan Akbal<sup>1</sup>,  Omer Faruk Yakut<sup>2</sup>,  Sengul Dogan<sup>3</sup>,  Turker Tuncer<sup>4</sup>,  Fatih Ertam<sup>5</sup>

<sup>1</sup>Corresponding Author; Firat University, Technology Faculty, Digital Forensics Engineering, Turkey; erhanakbal@firat.edu.tr; +90 533 493 46 03

<sup>2</sup> Firat University, Department of Digital Forensics Engineering, Turkey; omerfaruk.yakut@egm.gov.tr

<sup>3</sup> Firat University, Department of Digital Forensics Engineering, Turkey; sdogan@firat.edu.tr

<sup>4</sup> Firat University, Department of Digital Forensics Engineering, Turkey; turkertuncer@firat.edu.tr

<sup>5</sup> Firat University, Department of Digital Forensics Engineering, Turkey; fatih.ertam@firat.edu.tr

Received 13 November 2021; Revised 24 November 2021; Accepted 07 December 2021; Published online 31 December 2021

### Abstract

The development and widespread use of computer systems has increased the need for secure storage of data. At the same time, the analysis of digital data storage devices is very important for forensic IT professionals who aim to access information to clarify the crime. File systems of disk drives use partition structures to securely store data and prevent problems such as corruption. In this study, deletion or corruption of partitions on commonly used DOS / Master Boot Record (MBR) configured hard disk drives are investigated by using forensic tools. In order to analyze hard disk drives, Forensic Tool Kit (FTK), Magnet AXIOM, Encase, Autopsy and The Sleuth Kit (TSK), which are widely used as commercial and open source, are analyzed by using a presented scenario. In the scenario, the primary partition and the extended partition are created using the DOS / MBR partitioning structure on the test disk. Test files are added to the sections and the sections are deleted. The digital forensics tools were tested on the presented scenario. According to the obtained results, TSK and Encase are successful tools for DOS / MBR structured HDD analysis. However, FTK, Magnet AXIOM and Autopsy could not achieve information detection on DOS/MBR structured disks. These results clearly demonstrated that crime data can be hidden in MBR structured HDD. To carve these data, the correct methodology should be selected.

**Keywords:** digital forensics, dos/mbr partition, extended partition, lost partition, recovery partition, antiforensic

### 1. Introduction

The purpose of forensic analysis is to discover and present digital evidence in computer systems to reveal the reality of an event [1, 2]. Digital evidence is intended to be scientifically valid, reliable, and verifiable [3]. Knowledge extraction from big data in various formats is very important for digital forensics [4]. The digital evidence that is the main source of forensic information is stored on hard disk drives in computer systems. Digital forensics analysis is basically concerned with identifying, extracting, and analyzing file systems in these data storage systems [1]. With the rapid growth in computer systems, the use of large volume storage devices has increased. As a result of this increase in volume, the time allocated per case in forensic laboratories increases, and forensic processes are prolonged [5]. Digital forensics examiners use commercial or open-source forensics tools to minimize these delays and analyze errors in forensic processes. This age is called an information age [6]. Electronic evidence is crucial for judicial authorities. Therefore, the reliability of digital evidence is based on the correct use and reliability of forensic tools as well as the scientific implementation of the process [7]. Nowadays, digital devices for instance laptops, cameras, and mobile phones have evolved rapidly. Therefore, there are variable digital evidence in practice. In this rapidly changing dynamic environment, it became impossible to find a single forensic tool that could meet all needs [8].

The main task of digital forensic tools is to present obtained evidence in a convenient format for forensic examiners with superficial knowledge, and these tools have a crucial role in an investigation [9, 10]. Suspects may conceal data to prevent forensic analysts from accessing the data or disrupt the data

structure with Anti-Forensic methods. This may cause courts to decide on the basis of false or incomplete evidence [11, 12].

It has led to an increase in anti-forensic methods to prevent the judicial process and interfere with the evidence. The increase in the market share of anti-forensic tools clearly indicates this situation [13]. Moreover, users can easily access anti-forensic tools [14]. User-induced problems also cause data loss like anti-forensics tools. For example; The forensic tools that are dealing with the "42.zip" compression grenades cannot complete the evidence processing process because they cannot open the layered file [9]. Similarly, in the forensic analysis of the partition tables of Guid Partition Table disks, removing the Disk Protected Area and Device Configuration Overlay areas on the disk will prevent the analysis tools from accessing the spare part header and table at the end of the disk as it will change the position of the last sector [15]. In addition, disruption of extended partition structures on a disk configured with the widely used DOS / MBR partition table will prevent access to evidence and evidence metadata data within this corrupt partition.

A disk configured with the DOS / MBR partition table allows up to four primary partitions to be created by nature. In BIOS-based systems, it assigns one of the four standard partitions as extended partitions. These extended partitions are special partitions that can be divided into logical partitions [15, 16].

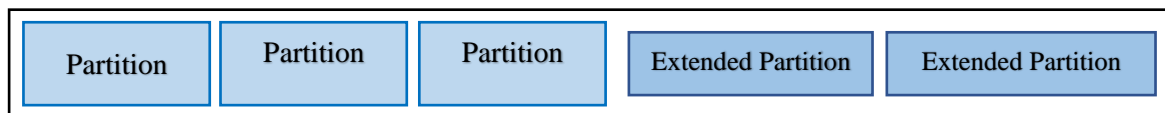


Figure1 Example section layout for bios based systems.

Extended partitions do not receive a partition ID, so logical partitions can be created as much as the capacity of the disk allows. Files can be stored on logical partitions and used as operating system partitions.

Knowing the capabilities of the forensic tool is very important for analysis. The copying and analysis processes of digital materials are completely dependent on forensic tools. For this reason, the findings of the forensic tools in the process of detecting guilt and innocence should be real, reliable, and reproducible. Errors occurring at any stage of the analysis can cause the potential data to be destroyed [17]. Forensic analysts generally rely on the used forensic tools, but different tools show different abilities in recovering and interpreting data on the same evidence. It should be known that all forensic tools have disadvantages as well as their advantages and that a single vehicle is not sufficient for all purposes [18, 19]. For this reason, if the partitions that are commonly encountered with DOS / MBR are corrupted or deleted, a schedule should be planned to detect these partitions.

### 1.1. Novelties and contributions

Novelties and contributions of our work are given below.

- A roadmap for the detection of lost extended partition structures on disks configured with the commonly used DOS / MBR partition table is proposed.
- The performances of popular forensic tools in comparison to the complexity of the extended section structures are compared.
- Data hiding and destruction methods on various disk areas are defined by using partition structures.
- The method for determining the location of the missing partitions on the disk by calculating all the parts on the disk is proposed.
- A comparison table regarding the detection of the deleted and destroyed Primary and Logical sections and the capabilities of the forensic tools in accessing the data within these sections were shown.
- Different forensics tools were examined.

## **1.2. Our scenario**

In this scenario, a five volume HDD is presented. Three of them primary and two of them secondary. Then, we stored documents these volumes. Then, a primary and a secondary volume were deleted. To recover the deleted document, analyses have been performed by using six tools and a manual analysis. By using this scenario, a comprehensive benchmark is obtained and an optimum algorithm has been obtained for the MBR partitioned problem.

## **1.3. Organization**

The rest of the article is organized as follows. The literature on anti-forensic methods has been examined. With the detection of deleted or destroyed partition structures on disks configured with DOS / MBR partition table, the methods of accessing the data in it are presented, and the competencies of commonly used forensic tools in this regard are compared according to the results of the sample scenario application and presented in the Methodology section. The results and the findings obtained in the discussion section are shown. The limits of our work are presented in the limitation section. Conclusion and future studies are presented in the last section.

## **2. Related Work**

Digital forensics processes are directly proportional to the understanding of anti-digital forensics applications. For this reason, the results caused by the techniques that prevent digital forensics processes should be examined further [20]. Tools designed for anti-digital forensics purposes are typically divided into two categories. The first category is special anti-digital forensics tools. These tools can operate in the form of data hiding, data removal, data processing/editing/masking, Data confusion, and physical destruction. The second category is disruptive technologies. Disruptive technologies have a primary legitimate function and goals. Thus, any investigation may also have a detrimental effect on the relevant digital data in a device [21]. Anti-digital forensics tools and methods, which try to endanger the existence or reliability of the evidence throughout the judicial processes, are becoming more common and used every day [22].

There are different studies on anti-forensic information methods that address current problems and point out future methods. For example, one study interfered with six different anti-forensics tools. At the end of each intervention, the forensic copy of the disk was examined with the FTK forensics tool. In the study where the performance of these anti-forensics tools was observed; It has been observed that each anti-digital forensics tool performs incomplete deletion on unallocated areas. In this case, it was pointed out that it could allow the recovery of data from unallocated areas [13].

In another study, the possibility of using timestamps of the ext4 file system, which is an effective tool for data hiding in environments such as Linux operating systems and android devices, was analyzed. In this study, an ext4 digital forensics technique has been designed that shows that the nanosecond part of Ext4 timestamps can be used to create a system with steganographic power [23]. Apart from these, it has been shown that important signatures can be easily changed in order not to be detected by the malware by a one-byte cancellation factor attack method [24]. In addition, it has been revealed that with semantic value manipulation attack, data values with significant semantic meanings have been changed [25]. Moreover, studies have been carried out on anti-digital forensics methods such as attention deficit technique, which creates false objects and increases the analysis time in order to put researchers into wrong solution processes [26]. In another study where anti-digital forensics methods were examined in two different categories as provable and unproven, inconsistencies were examined by comparing the evidence that was attacked with reliable evidence for the detection of counterfeit information in the log and warning information examined as evidence [27]. Apart from these studies, in the literature, hard disk and file cleaning [28], changing file signature information [29], forgery of file timestamps, use of a restricted folder or file names, circular referencing and the use of ASCII character text, attacks, forensic information evasion techniques used to present the findings and digital forensics techniques applied to eliminate traces in Windows operating systems [30-32].

Different studies have been carried out on obtaining data from harddisks. [33] presented a methodology for obtaining OS-independent data from storage devices using UEFI firmware. [15] developed a tool for forensic examination of disks using the GUID partition table. [34] measured the performance of hard disk drives debug interfaces and service access methods. As a result, they have shown that data can be obtained from SATA disks. [35] demonstrated the impact of file systems, memory management, and disk partitioning structures on evidence acquisition. They found that by applying different scenarios, it would be difficult to collect evidence. [36] proposed a validation method for scenario-based file scraping from discs.

### 3. Preliminaries

The main purpose of our study is to explain how to access the data on the disk in case the partition structures are deleted or corrupted on a disk with MBR structured partition structures. In addition, by suggesting a calculation method to determine whether there is a lost partition in the disk partitions, the effects on the MBR methodology and data hiding were examined.

#### 3.1. MBR Methodology

MBR is a disk partitioning system that was originally designed and started to be used in IBM systems. The first sector of MBR hard drives is 512 bytes in size, and bytes are stored as Little Endian [37]. It consists of 3 parts, and these parts are Master Boot Code, Master Partition Table, and MBR Signature [38].

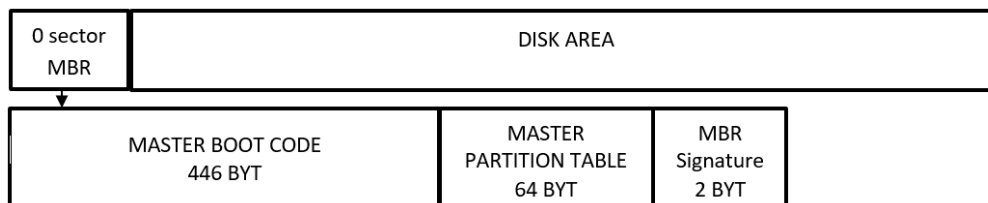


Figure 2 MBR disk location and basic structure.

The Master Boot Code in the MBR structure shown in Figure 2 contains the codes that the BIOS will read and run when the computer is first turned on. Master Partition Table is the part where primary partition information is kept. It can hold information with a range of to one from four sections. MBR signature defines MBR signature bytes. Partition Table size is kept in an area of 64 Bytes, and 16 Bytes are reserved for each section information on the MBR. This allows a maximum of 4 primary partitions to be created on a disk configured with MBR. The extended partition structure is used as a solution to this limitation.

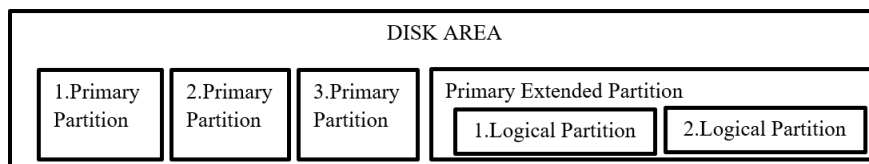


Figure 3 Schematical demonstration of the MBR of Partition Table.

The placement of the partition structures on the disk is shown in Figure 3. Three entries in the MBR define the primary partitions, and one extended partition is defined for the remaining disk space. Primary partition records and primary extended partition records are not kept on the MBR. Primary extended partitions are divided into Logical Partitions in themselves, and the addresses of these separated Logical partitions are kept in the MBR partition table in the first sector of the primary extended partition. Although this is a solution to the limitation of creating a limited number of sections in practice, the willful or unintentional destruction of the logical sections will cause losses related to the data on these sections [39].

In digital forensics analysis, as well as accessing the data, the location information of the data on the disk is also important in the evaluation phase. For example, while an inappropriate content that is inadvertently downloaded is in a location in the *WebBrowserName* \..... \..... within the user directory, the voluntarily downloaded content is usually located in the directories the user uses for storage. In order to reveal this difference, the correct location of the data in the examination process guides the forensic expert. For this reason, accessing the source information of the evidence recovered from deleted and destroyed departments is of great importance in terms of Forensic IT analysis [10].

### 3.2. Partitions can be hidden data

Digital forensic analysis uses data acquisition methods in different layers such as volume, file, and application layers. However, it is an accepted general approach to perform analysis operations on the entire copy of the hard disk. Regarding a forensic copy taken from the volume layer, for example, it will not be possible to access the sectors in the partition table that have been destroyed and the parts that have been deleted during the analysis, since the forensic tool will only copy the sectors in the addressed areas when making copies [40]. On the other hand, there is a reserved area between sectors 1-62 in disks using DOS partitioning structure, and evidence that can be hidden in these areas will not be available [39].

### 3.3. File system corruptions

Many data can be obtained on the partitions. However, basically the data is stored in file systems [41]. In file system analysis, it is possible to reach the location (path), content, and meta data information where the available data are stored. In case the partition structures are corrupted or deleted, the file system structure will also be corrupted as the file systems reside on the partition structures. In this case, although data recovery tools access data within the sectors, they will not be able to access the location (path), content, and meta data information of the data. Therefore, it is important to know the details of disk partitioning structures as well as knowing how a forensic tool works [15].

## 4. Scenario Analysis

A scenario has been created in the laboratory environment for forensic analysis on the disk partitions. On the created scenario, a review was performed with *six* forensic analysis tools. Many file systems have emerged in accordance with the needs arising with technological developments. The developed file systems bring many innovations with it. File systems generally show similarities to each other [42]. However, it differs according to the structure, storage method, and intended use. These differences also affect the analysis and data recovery methods in file systems in terms of Digital Forensics. One of the widely used file systems, New Technology File System (NTFS), was designed by Microsoft and used as the default file system for Microsoft Windows NT, Windows 2000, Windows XP, Windows 7,8,10 and Windows Server [43, 44]. The NTFS file system has been developed to replace the previously widely used File Allocation Table (FAT) file system. When the FAT file system was widely used, the NTFS file system was preferred only on the server-side. It is now widely used in personal computers. NTFS is a much more complex file system than FAT because it is capable and scalable. NTFS is designed for reliability and large storage devices, and thanks to its scalable structure, it allows changes to be made over time in line with new demands. Each byte of data in an NTFS file system is divided into one file [45]. The first entry in the NTFS file system is the "Boot Metadata" file that starts from Sector 0 and can take up to 16 Sectors in length. This file holds the base unit and location of \$MFT. One sector on each allocated NTFS volume belongs to a file. The MFT startup is in Volume Boot Record (VBR). VBR is in a \$Boot record in the MFT [45, 46].

Other legacy and widely used file system FAT is by far the simplest of the file systems supported by Windows NT. It is the map of the disk that indicates the areas in which the information of the files in a disk is recorded. In the FAT file system, the partition is divided into clusters, each containing a certain amount of sectors. Where and how files are written on these clusters is defined on the FAT system.

When the operating system wants to access any file, it takes advantage of this information overwritten by FAT [47].

Recovering data by using MFT / FAT records is a method frequently used by digital forensics experts. Most of the digital forensics tools use MFT records to successfully and rapidly perform data recovery. This situation allowed for the rapid progress of judicial processes [48]. Although manual data recovery methods can be applied using the hex editor, this can cause serious time and labor loss. Manual recovery methods should also be applied when necessary [49].

Digital forensics tools are achieved in data recovery methods with MFT / FAT records. However, in the analysis, there are cases where the location and meta-data information of the recovered data on lost and deleted partition structures on disk areas configured with MBR are missing. In some cases, it is not sufficient for digital forensics tools to search only on file system defined sections. Because in this case, it will not be possible to access the data in the deleted partition that cannot be determined to have a valid file system. The analysis process of disks configured with MBR and not using extended partition structure is easy, but extended partition complicates the analysis process [50].

There has been a significant increase in the size of storage media over the years. However, the size of the logical block format known as the sector, which forms an important part of hard drives, remained constant. In the 2010s, hard drive companies started moving from the old sector size of 512 bytes to a larger, more efficient sector size of 4096 bytes, often referred to as 4K sectors and now referred to as the Advanced Format by IDEMA (International Disk Equipment and Materials Association). However, long-term advantages and potential dangers have emerged during the transition from 512 bytes to 4K sectors. A 512-byte sector can usually correct defects up to 50 bytes in length. Hard drives today are pushing the limits of error correction. Consequently, it has become a basic need to improve the transition to larger sectors, error correction and format efficiencies in the hard drive industry.

It is not possible for the entire hard disk industry to move to the new 4K standard and to change all of these old assumptions suddenly. The methods and calculations to be applied in the study were carried out using traditional 512-byte sectors and disks addressed. It is not available for disk structures with a sector size of 4096 bytes or less 2048 byte, referred to as Advanced Format. For these reasons, in the scenario created for forensic analysis on disk partitions in the laboratory environment, the Test Disk was structured with MBR and created with 3 main partitions and 2 extended partitions. The partition structures created are formatted with NTFS and FAT file system. By labeling the section structures, documents with the same label as the section were copied into these sections, and the created test disk was analyzed with 6 forensic tools and the results were evaluated. The main purpose of the study is to determine the behavior of digital forensics tools related to the complete and lossless recovery of data within the partition structures structured with MBR and to propose a roadmap that will help identify lost partition structures.

#### **4.1. Analysis method**

The existing partition tables should be examined on a deleted disk with suspect partitions, and the consistency of the total size of the disk with the total size of the current partitions should be confirmed. Also, after the control of the end and start sectors of the sections, if there are lost partitions, these sections should be tried to be saved. To determine this process, performing the calculation suggested in Figure 4 on the disk will ensure the accuracy of the analysis process.

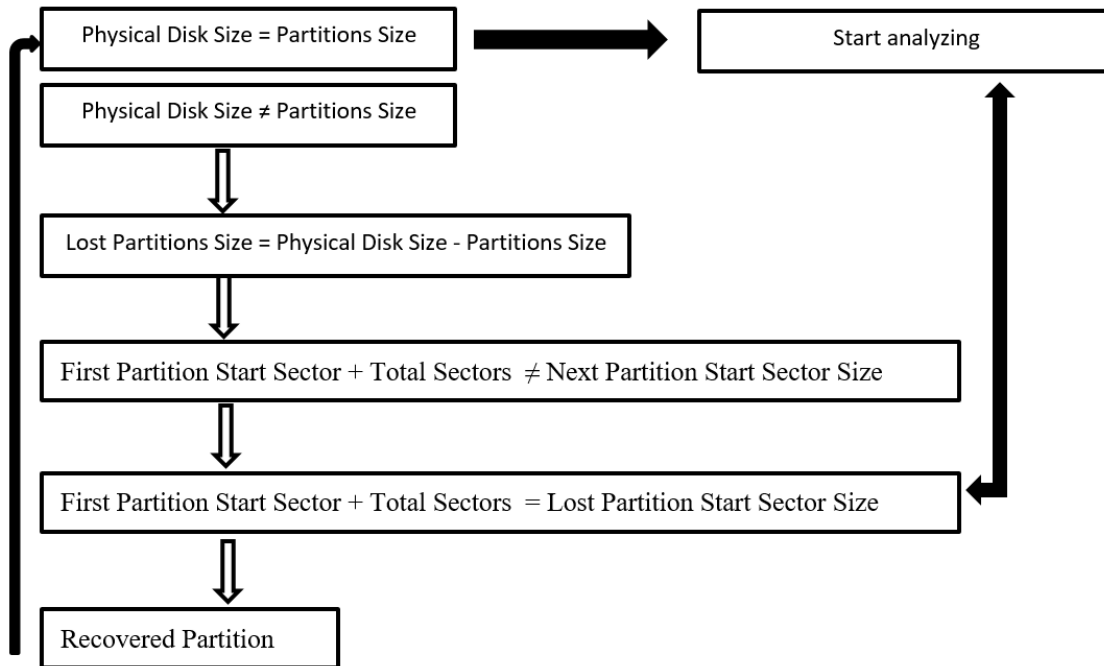


Figure 4 Flow chart of the proposed lost partition detection.

The steps of this process are given below.

**Step 1:** The Total size of the disk to be analyzed is compared with the total size of the available partitions.

**Step 1.1.** If the size is equal, after the confirmation of the operation with the controls in Step 2, the analysis process is started.

**Step 1.2.** If the size is not equal, it should be considered that a lost partition state occurred.

**Step 2:** The sum of the starting sector of the first partition on the disk and the total number of sectors is expected to give the starting sector of the next partition. If the result obtained does not match the results in the section table, it indicates that there may be a lost partition structure. The result obtained in this case gives the physical address of the first sector of the lost partition on the disk. The above procedure is performed on all partitions, respectively, to confirm whether the partition's start and end sectors are the same as in the partition table.

**Step 3:** File system tags (NTFS, FAT etc.) and signature value of 55AA are searched in the first sector of the lost part detected. With this label and signature value confirmed, lost partition recovery is performed.

**Step 4:** After the lost partition is recovered, the calculations in Step 1 are repeated and any lost partitions are detected. Operations continue until 1.1 step confirmation is achieved and then disk analysis is started.

## 4.2. Experimental setup

For this study, a Work Station Computer with HP Z840 intel® Xeon® CPU E5-2680 @ 2.40 GHz (2 Processors), 128 GB RAM and Samsung brand 160 GB hard disk (Test Disk) is used, and this disk is configured with MBR.

Since a maximum of 4 primary partitions can be created on the partitions configured with MBR, the test disk is divided into *five* sections in total, *three* primaries, and *two* extended logical partitions in order to use the extended partition structures. Test.docx, Test.xlsx, and Test.zip documents were created in these *five* sections. These files will be used in the analysis phase to evaluate the success of forensic tools. After deleting *one* primary partition and *one* extended partition from the partitions created in the second part of the study, the test disk will be analyzed using licensed and open-source forensic tools, and the results will be evaluated. The steps of this process are given below.

**Step 1:** The hard disk with 160 GB capacity of Samsung brand is configured with MBR and it is divided into *five* sections as *three* primary partitions and *two* extended partitions.

**Step 2:** Sections are named as VOLUME\_A, VOLUME\_B, VOLUME\_C, VOLUME\_D, and VOLUME\_E.

**Step 3:** Zip, excel, and word documents are created in the sections and are named to be related to the section letters.

**Step 4:** Test documents were added to the Primary Section named VOLUME\_B and to the Extended Section named VOLUME\_E.

**Step 5:** VOLUME B and VOLUME\_E sections were deleted.

The accuracy of the findings to be obtained in case of analyzing the mentioned processes after this scenario was determined.

Disk size and available partitions can be easily calculated with different software as well as using existing analysis software. The values obtained for the initial disk are shown in Table 1.

Table 1 Initial size and sector information of the test disk

Device Name	Disk Image
File Path	O:\SAMSUNG_160_GB_HDD_TEST_IMAGE_V\image.001
Total Size	160.041.888.256 Bytes (149.1 GB)
Total Sectors	312.581.813
Disk Signature	9201C3C1
Partitions	Valid

#### 4.3. The used digital forensics tools for analysis of the defined scenario

After preparing the scenario environment, licensed AccessData Forensic Toolkit, Magnet Axion, Encase open-source licensed Autopsy, and TSK tools were used in forensic investigations. Whether or not test data can be obtained from the scenario created with the analyzes made and accessibility to details such as location and date were investigated. The software and version information used are given in Table 2.

Table 2 The used digital forensics tools.

Software Tool	Version	License
Access Data Forensic Tool Kit	7.0.0.163	Licensed
Encase	8.7.00.93	Licensed
Magnet Axion	3.0.0.13673	Licensed
Autopsy	4.11.0	Open Source
The Sleuth Kit	4.7.0	Open Source

##### 4.3.1. Analysis of the scenario using AccessData Forensic Toolkit

After reading the size and sector information of the test disk, when the partitions determined by the software are checked, a total of 4 partition information was found. It was understood that one of these sections was labeled as a recovered section.

Name	Path	P-Size	L-Size	Category
[Recovered] Partition 1	image.001/[Recovered] Partition 1	29,30 GB	29,30 GB	Partition
Partition 1	image.001/Partition 1	22,09 GB	22,09 GB	Partition
Partition 2	image.001/Partition 2	24,41 GB	24,41 GB	Partition
Partition 5	image.001/Partition 5	19,53 GB	19,53 GB	Partition
Unpartitioned Space [basic disk]	image.001/Unpartitioned Space [basic disk]	n/a	n/a	Unpartitioned Space

Figure 5 Section information detected by FTK software



While the total disk size is supposed to be 149.1 GB, which is the initial calculated value, the total size of the partitions detected by the software; It appears to be 29.30 GB + 22.09 GB + 24.41 GB + 19.53 GB = 95.33 GB.

Consequently, since Physical Disk Size  $\neq$  Partitions Size, the existence of the lost partition structure should be considered. Figure 5 shows that the size of the recovered partition is 29.30 GB. When the files in the partition structure are given the same letter label as the partition label, when the documents in the recovered partition are checked; It is understood that there are documents named test\_file\_B.docx, test\_file\_B.rar and test\_file\_B.xlsx in VOLUME\_B. (See Figure 6)

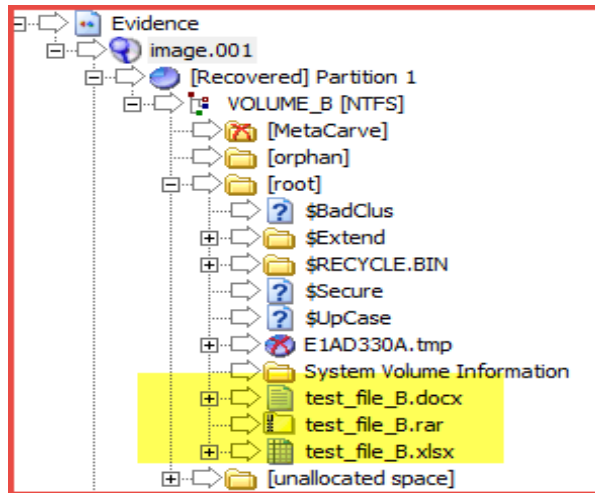


Figure 6 Documents labeled with the section name in the Recovered Section.

When analyzing the Extended Partition on the disk, it is seen that the deleted extended partition cannot be recovered. Since the forensic tools also perform sector-based data recovery operations, the data in these areas should be analyzed since the Unpartitioned Space may have recovered existing files on the area.

File List		
✓	Name	Path
<input type="checkbox"/>	Carved [33214464].zip	image.001/Unpartitioned Space [basic disk]/[unallocated space]/199940096*Carved [33214464].zip
<input type="checkbox"/>	Carved [33206272].zip	image.001/Unpartitioned Space [basic disk]/[unallocated space]/199940096*Carved [33206272].zip
<input type="checkbox"/>	Carved [33198080].zip	image.001/Unpartitioned Space [basic disk]/[unallocated space]/199940096*Carved [33198080].zip
<input type="checkbox"/>	Carved [33067008].zip	image.001/Unpartitioned Space [basic disk]/[unallocated space]/199940096*Carved [33067008].zip

Figure 7 Source information of recovered documents on Unpartitioned Space.

It can be seen in Fig. 8 that the names of the documents are Carved, and the extensions do not match their categories when the data on Unpartitioned Space is examined. If we need detailed information on the data obtained as carved, metadata records should be checked.

File List							
✓	Name	Category	Accessed	Modified	Created	P-Size	L-Size
<input type="checkbox"/>	Carved [33214464].zip	Excel 2016	n/a	n/a	n/a	n/a	8192 B
<input type="checkbox"/>	Carved [33206272].zip	Excel 2016	n/a	n/a	n/a	n/a	6604 B
<input type="checkbox"/>	Carved [33198080].zip	Excel 2016	n/a	n/a	n/a	n/a	6178 B
<input type="checkbox"/>	Carved [33067008].zip	Microsoft Word 2016 XML	n/a	n/a	n/a	n/a	11,41 KB

Figure 8 Metadata information of recovered documents on Unpartitioned Space.

In search of date information of the documents, it is shown in Figure 8 that these data cannot be recovered. When the processes in the scenario were examined, it was understood that the FTK forensic tool detected MBR partitioned primary partition (Volume\_B) but did not show the partition information about the extended Partition, Volume\_E. Also, information such as file type, name, and time information of the documents in Volume\_E obtained by data scraping could not be reached.

#### 4.3.2. Analysis using Encase software

Sections of the test disk obtained using Encase software are shown in Figure 9.

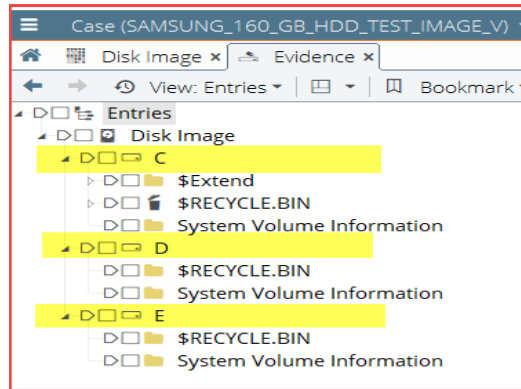


Figure 9 Section structures obtained with Encase

It is understood from Table 3 that there are *three* partition structures belonging to the test disk, and the total size of the partitions is 22.1 GB + 24.4 GB + 19.5 GB = 66 GB.

Table 3 Partition information obtained using Encase of the test disk

ID	Type	Start Sector	Total Sectors	Size
07	NTFS	2.048	46.336.000	22.1 GB
0c	FAT32X	107.778.048	51.200.000	24.4 GB
0c	FAT32X	158.980.033	40.960.000	19.5 GB

When the partition information of the test disk obtained with Encase is examined in Table 3; The total size of the *three* partitions detected was calculated as 66 GB. It is understood from Table 1 that the total disk size is 149.1 GB. When the total size of the available partitions and the total size of the test disk are compared, it is seen that Physical Disk Size is  $\neq$  Partitions Size. In this case, it is understood that the sections should be examined manually using the start and end sectors.

MBR records are kept in sector 0 in the partitions configured with MBR, and "sectors between 0-2047" are reserved as MBR area. For this reason, the 1st partition starts in the 2048 th sector, and the department signature information is at the end of this sector. The sum of the first partition start sector and the total number of sectors will give us the start part of the *two* partitions. As a result of the calculation, it is seen that it is  $2048 + 46.336.000 = 46.338.048$ , and it should be partition starting from 46.338.048 sector. However, when the partition table was examined, it was understood that there was no such partition. This situation shows us that there is a lost partition.

The Disk View feature of the encase forensic tool was used to see the 46338048 startup sector of the lost partition. It should be confirmed that the sector specified as a result of the addition is correct. 55AA signature value of the NTFS file system was seen in the last bytes of the sector in Figure 10.

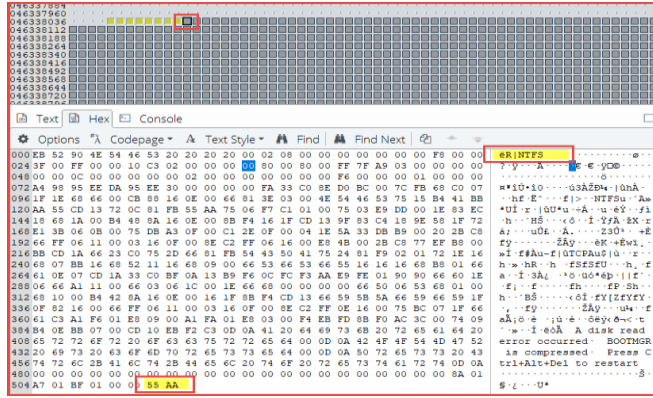


Figure 10 Signature of 55AA at the end of 46338048 sector and NTFS file system tag.

In the initial sector of 46338048 lost partitions, adding partition was performed. Thus, the contents of the lost partitions that were not visible at the beginning but as a result of calculations can be accessed.

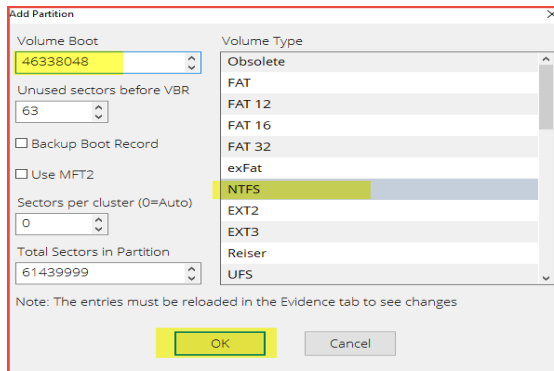


Figure 11 46338048 section information within the sector.

Manual addition is determined according to the starting sector determined in Figure 11. It is possible to access lost partition information after entering file type and start sectors.

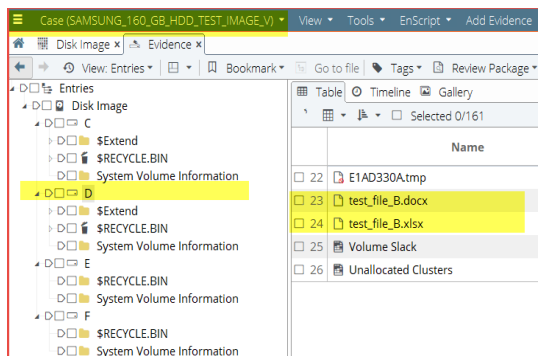


Figure 12 File structure of the disk partitions after adding the recovered primary partition of the test disk and the labeled documents in the partition

After performing the specified operations, the partition table view changed as in Table 4. However, the total number of sectors still does not match the number of sectors of the disk. Therefore, calculations are required.

Table 4 Partition table view after adding the recovered partition of the test disk

ID	Type	Start Sector	Total Sectors	Size
07	NTFS	2,048	46.336.000	22.1 GB

00	Recovered	46.337.985	61.440.062	29.3 GB
0c	FAT32X	107.778.048	51.200.000	24.4 GB
0c	FAT32X	158.980.033	40.960.000	19.5 GB

The partition table obtained after adding the lost partition is shown in Table 4. When the total size of the sections determined in this section table is calculated, 22.1 GB + 29.3 GB + 24.4 GB + 19.5 GB = 95.3 is obtained. When the total size of the available partitions and the total size of the test disk are compared, it is seen that Physical Disk Size is  $\neq$  Partitions Size. As a result of this calculation, it is concluded that there are other lost parts. According to the calculation, a new lost partition asset has emerged. This situation shows the existence of at least 5 sections. In this case, it is concluded that there is an extended partition on the test disk.

In the future operations, the lost part should be made considering that it is an extended part. After the existence of the lost partition was understood, the determination process of the starting sector of the lost partition was started. According to the section table in Table 4, it is expected that the 4th partition will give the 5th partition total of the start sector and the total sector. When the calculation related to the 4th partition is realized, it is understood that  $158.980.033 + 40.960.000 = 199.940.033$ . However, since the 4th and the lost partition are extended sections, the 63 sectors reserved for Volume Boot Record should be added to this total after 2048 sectors are added to this sector. As a result, the starting sector of the lost partition was calculated as  $2048 + 63 + 199.940.033 = 199.942.144$ .

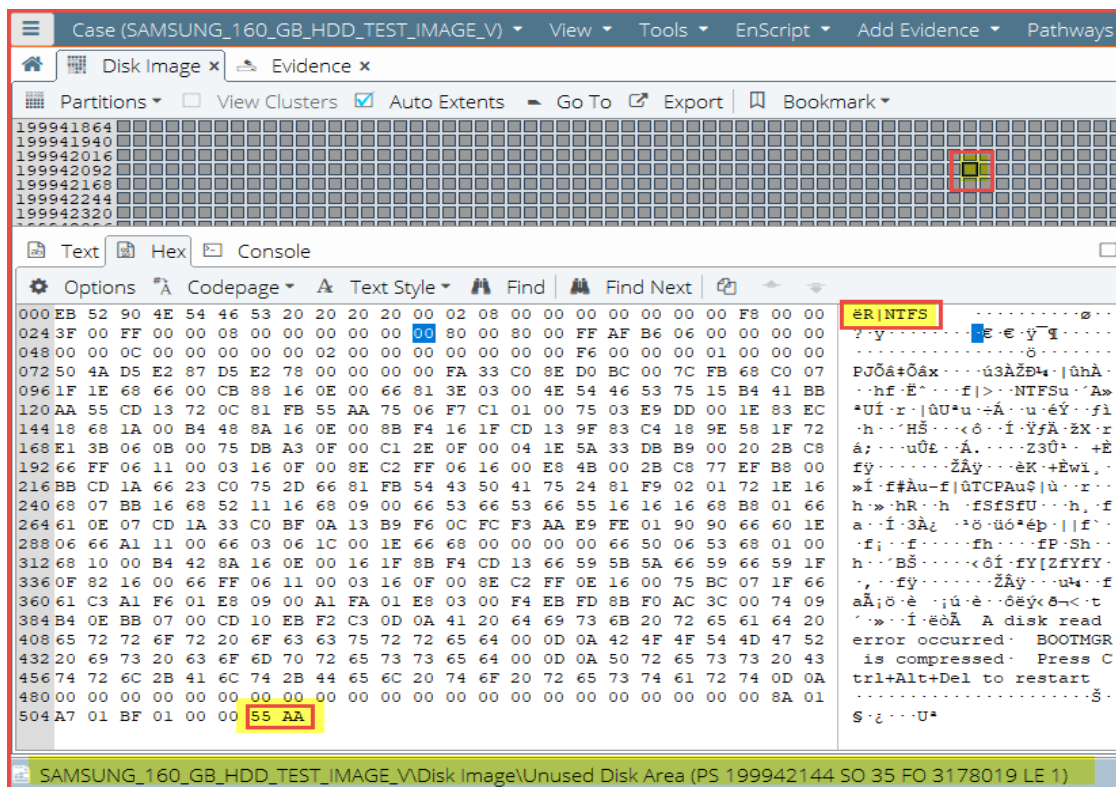


Figure 13 Section signature of 55AA at the end of 199942144 sector

Figure 13 shows the 55AA signature value of the NTFS file system in the last bytes of the sector. Thus, it is understood that there is one more section content. In the next stage, manual section addition was performed. The process for the addition is shown in Figure 14.

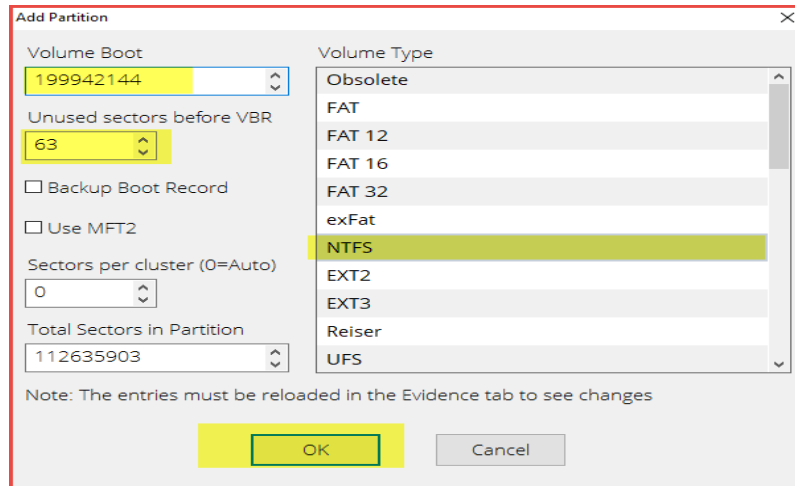


Figure 14 199942144 section information held within the sector.

After entering the file type and initial sectors, it is possible to access the lost partition information and its contents.

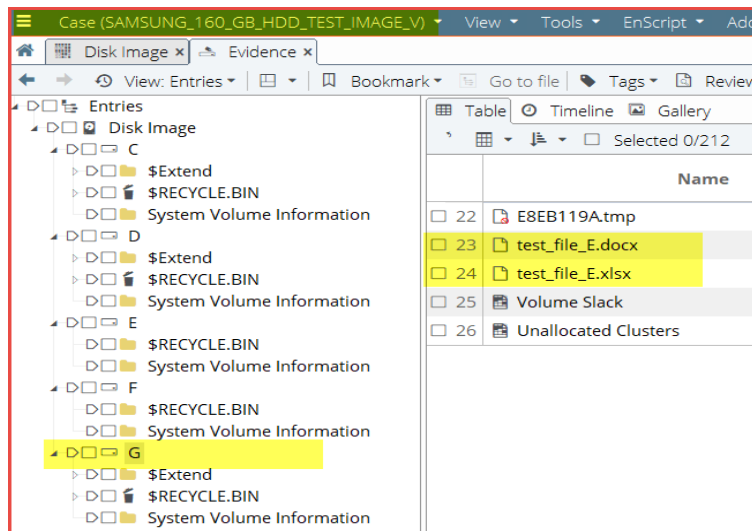


Figure 15 File structure of the disk partitions after the recovered extended partition of the test disk is added and the labeled documents in the partition.

After all manual additions were performed, all of the sections that were not visible at the beginning but deleted were accessed, and the lost partition information was reached. Table 5 shows the latest partition information.

Table 5. Partition table view after recovered partitions

ID	Type	Start Sector	Total Sectors	Size
07	NTFS	2.048	46.336.000	22.1 GB
00	Recovered	46.337.985	61.440.062	29.3 GB
0c	FAT32X	107.778.048	51.200.000	24.4 GB
0c	FAT32X	158.980.033	40.960.000	19.5 GB
00	Recovered	199.942.081	112.635.966	53.7 GB

As a result of the examination carried out with the Encase forensics tool, all the section structures were not shown directly to the user. However, encase allows the specialist to add a manual partition structure. Therefore, as a result of the size mismatch, the investigator should search the section signature

information. Then, it is necessary to add a manual section by looking at the section start sector and total size information. In this case, all section structures, location information, and metadata data could be accessed.

### 4.3.3. Analysis using Magnet AXIOM Examine software

Magnet AXIOM program is one of the programs widely used in forensics science. Figure 16 was obtained when the image file obtained from the test disk was opened with the magnet program.

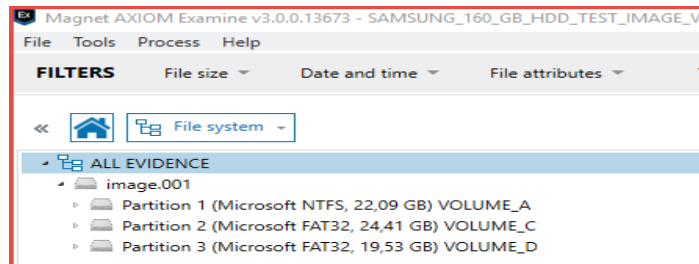


Figure 16 Section information detected by Magnet Axiom software

While the total disk size of the test disk should be 149.1 GB, the total size of the partitions detected by Magnet appears to be 22.09 GB + 24.41 GB + 19.53 GB = 66.03 GB.

As a result, since Physical Disk Size  $\neq$  Partitions Size, the existence of the lost partition structure is considered. Figure 13 shows that primary and secondary Partition structures are not recovered by the software. Since the forensics tools perform the sector-based rescue, document files belonging to the deleted sections are searched on the unpartitioned areas. As a result of the search, Word documents that were previously labeled with the VOLUME tag, whose name and path information could not be found, were identified and shown in Figure 17. The findings show that the data cannot be found in the correct location and content. For this reason, it is not possible to obtain content that may be evidence. This situation may affect the forensics process negatively.

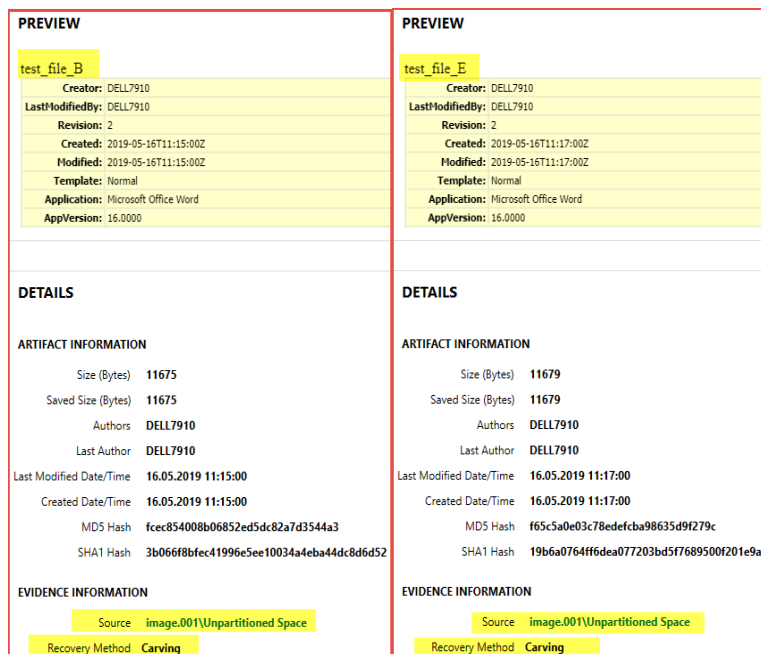


Figure 17 Metadata information of recovered documents on Unpartitioned Space.

Considering the findings obtained with Magnet Axiom, it was seen that no content related to primary and extended section information was available. The software does not offer the ability to add an

external partition. As a result of data carving, initial test data could be accessed with different names, but location information could not be accessed.

#### 4.3.4. Analysis using Autopsy 4.11.0 software

Autopsy program is an open-source licensed and widely used forensics tool that can perform many operations manually. The partition structures of the test disk were obtained with Autopsy as shown in Figure 18. In the figure, Vol3 corresponds to the Volume\_A that we initially configured, and Vol9 corresponds to the Volume\_E partitions. According to the section descriptions, the field type is marked as Unallocated. Although Volume\_B and Volume\_E were initially deleted, only the primary partition has been recovered, but the data in the secondary extended partition have not been accessed.

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-46338047)	2	2048	46336000	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 46338048-107778047)	3	46338048	61440000	Unallocated	Unallocated
vol4 (Win95 FAT32 (0x0c): 107778048-158978047)	4	107778048	51200000	Win95 FAT32 (0x0c)	Allocated
vol7 (Unallocated: 158978048-158980095)	7	158978048	2048	Unallocated	Unallocated
vol8 (Win95 FAT32 (0x0c): 158980096-199940095)	8	158980096	40960000	Win95 FAT32 (0x0c)	Allocated
vol9 (Unallocated: 199940096-312581807)	9	199940096	112641712	Unallocated	Unallocated

Figure 18 Partition information detected by the Autopsy 4.11.0 software of the test disc

It is shown in Figure 19 that there is one recovered partition among the sectors Vol3 (Unallocated: 46338048-107778047), existing metadata information of the documents is recovered, but location information cannot be recovered.

Name	Modified Time	Change Time	Access Time	Created Time	Location
test_file_B.xlsx	2019-05-16 14:15:23 EET	2019-05-16 14:15:24 EET	2019-05-16 14:15:23 EET	2019-05-16 14:15:15 EET	
test_file_B.rar	2019-05-16 14:15:28 EET	2019-05-16 14:15:31 EET	2019-05-16 14:15:28 EET	2019-05-16 14:15:28 EET	
test_file_B.docx	2019-05-16 14:15:08 EET	2019-05-16 14:15:09 EET	2019-05-16 14:15:08 EET	2019-05-16 14:14:53 EET	

Figure 19 Tagged documents in Vol 3 Unallocated section

It can be seen in Figure 19 that only primary partition structures are recovered by the software, but secondary partition structures are not recovered. Forensic tools perform the sector-based rescue. When searching the document files of the deleted sections on the non-partitioned areas, documents whose name and path information are not known and which were previously tagged by us with the VOLUME label were identified. However, it was not possible to reach the information in which position the documents are or by whom.

#### 4.3.5. Analysis using The Sleuth Kit (TSK) tools

TSK is open-source software that offers many libraries and command lines to the user to analyze disk images. TSK provides an analysis of the partition and file system data independent of the partition structure. When the test disk image was opened with the TSK tool mmls, the areas shown in Figure 20 were obtained.

```

root@kali:~/media/root/97EB-BDE2/SAMSUNG_160_GB_HDD_TEST_IMAGE_V# mmls image.001
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot  Start      End          Length      Description
000:  Meta      0000000000  0000000000  0000000001  Primary Table (#0)
001:  -----  0000000000  0000002047  0000002048  Unallocated
002:  000:000  0000002048  0046338047  0046336000  NTFS / exFAT (0x07)
003:  -----  0046338048  0107778047  0061440000  Unallocated
004:  000:001  0107778048  0158978047  0051200000  Win95 FAT32 (0x0c)
005:  Meta      0158978048  0312578047  0153600000  Win95 Extended (0x0f)
006:  Meta      0158978048  0158978048  0000000001  Extended Table (#1)
007:  -----  0158978048  0158980095  0000002048  Unallocated
008:  001:000  0158980096  0199940095  0040960000  Win95 FAT32 (0x0c)
009:  -----  0199940096  0312581807  0112641712  Unallocated
    
```

Figure 20 Partition information obtained using TSK tools

It should be considered that there is a lost partition in the unallocated area between sectors 46338048-107778047 shown in Figure 20. In addition, it is seen that there is an extended partition area among sectors 158978048-312578047 (Win95 Extended). However, it is understood that the extended partition identified is between the sectors 158980096-199940095. Thus, it is observed that there is one lost partition between sectors 199940096- 312581807. The information obtained with the fsstat command is given in Figure 21.

```

root@kali:~/media/root/97EB-BDE2/SAMSUNG_160_GB_HDD_TEST_IMAGE_V# fsstat -o 0046338048 image.001
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: 30EE95DAEE9598A4
OEM Name: NTFS
Volume Name: VOLUME_B
Version: Windows XP
    
```

Figure 21 2. partition partition information deleted by using test disk with TSK tools

When fls command is used to detect the files in the section, *three* documents are accessed, which are labeled with the section tag shown in Figure 22.

```

root@kali:~/media/root/97EB-BDE2/SAMSUNG_160_GB_HDD_TEST_IMAGE_V# fls -o 0046338048 image.001
r/r 4-128-1: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-4: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
r/r 2-128-1: $LogFile
r/r 0-128-0: $MFT
r/r 1-128-1: $MFTMirr
d/d 40-144-1: $RECYCLE.BIN
r/r 9-128-3: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 10-128-4: $UpCase:$Info
r/r 3-128-3: $Volume
d/d 36-144-1: System Volume Information
r/r 44-128-3: test file B.docx
r/r 39-128-1: test file B.rar
r/r 45-128-3: test file B.xlsx
-r/r * 43-128-3: E1AD330A.tmp
V/V 256: $OrphanFiles
    
```

Figure 22 File information in deleted partition 2 obtained using the test disk with TSK tools

Since the extended partition table is in sector 0158978048, the content of the Extended partition table is shown in Figure 23 using the mmls command. Here, it is clearly seen that 2048 sectors are reserved areas.

```

root@kali:~/media/root/97EB-BDE2/SAMSUNG_160_GB_HDD_TEST_IMAGE_V# mmls -o 0158978048 image.001
DOS Partition Table
Offset Sector: 158978048
Units are in 512-byte sectors

    Slot  Start      End          Length      Description
000:  Meta      0000000000  0000000000  0000000001  Primary Table (#0)
001:  -----  0000000000  0000002047  0000002048  Unallocated
002:  000:000  0000002048  0040962047  0040960000  Win95 FAT32 (0x0c)
003:  -----  0040962048  0312581807  0271619760  Unallocated
    
```

Figure 23 Extended Partition table information obtained by using Testdisk with TSK tools



It is understood that deleted extended partition started in 0199940096 sectors. Thus,  $2048 + 199940096 = 199942144$  will give the sector where the sector information is available. The `fsstat` command was used to get detailed information about the deleted extended partition and the information seen in Figure 24 was obtained. It has been accessed that the file format of the Partition is NTFS, and the partition name is `VOLUME_E`.

```
root@kali: /media/root/97EB-BDE2/SAMSUNG_160_GB_HDD_TEST_IMAGE_V# fsstat -o 0199942144 image.001
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: 78E2D587E2D54A50
OEM Name: NTFS
Volume Name: VOLUME_E
Version: Windows XP
```

Figure 24 Partition information of deleted extended partition obtained by using the test disk with TSK tools

The `fls` command was used to detect the files in the section, and *three* documents that we labeled with the section tag in Figure 25 were accessed.

```
root@kali: /media/root/97EB-BDE2/SAMSUNG_160_GB_HDD_TEST_IMAGE_V# fls -o 199942144 image.001
r/r 4-128-1: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-4: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
r/r 2-128-1: $LogFile
r/r 0-128-6: $MFT
r/r 1-128-1: $MFTMirr
d/d 39-144-1: $RECYCLE.BIN
r/r 9-128-8: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 10-128-4: $UpCase:$Info
r/r 3-128-3: $Volume
d/d 36-144-1: System Volume Information
r/r 43-128-3: test_file_E.docx
r/r 38-128-1: test_file_E.rar
r/r 44-128-3: test_file_E.xlsx
-/r * 42-128-3: E8EB119A.tmp
V/V 256: $OrphanFiles
```

Figure 25 File information in deleted extended partition obtained using TSK tools.

The tools in the TSK allow many operations related to a disk image to be performed manually. Therefore, the process using this tool can also be evaluated as a manual analysis. As a result of the analysis, it has been seen that by performing the calculations correctly, all the partitions and files on the disk can be accessed together with the location information. However, it is important to know the disk structure and partitioning structures in order to ensure the full and correct use of the TSK.

#### 4.3.6. Analysis using X-Ways Forensics tools

X-Ways Forensic analysis software is one of the most widely used forensics tools by digital forensics analysts. When the partition structures are checked by opening the image file obtained from the Test Disk with X-Ways Forensic Analysis software; There are five partition structures identified in Figure 26.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Partition 1	NTFS	22,1 GB					2.048
Partition 2	NTFS	29,3 GB					46.338.048
Partition 3	FAT32	24,4 GB					107.778.048
Partition 4	FAT32	19,5 GB					158.980.096
Partition 5	NTFS	53,7 GB					199.942.144

Figure 26 Section information detected by X-Ways software

It has been determined that partition 2 and partition 5 on the test disk image are primary and extended partition structures created and deleted in the scenario part. When the detected deleted partition

structures are checked, it is shown that the data in the partition structures are completely recovered and presented in Figure 27.

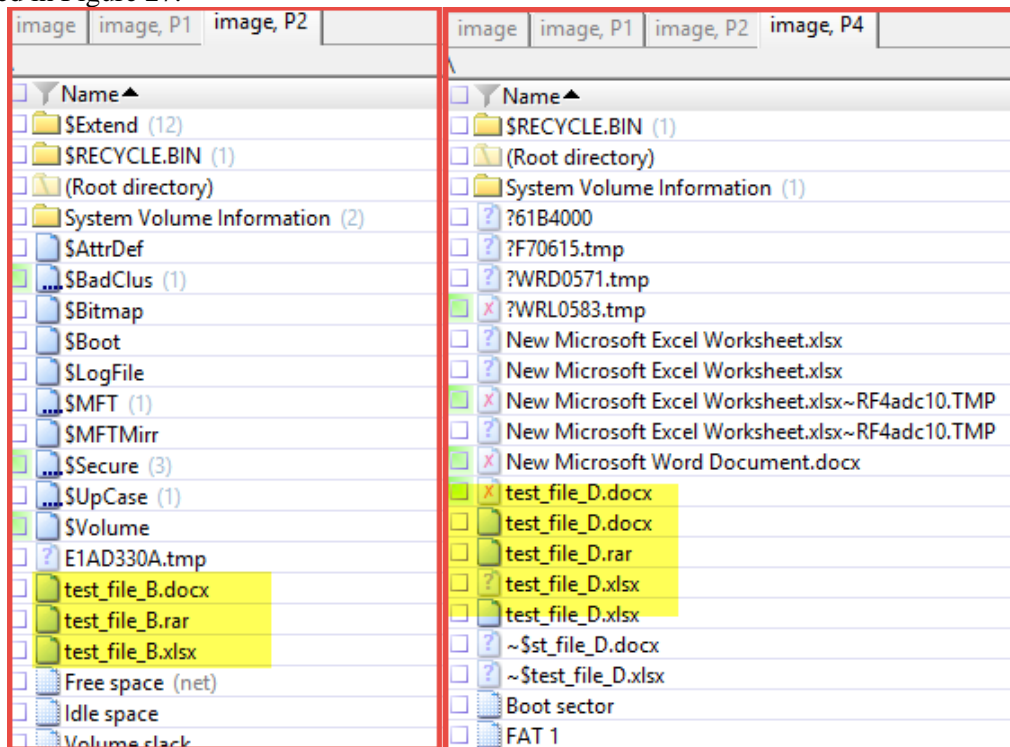


Figure 27 Data in deleted partitions.

When the test disk image was analyzed with X-Ways software, it was determined that deleted primary and extended partition structures were automatically detected and added by the software. In addition, it has been understood that the data in it was recovered without the need for any manual intervention.

#### 4.3.7. Discussion

[15] demonstrated methods of obtaining data from disks partitioned with GPT. Similarly, [33] there are studies on obtaining data from UEFI disks. However, there are no studies showing the methods of obtaining data from MBR disks. However, it is still possible to encounter MBR disks.

In this work, a MBR disk analysis methodology has been presented by using a scenario and the widely used forensics tools. According to the obtained findings, these points are highlighted.

Benefits;

- A new scenario is presented to analysis MBR partitioned disks.
- Six analyses methods have been presented and results of them have been given.
- A comprehensive benchmark for MBR forensics analysis have been presented.

Limitation;

- The results are depended on the presented scenario. More scenarios can be analyzed for obtaining comprehensively results.

#### 5. Conclusions

A sample scenario was prepared in the study. A hard disk image that is configured with MBR created in this scenario and deleted partition structures are used. Thus, the performance of 5 different forensics tools was tested on this disk image with this study. With this study, it was observed that some forensics tools could not recover the partition structures, while others could not recover the extended partition structures by recovering the primary partition structures. Some forensic tools were evaluated to allow manual examination of the section structures.

In this work, there is a primary deleted partition labeled VOLUME\_B and deleted Extended partition labeled VOLUME\_E. These sections only allow manual evaluation of TSK and Encase forensics tool section structures. Thus, the structure of the section and the documents in it have been recovered without any problems (Metadata, Location, etc.).

Magnet Axiom failed during partition recovery and was able to recover only document and metadata. The FTK can only recover deleted primary partitions. It was also able to recover documents without metadata data. In the analysis with Autopsy, similar results were obtained with the FTK forensics tool. X-Ways has the ability to automatically recover primary and extended partition structures. The findings obtained are given in Table 6.

Table 6. Comparison table of the findings obtained

	FTK	Encase	Magnet Axiom	Autopsy	TSK Tool	X-Ways
Partition 1 recovery	X	X	-	X	X	X
Partition 2 recovery	-	X	-	-	X	X
Extended partition recovery	-	X	-	-	X	X
Document recovery	X	X	X	X	X	X
Metadata information detection	X	X	X	X	X	X
Location information detection	-	X	-	-	X	X

The basic principles of digital forensic tools are the same. However, the analyst should not be content with the results obtained by the forensic tools and should manually intervene when necessary. For this reason, possible situations that may be caused by the complex structure of extended partitions were taken into account in the analysis of disks configured with MBR. In such a case, sample analysis was carried out by proposing an evaluation, and the results obtained from this analysis are presented in a comparison table. It should be confirmed that especially the initial size of the disk and the sum of sectors obtained from forensics software are the same. Otherwise, in the forensics investigation, the lost partitions will not be examined, and many contents that may be of evidence will not be available.

Our future directions are given as follows. This paper show advantages and disadvantages of the widely used digital forensics analyses tools. We are planning to propose a new successful MBR analyses tool for overcoming the disadvantages of the exist analyses analysis models.

Authors' Contributions: All authors contributed equally to the study.

Statement of Conflicts of Interest: There is no conflict of interest between the authors.

Statement of Research and Publication Ethics: The author declares that this study complies with Research and Publication Ethics.

## References

- [1] C. Altheide and H. Carvey, *Digital forensics with open source tools*. Elsevier, 2011.
- [2] B. Carrier, "Open source digital forensics tools: The legal argument," *stake*, 2002.
- [3] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," *digital investigation*, vol. 3, pp. 44-49, 2006.
- [4] G. Horsman, "Formalising investigative decision making in digital forensics: proposing the Digital Evidence Reporting and Decision Support (DERDS) framework," *Digital Investigation*, vol. 28, pp. 146-151, 2019.

- [5] T. Vidas, B. Kaplan, and M. Geiger, "OpenLV: Empowering investigators and first-responders in the digital forensics process," *Digital Investigation*, vol. 11, pp. S45-S53, 2014.
- [6] S. L. Garfinkel, "Digital forensics research: The next 10 years," *digital investigation*, vol. 7, pp. S64-S73, 2010.
- [7] Y. Guo, J. Slay, and J. Beckett, "Validation and verification of computer forensic software tools—Searching Function," *digital investigation*, vol. 6, pp. S12-S22, 2009.
- [8] A. C. Bogen and D. A. Dampier, "Unifying computer forensics modeling approaches: a software engineering perspective," in *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, 2005: IEEE, pp. 27-39.
- [9] M. Wundram, F. C. Freiling, and C. Moch, "Anti-forensics: the next step in digital forensics tool testing," in *2013 seventh international conference on it security incident management and it forensics*, 2013: IEEE, pp. 83-97.
- [10] G. C. Kessler, "Anti-forensics and the digital investigator," 2007.
- [11] A. Khan, U. K. Wiil, and N. Memon, "Digital forensics and crime investigation: Legal issues in prosecution at national level," in *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2010: IEEE, pp. 133-140.
- [12] R. W. Taylor, E. J. Fritsch, and J. Liederbach, *Digital crime and digital terrorism*. Prentice Hall Press, 2014.
- [13] M. Geiger, "Evaluating Commercial Counter-Forensic Tools," in *DFRWS*, 2005.
- [14] S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," in *2nd International Conference on i-Warfare and Security*, 2007, vol. 20087, pp. 77-84.
- [15] B. J. Nikkel, "Forensic analysis of GPT disks and GUID partition tables," *Digital Investigation*, vol. 6, no. 1-2, pp. 39-47, 2009.
- [16] Y. Liu, J. Fang, and C. Han, "A new R-tree node splitting algorithm using MBR partition policy," in *2009 17th International Conference on Geoinformatics*, 2009: IEEE, pp. 1-6.
- [17] G. Horsman, "Tool testing and reliability issues in the field of digital forensics," *Digital Investigation*, vol. 28, pp. 163-175, 2019.
- [18] S. Bommisetty, R. Tamma, and H. Mahalik, *Practical mobile forensics*. Packt Publishing Ltd, 2014.
- [19] H. Mahalik, R. Tamma, and S. Bommisetty, *Practical Mobile Forensics*. Packt Publishing Ltd, 2016.
- [20] M. Al Fahdi, N. L. Clarke, and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions," in *2013 Information Security for South Africa*, 2013: IEEE, pp. 1-8.
- [21] G. Horsman and D. Errickson, "When finding nothing may be evidence of something: Anti-forensics and digital tool marks," *Science & Justice*, vol. 59, no. 5, pp. 565-572, 2019.
- [22] K. Conlan, I. Baggili, and F. Breitingner, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," *Digital investigation*, vol. 18, pp. S66-S75, 2016.
- [23] T. Göbel and H. Baier, "Anti-forensics in ext4: On secrecy and usability of timestamp-based data hiding," *Digital Investigation*, vol. 24, pp. S111-S120, 2018.
- [24] T. Haruyama and H. Suzuki, "One-byte modification for breaking memory forensic analysis," *Black Hat Europe*, 2012.
- [25] A. Prakash, E. Venkataramani, H. Yin, and Z. Lin, "Manipulating semantic values in kernel data structures: Attack assessments and implications," in *2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2013: IEEE, pp. 1-12.
- [26] K. Lee, H. Hwang, K. Kim, and B. Noh, "Robust bootstrapping memory analysis against anti-forensics," *Digital Investigation*, vol. 18, pp. S23-S32, 2016.
- [27] S. Rekhis and N. Boudriga, "A system for formal digital forensic investigation aware of anti-forensic attacks," *IEEE transactions on information forensics and security*, vol. 7, no. 2, pp. 635-650, 2011.
- [28] A. Regenscheid, L. Feldman, and G. Witte, "NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization," National Institute of Standards and Technology, 2015.
- [29] D. Hurlbut-AccessData, "Fuzzy Hashing for Digital Forensic Investigators," 2009.

- [30] K. Hausknecht, D. Foit, and J. Burić, "RAM data significance in digital forensics," in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2015: IEEE, pp. 1372-1375.
- [31] E. Casey and G. J. Stellatos, "The impact of full disk encryption on digital forensics," *ACM SIGOPS Operating Systems Review*, vol. 42, no. 3, pp. 93-98, 2008.
- [32] B. Dolan-Gavitt, "Forensic analysis of the Windows registry in memory," *digital investigation*, vol. 5, pp. S26-S32, 2008.
- [33] D. Jeong and S. Lee, "Forensic signature for tracking storage devices: Analysis of UEFI firmware image, disk signature and windows artifacts," *Digital Investigation*, vol. 29, pp. 21-27, 2019.
- [34] M. Gruhn, "Forensic limbo: Towards subverting hard disk firmware bootkits," *Digital Investigation*, vol. 23, pp. 138-150, 2017.
- [35] F. Freiling, T. Glanzmann, and H. P. Reiser, "Characterizing loss of digital evidence due to abstraction layers," *Digital Investigation*, vol. 20, pp. S107-S115, 2017.
- [36] H. Kim, J. Kim, and T. Kwon, "A Study of Verification Methods for File Carving Tools by Scenario-Based Image Creation," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 29, no. 4, pp. 835-845, 2019.
- [37] T. Sammes and B. Jenkinson, *Forensic computing*. Springer, 2007.
- [38] B. Carrier, *File system forensic analysis*. Addison-Wesley Professional, 2005.
- [39] K. Sindhu and B. Meshram, "Digital forensics and cyber crime datamining," 2012.
- [40] B. Carrier, "Defining digital forensic examination and analysis tools using abstraction layers," *International Journal of digital evidence*, vol. 1, no. 4, pp. 1-12, 2003.
- [41] K. Eckstein and M. Jahnke, "Data Hiding in Journaling File Systems," in *DFRWS*, 2005.
- [42] F. Ahsan, M. I. Lali, I. Ahmad, A. Ishaq, and S. Mohsin, "Exploring the effect of directory depth on file access for FAT and NTFS file systems," *ISTASC*, vol. 8, pp. 130-135, 2008.
- [43] J. Davis, J. MacLean, and D. Dampier, "Methods of information hiding and detection in file systems," in *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2010: IEEE, pp. 66-69.
- [44] W. Hong-biao, "The Features and Applications of FAT and NTFS File Systems [J]," *Computer Knowledge and Technology (Academic Exchange)*, vol. 6, 2007.
- [45] P. Nabity and B. J. Landry, "Recovering deleted and wiped files: A digital forensic comparison of FAT32 and NTFS file systems using evidence eliminator," ed: SWDSI, 2013.
- [46] M. Trawicki, "File Systems," 2002.
- [47] J. M. Rodriguez and J. Duffany, "Computer Forensics Tutorial Disk File Systems (FAT16, FAT32, NTFS)," POLYTECHNIC UNIV OF PUERTO RICO SAN JUAN, 2012.
- [48] N. Zhang, Y. Jiang, and J. Wang, "The Research of Data Recovery on Windows File Systems," in *2020 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, 2020: IEEE, pp. 644-647.
- [49] S. G. Taskin and E. U. Kucuksille, "Recovering Data Using MFT Records in NTFS File System," *Academic Perspective Procedia*, vol. 1, no. 1, pp. 448-457, 2018.
- [50] K. L. Rusbarsky and K. City, "A forensic comparison of NTFS and FAT32 file systems," [http://www.marshall.edu/forensics/files/RusbarskyKelsey\\_Research-Paper-Summer-2012.pdf](http://www.marshall.edu/forensics/files/RusbarskyKelsey_Research-Paper-Summer-2012.pdf). *Fetched: July*, vol. 6, p. 2017, 2012.