Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 4, October 2024
DOI : https://doi.org/10.33395/sinkron.v8i4.14042

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Analysis Technique Data hiding using HPA DCO on SATA Hard Drive

Muhammad Reyfasha Ilhami [1)*] , Niken Dwi Cahyani [2)] , Erwid Musthofa Jadied [3)]
[1)2)] School of Computing, Telkom University, Indonesia
[1)]mreyfashailhami@student.telkomuniversity.ac.id, [2)]nikencahyani@telkomuniversity.ac.id,
[3)]jadied@telkomuniversity.ac.id

Submitted :Aug 19, 2024 | **Accepted** : Aug 22, 2024 | **Published** : Oct 7, 2024

Abstract: Data hiding techniques in the Host Protected Area (HPA) and Device Configuration Overlay (DCO) areas of SATA Hard Disk Drives have become a frequently used anti-forensic activity to hide data and evidence. The area is inaccessible to standard operating systems and software, making it capable of hiding data. This technique utilizes the ability of the SATA Hard Disk Drive to reconfigure the storage size so as to hide evidence. When anti-forensic data hiding Host Protected Area (HPA) and Device Configuration Overlay (DCO) activities occur, it is necessary to conduct a digital forensic investigation to find clues that are useful in solving crimes. Therefore, in this research, an assessment of data hiding techniques using Host Protected Area (HPA) and Device Configuration Overlay (DCO) on SATA Hard Disk Drives is carried out. The implementation of the HPA DCO data hiding technique on a SATA Hard Disk Drive by identifying the HPA DCO area on the SATA HDD and investigating the acquisition results on the SATA HDD is the subject of this research. It is expected that the results will provide a comprehensive overview of HPA DCO data hiding techniques on a SATA HDD as well as recommendations on how to identify and investigate SATA HDDs that have HPA DCO. This effort aims to evaluate the HPA DCO data hiding technique in various cases and provide insight into the potential use of this technique in hiding data or evidence.

Keywords: Anti-Forensics, DCO, Data Hiding, HPA, SATA HDD

INTRODUCTION

In today's digital era, data plays an important role in criminal investigations by using effective tools to conduct examinations aimed at finding evidence. In broader forensic science, some tools are used to commit crimes for profit and to eliminate traces by conducting anti-forensic activities. Data containing this information can be manipulated, hidden, and even removed to hinder investigators' investigations. Maintaining information security is a major challenge of today's technological developments. Anti-forensic operations are one of the attacks that need to be watched out for (Anderson & McGrew, 2017).

Digital forensics plays an important role in the anti-forensic investigation process. It involves disciplines such as evidence collection, analysis of investigation results, and maintaining data integrity to become intact evidence. However, with the development of anti-forensic techniques, forensic investigators will face more complicated challenges (Li et al., 2011). An example of an anti-forensic technique that complicates investigations by forensic experts is the data hiding technique. Data hiding is one of the frequently used anti-forensic techniques. This technique includes methods such as file hiding, steganography, and watermarking with the aim of hiding the actual existence of the data. Data hidden using these methods often escape and cannot be detected(Sahu & Sahu, 2020). However, there are concealment techniques that involve hardware by using Host Protected Area (HPA) and Device Configuration Overlay (DCO) areas.

The Host Protected Area (HPA) was first introduced in the ATA-4 series, where this area can be used to hide information so that it cannot be modified, changed, or accessed easily by users through the BIOS or OS. The Device Configuration Overlay (DCO) is an area that can hide evidence. DCO allows some of the storage capacity to be hidden from the operating system or forensic tools. This area can be accessed only with special forensic tools, so the data hidden in this area is almost impossible to find (Gupta et al., 2006). Several Computer Forensic Tools (CFTs) can assist in the investigation process, which have facilitated the growth of digital forensics with the ability to identify anti-forensic attacks. Digital forensic investigations can be considered inconclusive if there are doubts about the credibility of the forensic tools used. Because digital evidence that will be submitted to the court from the CFT results can be misleading if the tools used are not credible (Bhat et al., 2021).

*name of corresponding author

Based on the problems above, this research will implement the HPA DCO data hiding technique on a SATA Hard Disk Drive and analyze it using computer forensic tools. By doing this research, it aims to find out whether SATA Hard Disk Drives that have HPA and DCO can be successfully identified and investigated using open-source forensic tools. The Focus of this research is to investigate a SATA hard disk drive that is indicated to have HPA DCO area by identifying the existence of HPA DCO and can recover data hidden in HPA DCO area directly and focusing on the analysis of data hiding techniques that utilize HPA and DCO, as well as the evaluation of tools and methods used in the forensic process to overcome these challenges. This research will also explore the implications of the use of HPA and DCO on data integrity and the validity of forensic investigation results, with the aim of developing a more effective and accurate approach to detecting and recovering hidden data on SATA hard disks.

LITERATURE REVIEW

In this chapter, we will discuss the literature used in this research. Some of them are Anti-Forensics, Data Hiding HPA DCO, Host Protected Area (HPA), Device Configuration Overlay (DCO), and Acquisition Disk (Imaging).

Anti-forensic

Anti-forensic technology is designed to hide or tamper with computer evidence, rendering it ineffective in legal proceedings that already spend a lot of time and resources investigating it (Abdullahi, 2023)**.** As cybercrime increases and software can be used to compromise the forensic investigation process, practitioners need to be able to identify the same anti-forensic activity that others have experienced in the past (Conlan et al., 2016). Currently, there is no universal definition established for anti-forensic science. Several definitions are available, and each has a different explanation, and some see anti-forensics as the science of tampering with tools or avoiding detection of forensic tools (Harris, 2006). Anti-forensic techniques have a high value in terms of security and priority. However, it is still a largely understudied field of forensic science. One technique that is effectively used and attracts the attention of forensic experts is steganography and data encryption (Chand Bansal et al., 2021). According to Marcus Rogers, the definition of anti-forensics is “An attempt to negatively affect the presence, quantity and/or quality of evidence from a crime scene, or to make the analysis and examination of evidence difficult or impossible” (IDAP’17: International Artificial Intelligence and Data Processing Symposium: September 16-17, 2017). According to Garfinkel, “anti-forensics consists of tools and methods that develop with the aim of hindering the use of forensic tools, investigations, and expert forensic experts” (Garfinkel, 2007). From the above statement, it can be concluded that anti-forensics is a crime with the aim of complicating the investigation and analysis process carried out by forensic experts for their own interests. Referring to (Kretowicz et al., 2016), anti-forensic activities can be categorized as follows:

- Forgery, concealment, obfuscation, and encryption of data,
- Deletion or destruction of data,
- Prevention of Analysis,
- Obstruction of evidence collection,
- Tools of subversion.

Data Hiding HPA DCO

One of the main anti-forensic techniques commonly used is data hiding. The main purpose of this technology is to hide or tamper with digital evidence so that it cannot be used in legal proceedings or is too expensive or inconvenient to recover or investigate (Abdullahi, 2023). Nowadays, hard disk drives are equipped with a backup space called Host Protected Area (HPA) and Device Configuration Overlay (DCO) (Leng & Li, 2018). According to Douglas et al. in an article entitled “An overview of steganography techniques applied to the protection of biometric data”, this technique is used to hide information in digital media so that it cannot be detected without using specialized forensic tools (Douglas et al., 2018). This technique has the aim of increasing the security of information without reducing data quality (Verma et al., 2019). According to Antti and Pekka Kinnunen, in an article entitled “What are HPAs and DCOs and why do they matter” explains that the hidden part of a Hard Drive known as HPA is invisible to the computer operating system. HPAs are designed to capture information that is difficult for users to find or modify. On the other hand, DCOs are used by computer system vendors to make the Hard Drive size different from its original capacity (Blancco, 2017). Nonetheless, HPAs and DCOs are not accessible (Gruhn, 2017). There is software that can be used to change the HPA and DCO areas, such as hdparm (Linux) and ATATool (Windows) (Chand Bansal et al., 2021). It can be concluded that HPA DCO data hiding is a technique for hiding data or evidence containing information by utilizing hidden areas on the Hard Drive so that it is not easily detected by the computer operating system or forensic tools.

*name of corresponding author

Host Protected Area (HPA)

A hidden partition on the Hard Drive that can be used to hide data so that it cannot be detected by the operating system. After the development of the ATA-5 protocol, the Hard Disk Drive will introduce HPA by using the ATA command to create an area that protects the end of the Hard Disk Drive to hide data so that the operating system or BIOS cannot read the area. Some forensic software cannot easily get the data hidden in the area (Leng & Li, 2018). This area is usually used to hide Hard Disk utilities, configuration files, and diagnostic tools.

Device Configuration Overlay (DCO)

A hidden partition on the Hard Drive can be used to hide data so that it cannot be detected by the operating system. After the development of the ATA-5 protocol, the Hard Disk Drive will introduce HPA by using the ATA command to create an area that protects the end of the Hard Disk Drive to hide data so that the operating system or BIOS cannot read the area. Some forensic software cannot easily get the data hidden in the area. This area is usually used to hide Hard Disk utilities, configuration files, and diagnostic tools. Although this area is not accessible, there are some forensic tools that can modify the HPA location to hide data (Wani et al., 2020).

Acquisition Disk (Imaging)

Data acquisition (imaging) in investigative activities in the forensic world is very important, where the results of the acquisition are the results of the disk as a whole and do not change the evidence on the hard disk. Usually, disk acquisition is done using FTK Imager in order to obtain the physical disk while maintaining its integrity. If a drive with hidden sectors is physically detected in the host protection area or device configuration overlay, the tool will not remove the HPA or DCO. FTK Imager does not detect any sectors hidden by HPA (DA-08-ATA28 and DA-08- ATA48) or DCO (DA-08-DCO) (Mukasey & Hagy, 2008).

METHOD

To achieve the objectives, the author designed a workflow to facilitate the research, which is structured as follows:

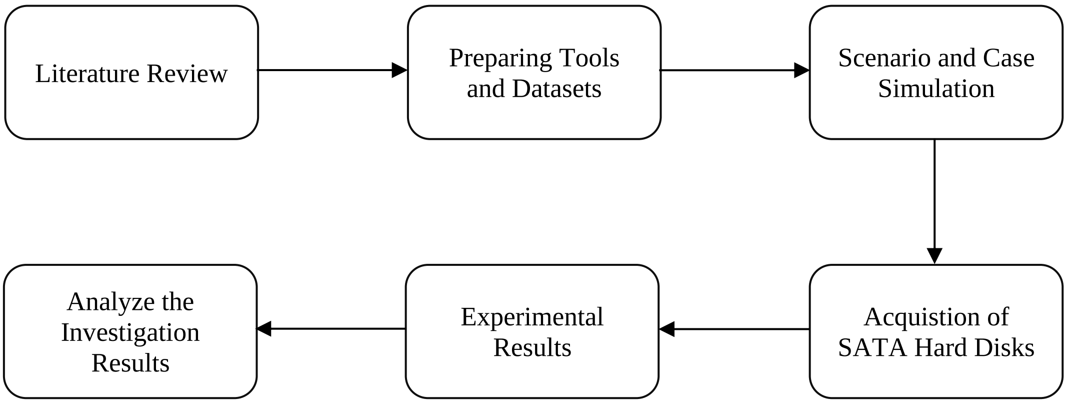

Literature Review
Preparing Tools and Datasets
Scenario and Case Simulation
Acquistion of SATA Hard Disks
Experimental Results
Analyze the Investigation Results

Fig. 1 Experimental Flow

A research plan structure called research methodology comprises plans and procedures for conducting research, including broad hypotheses, research strategies, techniques for research, and in-depth analysis (Ishtiaq, 2019). This research uses qualitative methods as a research strategy, by conducting a literature review of previous research2, implementing HPA DCO data hiding techniques, and conducting investigations in the form of identifying HPA DCO and files hidden in the area (Figure1). The result of this research is the success or failure of the HPA DCO area to be identified and see the files hidden in the HPA DCO area.

Preparing tools and datasets

The tools used in this research include a laptop, forensic tools, and two hard disk drive SATA. The laptop serves to implement data hiding techniques using forensic tools on SATA hard disk drives. The WDC WD16 hard disk drive serves to be the research object of the data hiding technique, the SKHynix SSD serves to store the acquisition results of the hard disk that is the object of research. Forensic tools serve to perform data hiding anti-forensics implementation and assist hard disk investigation of anti-forensics data hiding activities. All the tools and components mentioned above are integral to the research methodology used in this final project or thesis.

Thus, the selection and configuration of these tools are directed to ensure the validity and accuracy of the research results produced.

Table 1 Research Tools

No	Hardware / Software	Note
1	Hard Disk Drive (HDD) SATA WDC WD16 160GB	Research Object
2	Solid State Drive (SSD) SKHynix 512GB	Object to store the acquisition result
3	FTK Imager 4.7.1	Acquiring hard disks drive SATA
4	OSForensics 11.0	Identify the HPA/DCO area and be a replacement for the write blocker tool
5	WinHex 21.2	Identification of disk image results
6	Autopsy 4.20.1	Identification of disk image results
7	VM VirtualBox 7.0	Running Linux OS
8	ISO Kali Linux 4GB	Linux installation media for VirtualBox VMs
9	Hdparm 9.60	Linux software for implementation and identification of HPA DCO data hiding
10	‘dd’	Linux software to insert files into HPA DCO sectors

Table 2 Dataset

Data	Size	Hash File (MD5)
Skenario_Pembunuhan.docx	16275 bytes	e670174f5ada44e85074cc3637e722ba
Bukti_Percakapan.txt	2491 bytes	e2d98123d7df35cce12ee472f7997f72
Rincian_Pembayaran.xlsx	5704 bytes	ac784ed39a52988378c7d6943f422676
Informasi_Target.pdf	63871 bytes	4b23460efc843fcd65771e29c467aef9
Setelah_Eksekusi.jpg	9157 bytes	de464baaddbb766bf16011b356d540b0
Sebelum_Eksekusi.png	8134 bytes	fe434ca823e8dc5525e70ce6e7e4714b

Tables 1 and 2 are a tool that will be used to help this research, as for the data that will be hidden in the HPA DCO sector.

Scenario and Case Simulation

In the research Scenario and Case Simulation, an anti-forensic case of HPA DCO data hiding technique is performed on a WDC WD16 Hard Disk Drive SATA by hiding 3 data in the HPA area of 1GB and 3 data in the DCO area of 2GB. After that, an investigation will be conducted to identify the existence of HPA DCO and recover the hidden data. This test uses VirtualBox (7.0) VM software combined with Kali Linux ISO, Hdparm (9.60) and 'dd' (command line utility). Here is an overview of the HDD size and the presence of both HPA and DCO areas.

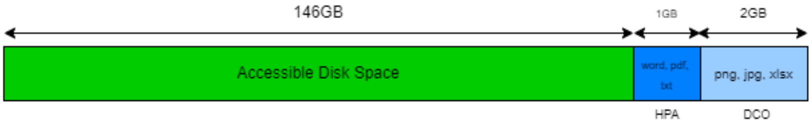


Fig. 2 Layout of the Disk

In figures 2, a research scenario is created on a 149GB hard disk that will be used to implement the HPA DCO data hiding technique on a SATA HDD with HPA of 1GB and DCO of 2GB. The HPA area is used to hide 3 files, consisting of “Skenario_Pembunuhan.docx”, “Informasi_Target.pdf”, and “Bukti_Percakapan.txt”. While

*name of corresponding author

the DCO area contains 3 files, consisting of “Sebelum_Eksekusi.png”, “Setelah_Eksekusi.jpg”, “Rincian Pembayaran.xlsx”.

Acquisition of SATA Hard Disks

Hard Disk Drive SATA acquisition will be performed on FTK Imager forensic tools. This step is used as a stage and guide for live forensic acquisition where acquisition is made when the hard disk drive SATA is still on. In this step, assisted by OSForensics tool as a write blocker to maintain the authenticity of the hard disk drive.

Experimental Results

Experimental results contain the results of the implementation of HPA DCO data hiding techniques and HPA DCO identification on the results of disk images and hard disks directly. In addition, whether the hidden evidence is successfully recovered or not.

Analyze the Investigation Results

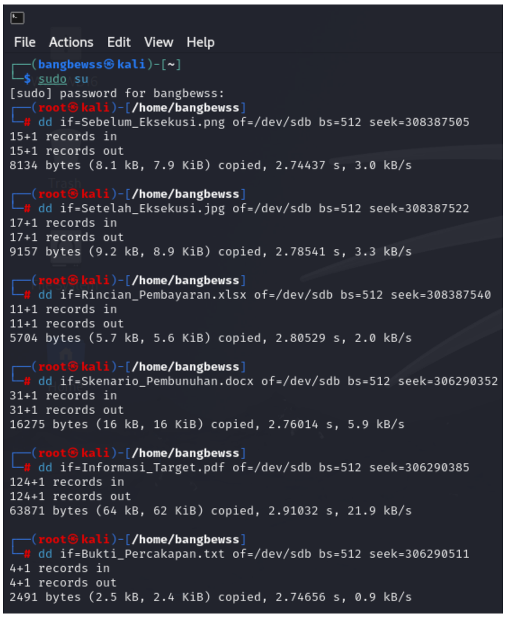
Analyzing the investigation is the final stage where the analysis process is carried out based on the knowledge gained previously and conclusions are drawn from the analysis results. The results of this will prove whether this research is complete or can still be developed in further research.

RESULT

The results of the analysis of HPA DCO data hiding techniques on SATA hard disk drives reveal that the results of the identification of the HPA DCO area using the results of disk images and directly from the SATA hard disk drive can identify the presence of HPA DCO. It can be seen from the reduction in the size of the disk offset when analyzed using the results of the disk image, while indicating the presence of HPA DCO by displaying the size of HPA DCO and providing information on the existence of the area. Can be seen in the Identification of HPA DCO presence section. Before carrying out identification, data will be hidden in the sector that will be hidden by HPA DCO which can be seen in the Hide files into the HPA DCO sector section. The results of the HPA DCO identification investigation using forensic tools can also be seen in table 3 Identification Results which explains to what extent the tools used can identify the HPA DCO area.

Hide files into the HPA DCO sector

Implementation of data hiding to the sector that will be the HPA DCO areas. Inserting files into the back sector of the hard disk. This is the first step to perform data hiding in the sector that will be used as HPA DCO, where it is expected from this activity to successfully insert files into the hard disk sector. To perform data hiding in this research, it is carried out using a Linux OS that is run by a VirtualBox VM. After that, inserting the file into the Linux OS storage on the VirtualBox VM so that the file can be hidden in the HPA DCO area. By using Linux software in the form of hdparm which will help to detect whether the HPA DCO area can be activated or not, then using the dd command utility available in Linux to insert 6 files that have been stored in the Linux OS libraries. How to enter it is with the command dd if=file_name of=/dev/sdx bs=x seek=sektor_disk. “file_name” is the name of the file that will be hidden into the HPA or DCO sector, ‘/dev/sdX’ is the hard disk that will be used as an object for the implementation of the HPA DCO data hiding technique. bs=x is ‘bit sectors’, where it depends on the bit sector of the hard disk that will be used, and ‘seek=disk_sector’ is the initial sector of the disk that will be used.



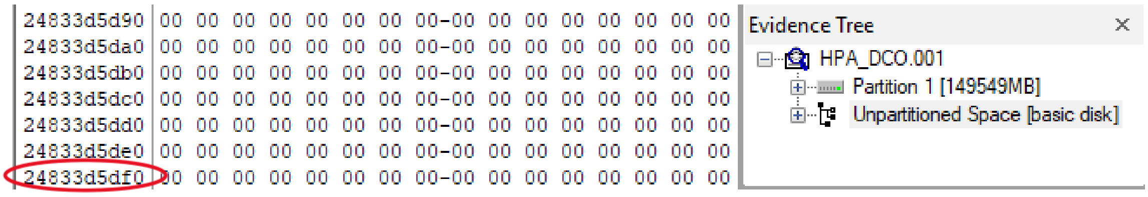
```
┌──(bangbewss㉿kali)-[~]
└─$ sudo su
[sudo] password for bangbewss:
┌──(root㉿kali)-[/home/bangbewss]
└─# dd if=Sebelum_Eksekusi.png of=/dev/sdb bs=512 seek=308387505
15+1 records in
15+1 records out
8134 bytes (8.1 kB, 7.9 KiB) copied, 2.74437 s, 3.0 kB/s

┌──(root㉿kali)-[/home/bangbewss]
└─# dd if=Setelah_Eksekusi.jpg of=/dev/sdb bs=512 seek=308387522
17+1 records in
17+1 records out
9157 bytes (9.2 kB, 8.9 KiB) copied, 2.78541 s, 3.3 kB/s

┌──(root㉿kali)-[/home/bangbewss]
└─# dd if=Rincian_Pembayaran.xlsx of=/dev/sdb bs=512 seek=308387540
11+1 records in
11+1 records out
5704 bytes (5.7 kB, 5.6 KiB) copied, 2.80529 s, 2.0 kB/s

┌──(root㉿kali)-[/home/bangbewss]
└─# dd if=Skenario_Pembunuhan.docx of=/dev/sdb bs=512 seek=306290352
31+1 records in
31+1 records out
16275 bytes (16 kB, 16 KiB) copied, 2.76014 s, 5.9 kB/s

┌──(root㉿kali)-[/home/bangbewss]
└─# dd if=Informasi_Target.pdf of=/dev/sdb bs=512 seek=306290385
124+1 records in
124+1 records out
63871 bytes (64 kB, 62 KiB) copied, 2.91032 s, 21.9 kB/s

┌──(root㉿kali)-[/home/bangbewss]
└─# dd if=Bukti_Percakapan.txt of=/dev/sdb bs=512 seek=306290511
4+1 records in
4+1 records out
2491 bytes (2.5 kB, 2.4 KiB) copied, 2.74656 s, 0.9 kB/s
```

Fig. 3 Hidden Files using ‘dd’

As shown in figure 3 the implementation of data hiding into the disk sector that will be used as the HPA DCO area has been carried out. This process is essential for hiding data using ‘dd’ in disk sectors.

Identification of HPA DCO presence

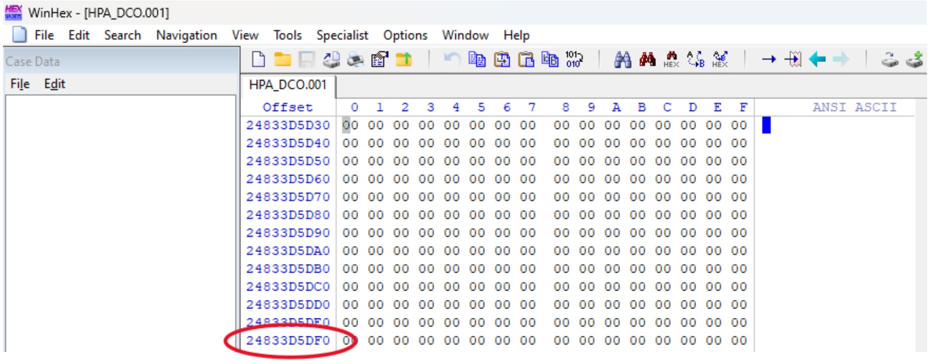
The examination using forensic tools focused on identifying the HPA DCO area and the files hidden within it by opening the disk image results and reading the hard disk directly.



```
24833d5d90  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
24833d5da0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
24833d5db0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
24833d5dc0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
24833d5dd0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
24833d5de0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
24833d5df0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

Fig. 4 FTK Imager Identification

As shown in figure 4 FTK Imager cannot identify the HPA DCO directly, but the final offset of the disk image is 24833d5df0 or about 146GB which means the disk size is reduced by 3GB. It is certain that there is an unreadable sector due to the presence of HPA DCO in the last sector.

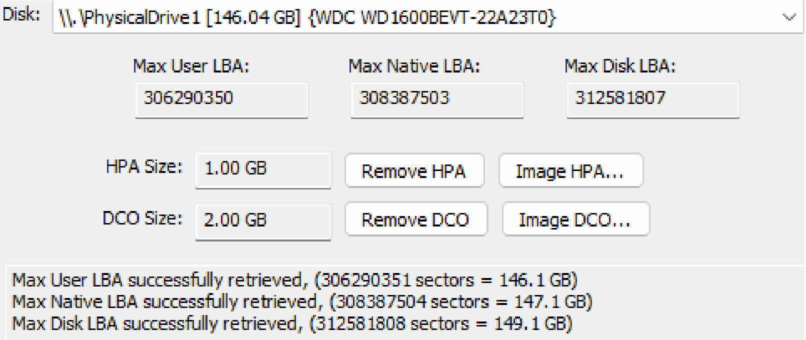

WinHex - [HPA_DCO.001]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
HPA_DCO.001

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
24833D5D30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5D40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5D50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5D60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5D70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5D80  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5D90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5DA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5DB0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5DC0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5DD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5DE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D5DF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Fig. 5 WinHex Identification

As shown in figure 5 Winhex also produces the same results as FTK Imager, where the final offset of the read disk is 24833d5df0 or about 146GB. Which means a reduction in disk size from the original.

*name of corresponding author


Disk: \\.\PhysicalDrive1 [146.04 GB] {WDC WD1600BEVT-22A23T0}

Max User LBA: 306290350
Max Native LBA: 308387503
Max Disk LBA: 312581807

HPA Size: 1.00 GB
DCO Size: 2.00 GB

Max User LBA successfully retrieved, (306290351 sectors = 146.1 GB)
Max Native LBA successfully retrieved, (308387504 sectors = 147.1 GB)
Max Disk LBA successfully retrieved, (312581808 sectors = 149.1 GB)

Fig 6 OSForensics Identification

As shown in figure 6 OSForensics can identify the HPA DCO by showing the size of the HPA as 1GB and the DCO as 2GB. It also states that the Max Disk LBA (actual disk) size is 312581807 sectors or 149GB. In the Max User LBA (usable disk) section, it is 306290350 sectors or 146GB. These results prove that the hard disk has an active HPA DCO. However, it is not possible to see the contents of the HPA DCO areas.

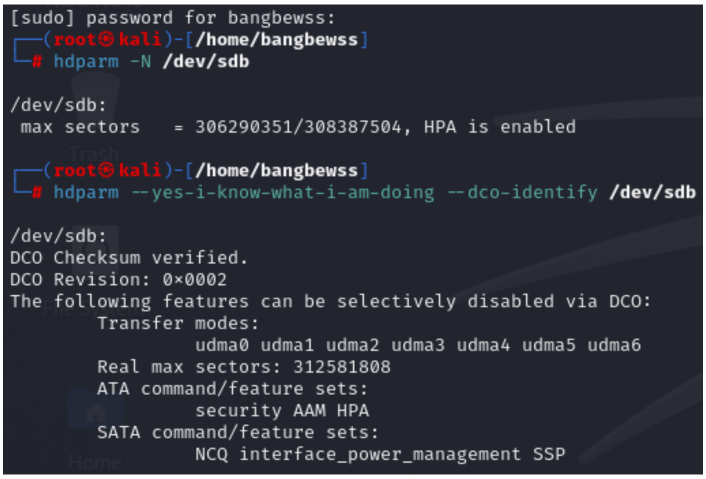
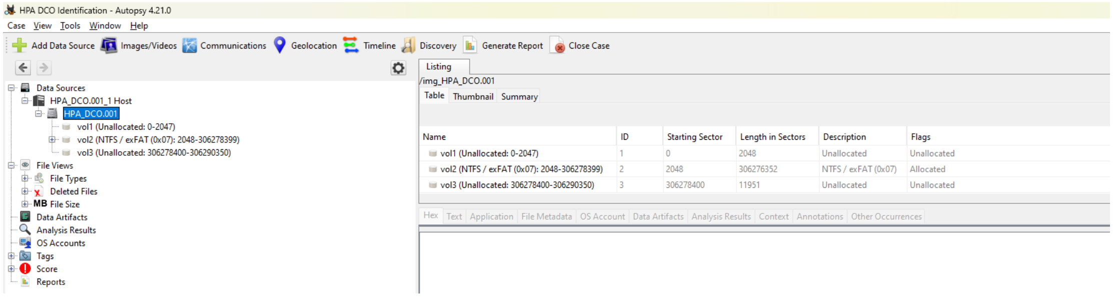

```
[sudo] password for bangbewss:
┌──(root㉿kali)-[/home/bangbewss]
└─# hdparm -N /dev/sdb

/dev/sdb:
 max sectors   = 306290351/308387504, HPA is enabled

┌──(root㉿kali)-[/home/bangbewss]
└─# hdparm --yes-i-know-what-i-am-doing --dco-identify /dev/sdb

/dev/sdb:
DCO Checksum verified.
DCO Revision: 0x0002
The following features can be selectively disabled via DCO:
        Transfer modes:
                 udma0 udma1 udma2 udma3 udma4 udma5 udma6
        Real max sectors: 312581808
        ATA command/feature sets:
                 security AAM HPA
        SATA command/feature sets:
                 NCQ interface_power_management SSP
```

Fig 7 Hdparm Identification

As shown in figure 7 Hdparm also provides information on the presence of HPA DCO on the hard disk, where the HPA area can be identified from the number of disk sectors that are read with the sectors that should be read. The DCO area is also verified by showing the 'real max sectors' of the hard disk which means there are sectors hidden due to the DCO.



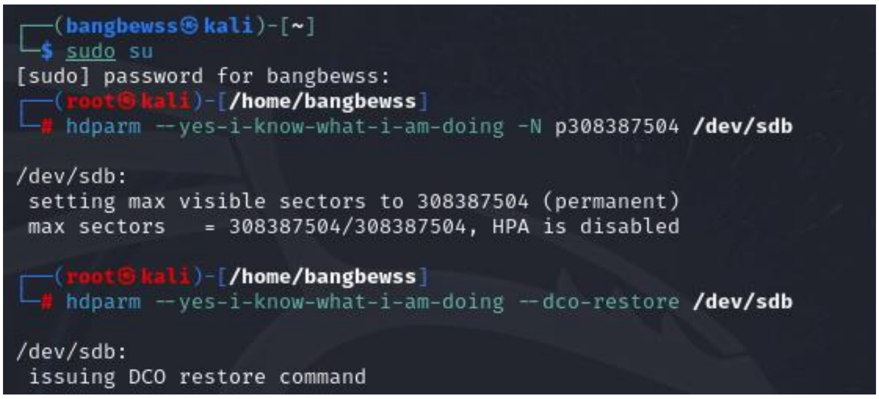
Data Sources
HPA_DCO.001_1 Host
HPA_DCO.001
vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-306278399)
vol3 (Unallocated: 306278400-306290350)
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports

/img_HPA_DCO.001

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-306278399)	2	2048	306276352	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 306278400-306290350)	3	306278400	11951	Unallocated	Unallocated

Fig 8 Autopsy Identification

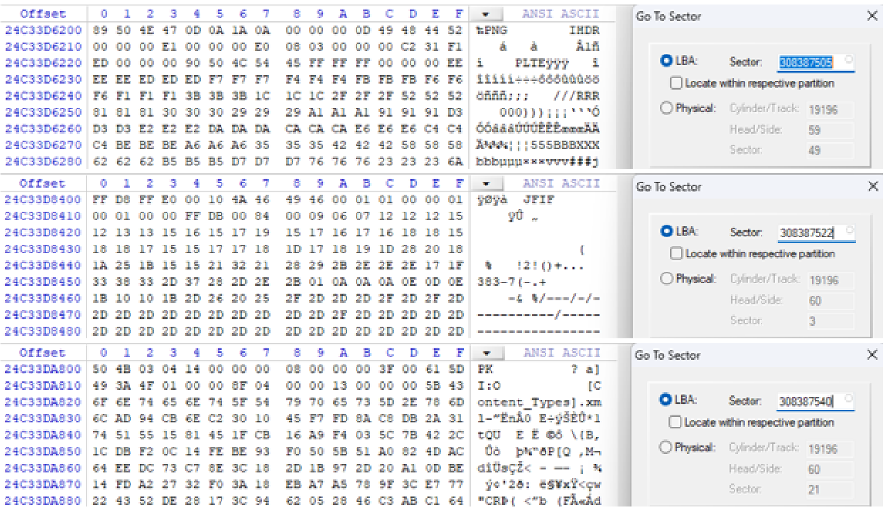
As shown in figure 8 Autopsy cannot identify the presence of HPA DCO, just like FTK Imager and Winhex which only read the offset and disk size changes due to the presence of HPA DCO.



```
┌──(bangbewss㉿kali)-[~]
└─$ sudo su
[sudo] password for bangbewss:
┌──(root㉿kali)-[/home/bangbewss]
└─# hdparm --yes-i-know-what-i-am-doing -N p308387504 /dev/sdb

/dev/sdb:
 setting max visible sectors to 308387504 (permanent)
 max sectors   = 308387504/308387504, HPA is disabled

┌──(root㉿kali)-[/home/bangbewss]
└─# hdparm --yes-i-know-what-i-am-doing --dco-restore /dev/sdb

/dev/sdb:
 issuing DCO restore command
```

Fig 9 Turn off HPA DCO

As shown in figure 9 disables the HPA DCO area to be able to view files hidden in sectors previously hidden by the HPA DCO. Using linux hdparm software to disable HPA DCO area because the tools used in this study do not allow direct analysis of the sectors concealed by the presence of HPA DCO. Consequently, turning off HPA DCO first allows for the reading and analysis of the previously hidden sectors, which is one method of examining the contents of the HPA DCO area.



```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
24C33D6200  89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52  ‰PNG        IHDR
24C33D6210  00 00 00 E1 00 00 00 E0  08 03 00 00 00 C2 31 F1     á   à     Å1ñ
24C33D6220  ED 00 00 00 90 50 4C 54  45 FF FF FF 00 00 00 EE  í   PLTEÿÿÿ   î
24C33D6230  EE EE ED ED ED F7 F7 F7  F4 F4 F4 FB FB FB F6 F6  îîííí÷÷÷ôôôûûûöö
24C33D6240  F6 F1 F1 F1 3B 3B 3B 1C  1C 1C 2F 2F 2F 52 52 52  öñññ;;;   ///RRR
24C33D6250  81 81 81 30 30 30 29 29  29 A1 A1 A1 91 91 91 D3     000)))¡¡¡'''Ó
24C33D6260  D3 D3 E2 E2 E2 DA DA DA  CA CA CA E6 E6 E6 C4 C4  ÓÓâââÚÚÚÊÊÊæææÄÄ
24C33D6270  C4 BE BE BE A6 A6 A6 35  35 35 42 42 42 58 58 58  Ä¾¾¾¦¦¦555BBBXXX
24C33D6280  62 62 62 B5 B5 B5 D7 D7  D7 76 76 76 23 23 23 6A  bbbµµµ×××vvv###j
```

Go To Sector
● LBA: Sector: 308387505
□ Locate within respective partition
○ Physical: Cylinder/Track: 19196 Head/Side: 59 Sector: 49

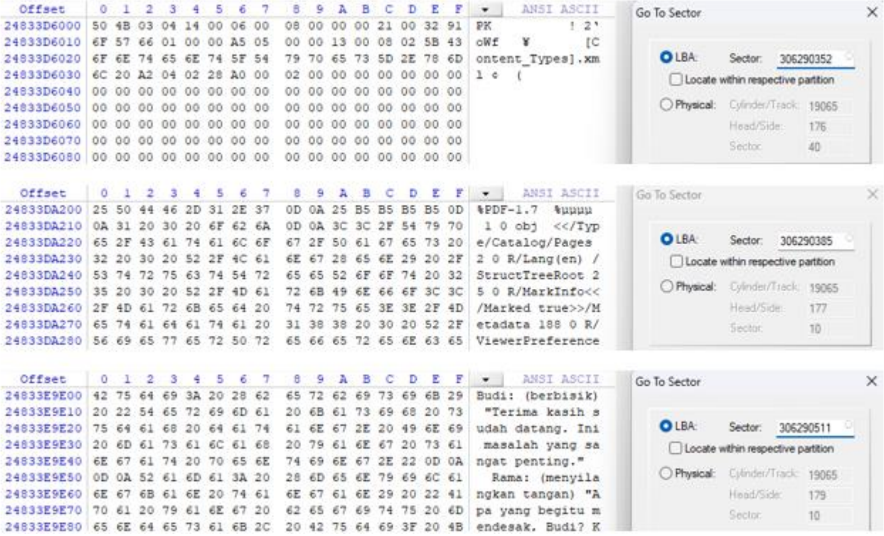
```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
24C33D8400  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 00 00 01  ÿØÿà  JFIF
24C33D8410  00 01 00 00 FF DB 00 84  00 09 06 07 12 12 12 15      ÿÛ „
24C33D8420  12 13 13 15 16 15 17 19  15 17 16 17 16 18 18 15
24C33D8430  18 18 17 15 15 17 17 18  1D 17 18 19 1D 28 20 18              (
24C33D8440  1A 25 1B 15 15 21 32 21  28 29 2B 2E 2E 2E 17 1F   %   !2!()+...
24C33D8450  33 38 33 2D 37 28 2D 2E  2B 01 0A 0A 0A 0E 0D 0E  383-7(-.+
24C33D8460  1B 10 10 1B 2D 26 20 25  2F 2D 2D 2D 2F 2D 2F 2D      -& %/---/-/-
24C33D8470  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2F 2D 2D 2D 2D 2D  ----------/-----
24C33D8480  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  ----------------
```

Go To Sector
● LBA: Sector: 308387522
□ Locate within respective partition
○ Physical: Cylinder/Track: 19196 Head/Side: 60 Sector: 3

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
24C33DA800  50 4B 03 04 14 00 00 00  08 00 00 00 3F 00 61 5D  PK          ? a]
24C33DA810  49 3A 4F 01 00 00 8F 04  00 00 13 00 00 00 5B 43  I:O           [C
24C33DA820  6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D  ontent_Types].xm
24C33DA830  6C AD 94 CB 6E C2 30 10  45 F7 FD 8A C8 DB 2A 31  l-"ËnÂ0 E÷ýŠÈÛ*1
24C33DA840  74 51 55 15 81 45 1F CB  16 A9 F4 03 5C 7B 42 2C  tQU  E Ë ©ô \{B,
24C33DA850  1C DB F2 0C 14 FE BE 93  F0 50 5B 51 A0 82 4D AC   Ûò  þ¾"ðP[Q ,M¬
24C33DA860  64 EE DC 73 C7 8E 3C 18  2D 1B 97 2D 20 A1 0D BE  dîÜsÇŽ< - — ¡ ¾
24C33DA870  14 FD A2 27 32 F0 3A 18  EB A7 A5 78 9F 3C E7 77   ý¢'2ð: ë§¥xŸ<çw
24C33DA880  22 43 52 DE 28 17 3C 94  62 05 28 46 C3 AB C1 64  "CRÞ( <"b (FÃ«Ád
```

Go To Sector
● LBA: Sector: 308387540
□ Locate within respective partition
○ Physical: Cylinder/Track: 19196 Head/Side: 60 Sector: 21

Fig 10 Files hidden in DCO sector



```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
24833D6000  50 4B 03 04 14 00 06 00  08 00 00 00 21 00 32 91  PK          ! 2'
24833D6010  6F 57 66 01 00 00 A5 05  00 00 13 00 08 02 5B 43  oWf    ¥      [C
24833D6020  6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D  ontent_Types].xm
24833D6030  6C 20 A2 04 02 28 A0 00  02 00 00 00 00 00 00 00  l ¢   (
24833D6040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D6050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D6060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D6070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
24833D6080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Go To Sector
● LBA: Sector: 306290352
□ Locate within respective partition
○ Physical: Cylinder/Track: 19065 Head/Side: 176 Sector: 40

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
24833DA200  25 50 44 46 2D 31 2E 37  0D 0A 25 B5 B5 B5 B5 0D  %PDF-1.7  %µµµµ
24833DA210  0A 31 20 30 20 6F 62 6A  0D 0A 3C 3C 2F 54 79 70   1 0 obj  <</Typ
24833DA220  65 2F 43 61 74 61 6C 6F  67 2F 50 61 67 65 73 20  e/Catalog/Pages
24833DA230  32 20 30 20 52 2F 4C 61  6E 67 28 65 6E 29 20 2F  2 0 R/Lang(en) /
24833DA240  53 74 72 75 63 74 54 72  65 65 52 6F 6F 74 20 32  StructTreeRoot 2
24833DA250  35 20 30 20 52 2F 4D 61  72 6B 49 6E 66 6F 3C 3C  5 0 R/MarkInfo<<
24833DA260  2F 4D 61 72 6B 65 64 20  74 72 75 65 3E 3E 2F 4D  /Marked true>>/M
24833DA270  65 74 61 64 61 74 61 20  31 38 38 20 30 20 52 2F  etadata 188 0 R/
24833DA280  56 69 65 77 65 72 50 72  65 66 65 72 65 6E 63 65  ViewerPreference
```

Go To Sector
● LBA: Sector: 306290385
□ Locate within respective partition
○ Physical: Cylinder/Track: 19065 Head/Side: 177 Sector: 10

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
24833E9E00  42 75 64 69 3A 20 28 62  65 72 62 69 73 69 6B 29  Budi: (berbisik)
24833E9E10  20 22 54 65 72 69 6D 61  20 6B 61 73 69 68 20 73   "Terima kasih s
24833E9E20  75 64 61 68 20 64 61 74  61 6E 67 2E 20 49 6E 69  udah datang. Ini
24833E9E30  20 6D 61 73 61 6C 61 68  20 79 61 6E 67 20 73 61   masalah yang sa
24833E9E40  6E 67 61 74 20 70 65 6E  74 69 6E 67 2E 22 0D 0A  ngat penting."
24833E9E50  0D 0A 52 61 6D 61 3A 20  28 6D 65 6E 79 69 6C 61    Rama: (menyila
24833E9E60  6E 67 6B 61 6E 20 74 61  6E 67 61 6E 29 20 22 41  ngkan tangan) "A
24833E9E70  70 61 20 79 61 6E 67 20  62 65 67 69 74 75 20 6D  pa yang begitu m
24833E9E80  65 6E 64 65 73 61 6B 2C  20 42 75 64 69 3F 20 4B  endesak, Budi? K
```

Go To Sector
● LBA: Sector: 306290511
□ Locate within respective partition
○ Physical: Cylinder/Track: 19065 Head/Side: 179 Sector: 10

Fig 11. Files hidden in HPA Sector

*name of corresponding author

As shown in figures 10 and 11 by using WinHex can see the existence of files that were previously hidden due to the HPA DCO area, can find 6 files hidden in the last disk sector which previously only read 146GB of offset. After HPA DCO was turned off, the contents of the previously unreadable sector could be seen.

Analyze the Investigation Results

Table 3 Identification results

Forensic Tools	Results
FTK Imager	The result is that it cannot directly identify the presence of HPA or DCO, but it can be seen when reading the disk image results that there is a reduction in disk size and the offset reads only up to 24833d5df0 or 146GB.
Autopsy	The result is that opening the resultant disk image containing HPA DCO does not successfully identify the presence of HPA DCO, only showing a reduction in disk size.
WinHex	The result is that it cannot directly identify the presence of HPA or DCO, but it can be seen when reading the disk image results that there is a reduction in disk size and the offset reads only up to 24833d5df0 or 146GB. However, when HPA DCO is turned off, it can see previously hidden sectors and find hidden files within them.
Hdparm	The result is to successfully identify the presence of HPA DCO by showing the number of sectors read, the number of sectors that should have been read, and the beginning of sectors from both HPA and DCO areas.
OSForensics	The result was to successfully identify the presence of HPA DCO and accurately indicate the size of HPA DCO. After that, it can identify the initial sector of the HPA DCO and the original disk sector.

DISCUSSIONS

In this research, the focus is on data-hiding techniques that utilize Host Protected Area (HPA) and Device Configuration Overlay (DCO) on SATA hard disks. HPA and DCO are methods used to hide data from operating systems and forensic tools by modifying the hard disk configuration. This research analyzes the extent to which the anti-forensic activities of the HPA DCO data-hiding technique can be implemented, identified, and analyzed.

These findings have significant implications for digital forensics practice. Researchers and forensic professionals should be aware that data hidden within HPAs and DCOs may not always be detectable with standard forensic tools. Therefore, a more comprehensive approach and more sophisticated techniques may be required to access and analyze hidden areas. For example, research conducted by Gruhn (2017), who try to identify the HPA DCO area, but it was very difficult to do because need the forensic tools. In addition, the results of this study have similarities with previous studies conducted by Gupta et al. (2005). Where the results are the HPA DCO area can be modified and identified using forensic tools. Linux utilities like dd and hdparm can identify and modify HPA DCO.

Recommendation for future research is needed to develop forensic tools capable of directly accessing and analyzing data in HPA and DCO without modifying the hard disk configuration. This research can also explore alternative techniques for identifying and accessing hidden data that may be more effective and less risky. This discussion is expected to provide deeper insights into the challenges and solutions related to HPA DCO data hiding techniques, as well as pave the way for better forensic tool research and development in the future.

CONCLUSION

This research aims to evaluate the anti-forensic data hiding activities of HPA DCO, focusing on identifying the HPA DCO area and recovering the data hidden within it. By utilizing tools such as FTK Imager, WinHex, Autopsy, OSForensics, Hdparm, etc. This research explores the extent to which HPA DCO anti-forensic data hiding activities can be successfully implemented, identified, and recovered. The experimental results show that although the HPA DCO is successfully identified, it cannot directly see the contents of the HPA DCO area, where the acquisition results of the hard disk that has HPA DCO cannot successfully lift the sector that is used as HPA DCO. This finding shows that this activity can be used to hide evidence that is difficult to identify. In this research, to see the hidden data, the HPA DCO area must be disabled and then the sector that initially appears can be seen and contains data that has been hidden and has not been successful in recovering the data residing in the HPA DCO sector.

REFERENCES

Abdullahi, Z. H. (2023). *An Overview of Anti-forensic Techniques and their Impact on Digital Forensic Analysis*. https://www.researchgate.net/publication/368365338

Anderson, B., & McGrew, D. (2017). Machine learning for encrypted malware traffic classification: Accounting for noisy labels and non-stationarity. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, *Part F129685*, 1723–1732. https://doi.org/10.1145/3097983.3098163

Bhat, W. A., AlZahrani, A., & Wani, M. A. (2021). Can computer forensic tools be trusted in digital investigations? *Science and Justice*, *61*(2), 198–203. https://doi.org/10.1016/j.scijus.2020.10.002

Chand Bansal, J., Kusum, ·, Nagar, A. K., Giri, K. J., Ahmad, S., Rumaan, P., Khan, B., & Editors, M. (2021). *Algorithms for Intelligent Systems Multimedia Security Algorithm Development, Analysis and Applications*. http://www.springer.com/series/16171

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *DFRWS 2016 USA - Proceedings of the 16th Annual USA Digital Forensics Research Conference*, S66–S75. https://doi.org/10.1016/j.diin.2016.04.006

Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications*, *77*(13), 17333–17373. https://doi.org/10.1007/s11042-017-5308-3

Garfinkel, S. L. (2007). *Anti-forensics: Techniques, detection and countermeasures*. https://www.researchgate.net/publication/228339244

Gruhn, M. (2017). Forensic limbo: Towards subverting hard disk firmware bootkits. *Digital Investigation*, *23*, 138–150. https://doi.org/10.1016/j.diin.2017.10.003

Gupta, M. R., Hoeschele, M. D., & Rogers, M. K. (2006). Hidden Disk Areas: HPA and DCO. In *International Journal of Digital Evidence Fall* (Vol. 5, Issue 1). www.ijde.org

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, *3*(SUPPL.), 44–49. https://doi.org/10.1016/j.diin.2006.06.005

IDAP'17 : International Artificial Intelligence and Data Processing Symposium : September 16-17. (2017). IEEE.

Ishtiaq, M. (2019). Book Review Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.). Thousand Oaks, CA: Sage. *English Language Teaching*, *12*(5), 40. https://doi.org/10.5539/elt.v12n5p40

Kretowicz, J., Sienicka, M., Strzelec, M., & Ziemianowicz, M. (2016). *Editor-in-Chief*. www.eforensicsmag.com

Leng, J., & Li, T. (2018). *Research on Computer System Information Hiding Anti-Forensic Technology*.

Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A Survey on Image Steganography and Steganalysis. In *Journal of Information Hiding and Multimedia Signal Processing c* (Vol. 2, Issue 2).

Mukasey, M. B., & Hagy, D. W. (2008). *Test Results for Digital Data Acquisition Tool: FTK Imager 2.5.3.14*. www.ojp.usdoj.gov/nijwww.ojp.usdoj.gov

Sahu, A. K., & Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. In *Open Computer Science* (Vol. 10, Issue 1, pp. 296–342). Walter de Gruyter GmbH. https://doi.org/10.1515/comp-2020-0136

Verma, S., Kapoor, V., & Maheshwari, R. (2019). An Enhanced Cryptographic System for Fast and Efficient Data Transmission. *Advances in Intelligent Systems and Computing*, *870*, 287–297. https://doi.org/10.1007/978-981-13-2673-8_31

Wani, M. A., Bhat, W. A., & Alzahrani, A. (2020). *File system anti-forensics-types, techniques and tools*.