Digital Forensics Tool Evaluation on Deleted Files

Miloš Stanković(✉) and Tahir M. Khan

Purdue University, West Lafayette 47906, USA
{mstankovic,tmkhan}@purdue.edu

Abstract. In a world where data is deleted every millisecond, whether on purpose or unintentionally, the question is whether deleted digital files still exist or if they are simply invisible to us on digital devices. Over the years, researchers have answered the question, but the rapid development of technologies and software makes the topic relevant. The global pandemic (coronavirus disease 2019) affected the physical and cyber worlds. Cyber attacks and data breaches have increased by over 400%. During these attacks, data is frequently deleted, mismanaged, or overwritten, making it difficult for users and digital investigators to recover and trace. Commercial tools that analyze deleted files are often expensive, and the unknown factor of free tools has always been a concern. In this paper, we evaluated two digital forensics tools, Magnet AXIOM, a commercial tool, and Autopsy, a free digital forensics tool, to partially bridge the gap for this era. We also used a differential analysis approach to investigate the persistence of deleted files. Moreover, for the best evaluation of the tools, we created files of various types and activities that mimic the daily usage of an average user on a Windows 11 operating system. The activities are divided into phases based on the processes that will most likely overwrite the deleted files. We also discussed the findings of these phases and presented the recommendations and challenges faced during the research process.

Keywords: Computer Forensics · Digital Forensics · Magnet AXIOM Suite · Autopsy · Microsoft Windows 11 · Deleted Files

1 Introduction

Digital crimes have been on the rise for years and certainly, the last two of the global pandemic created further complications. According to [1] article, CrowdStrike, a cybersecurity company, reported a 400% increase in threats during 2019 and 2020, with four out of five coming from cybercriminals in 2020 alone. Forbes [2], noted how the year 2020 had surpassed all records regarding data breaches. On average, researchers, [3] recognized a cost increase of a data breach by $0.77 million in the last few years. Moreover, on average, a data breach costs an organization around $3.29 million [3]. Industry specialists [4] estimate the cost of downtime per minute for a small company, medium company, and large

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 61–83, 2023.
https://doi.org/10.1007/978-3-031-36574-4_4

company is $8,000, $74,000, and $11,600, respectively. Losing valuable time and data is not only costly but time-consuming as well. On average, it is shown, ransomware causes 16.2 days of downtime [4]. Fast and guided recovery from a cyber incident is paramount.

Besides understanding the nature of the threats and the systems they affect, it is crucial to understand the capabilities of the data recovery tools used to mitigate cyber incidents. Rapid technology development forced companies to adapt and diversify in order to keep up with the ever-growing market. The need for digital forensics recovery tools led companies to develop their proprietary products. The products have been costly, forcing software developers to create alternative solutions. Often these products have different results when tested against the same situation. The question, which one is better and is there a difference, looms within the digital forensics community. Previous research [5–7] has shown some evaluation of the tools; however, there has not been updated literature found on the topic.

This research aims to address the lack of literature on evaluating free and commercial recovery tools in digital forensics. The study will evaluate two tools, one commercial, and one free tool on a spinning hard drive utilizing newly released Microsoft Windows 11. Microsoft Windows is one of the most utilized Operating Systems and according to Microsoft [8] there is 1.3 billion users of Windows 10. Microsoft Windows 11 is the next step for the users and that is why this research has chosen Microsoft Windows 11. Despite the increased presence of solid state drives, spinning hard drives are still widely used and should not be forgotten when it comes to digital forensics analysis. According to [9], in 2020 there has been sold approximately 350 million spinning hard drives and 320 million solid state drives. Most of the tools have the capabilities of analyzing solid state and spinning hard drives today. The chosen commercial tool is Magnet AXIOM Process and Examine, created by Magnet Forensics [10]. Magnet Forensics is being used by many law enforcement offices and it was nominated as DFIR Commercial Tool of the Year in July of 2021 [11]. The free tool of choice for the research is Autopsy [12] and has been one of the best open source platforms for digital forensic investigators for years. Autopsy was approved by the National Institute of Standards and Technology (NIST) in 2012 and supporting Windows runtime environment. Finally, we used differential analysis approach to ensure the validity of our analysis [13].

Contributions of this research include:

- Detailed analysis of deleted files from Windows 11 OS and their persistence in multiple stages.
- Providing a detailed evaluation of the two tools used for the experiment.
- Comparison of the different stages of deleted files and their persistence utilizing differential analysis.

The rest of the document is structured as follows, Sect. 2 discusses the related work pertaining to the problem pointed out in the paper. Section 3, discusses the methodology and the design of the experiment. Section 4, discusses the results and the analysis of the experiment. Lastly, Sect. 5, presents the conclusion and the future works.

2 Related Work

The difference between free and commercially available tools for digital forensics has been debated for years. Free tools have been closing the gap in recent years but is that gap close enough to switch to the free tool? In the research [7], five tools were assessed under the same conditions to evaluate the outcome of the recovered files. The tools included in the study were, EnCase, FTK, Recuva, R-Studio, and Stellar Phoenix. The EnCase and FTK were commercial tools, where the other three tools were data recovery tools but did not classify as digital forensics tools [7]. The tools were picked based on popularity at the time of the paper. The experimental method included a machine with a Windows operating system and installation of previously selected applications as well as data population. The research [7] showed that neither tool had the same recovered data, and no tool recovered all the files.

In the research, [5] two popular filesystems New Technology File System (NTFS) and File Allocation Table 32 (FAT32) were examined. The end goal was to verify against predetermined files, forensically discovered files that had been deleted and recovered to examine the success of the file system. The process consisted of four phases, assess, acquire, analyze and report. The three sections used to organize hard drives included information, file storage, and basic data [5]. In order to prove the recoverability of the two different filessystems (FAT32 and NTFS), the files were deleted first and wiped afterward. Upon imaging process, FTK was used for analysis. The results of the experiment [5] showed that the deleted files using Evidence Emulator (EE) could not be recovered forensically. The EE at the time of the experiment was used to wipe all of the data from the storage devices.

Actions performed after the files have been deleted greatly impact the process of recovering deleted items. In the paper [13], a differential analysis approach was utilised to evaluate the persistence of deleted files and better understand the process of deletion. Similarly in [14], factors affecting deleted files were identified. The studies have compared the images taken before the files were deleted, after they were deleted as well as after some actions performed on the system. Images of the hard disks were compared and the conclusions were drawn. Throughout the process a prototype of the software was developed to aid the analysis. The developed software allows for parsing the DFXML file form the NTFS system [15]. The full code is available at the GitHub page (https://github.com/AllisonShen/security_mft). As the conclusion the study has shown the way of comparing different stages of the deleted files and their reminiscence.

Unauthorized access to computer systems has been a problem for years. Recent research [16], conducted an experiment from a data recovery perspective utilizing Windows and Unix platforms. The researchers wanted to utilize multiple methodologies on deleted data. The paper [16], pointed out a four-step process of acquiring digital evidence. The first step is the acquisition of the evidence. Next, authentication of the evidence is necessary to ensure the integrity of the data. The third step is to analyze gathered data. Lastly, evaluation of the information and if the evidence can be used in court. Later in the paper,

researchers explained the differences between Windows and Unix systems and showed the locations where the evidence is most likely to be. Tools used to recover data from Windows OS were, Drivespy, Encase, and Ilook. The Sleuth Kit and The Coroner's Tool Kit were used in Unix OS. Basics overview of computer forensics methods and tools was presented in the paper [16], and explaining an overview of the tools used.

The variety of digital evidence has increased, never the less, it still can be sorted into five different categories according to [6] paper. Out of the five categories, the main three related to this research include image/video like files, system files, and document files. Increased storage is gained through hard drives, which are comprised of programs to store data and an operating system. The research [6] designates six levels to organize the files. The structure of levels numbered 0 through 5 is as follows:

- regular files
- temporary files
- deleted files
- retained data blocks
- vendor hidden blocks
- overwritten data

The experiment [6] was conducted on different hard drive technologies and file structures. Various tools were applied to recover data on such structures as photographs and videos. These tools, when compared, were found to be able to recover the data to a certain extent. The results showed Encase performing the best compared to Autopsy, OSForensics, and Recuva. The difference was almost 90% between Autopsy and Encase in found files, although Autopsy had 70% of data usability after restoration. As a conclusion of the study [6] the researchers noted Encase was the tool best suited for recovering data and reliability of use, followed by Autopsy.

On the other hand, in the paper [17] researchers investigated connections within computer forensics and recovering of the data. Additionally, research [17] investigated applications of anti-forensics and computer forensics. Anti-forensics technology was divided into three main categories, data hiding, data erasure, and encrypted data [17]. The most common tool for data hiding is Runefs, manipulating data to be stored as bad blocks. Data erasure is the most effective anti-forensics strategy by attempting to remove evidence. Encrypted data is not hidden but unknown to a user, potentially containing malicious code. The research [17] also divided computer forensics technology into two levels, hardware and software forensics tools. Hardware forensics tools utilize disk reading, firmware restoration, and hardware substitution [17]. Software forensics tools vary based on the data in need of recovery. The researchers concluded that data recovery is an important link in the crime-solving process due to the increased number of cybercrimes.

A survey paper [18] examined ten database extraction tools that were selected based on recency and the ability to support different platforms. Supporting different platforms was important in order to reach a wide area of users. The

researchers could not evaluate tools on the same sample database due to the differences of each tool and their execution. Regardless of the different formats of the data used for the tools, the results were valid. The tools from the experiment [18] provided various uses, including verification and data extraction.

Computer forensics and mobile forensics have been becoming more coherent, with platforms sharing similar hardware and software specifications. In the paper [19], a comparison of android forensics was utilized for retrieving file systems. The methodology used in this study consisted of six stages. The stages included the evidence intake phase, identification phase, preparation phase, isolation phase, processing phase, verification phase, and documentation/reporting phase. The outcome showed the method of AccessData FTK Imager and dd Image Evidence Tree, file carving utilizing Autopsy produced the most results [19]. Moreover, the researchers recommended EaseUS Data Recovery Wizard Free for recovering deleted files.

3 Methodology

The goal of this study was to compare two tools and analyze their findings based on the different stages of the files being deleted. The files were carefully created for this experiment based on average user habits. For example, files were placed in the downloads and documents folder where the user is most likely to store them. Each folder contained multiple files and multiple types of files varying in size. After the deletion process, various activities were performed, such as web browsing, downloading of the files, watching videos, and many more. The process presented multiple stages of the user's activity, giving the researchers multiple points for the examination. The operating system of choice was a newly released Microsoft Windows 11 installed on a spinning hard drive.

The experimental design of the study follows the four-step methodology presented below.

3.1 Environment Preparation

The first step of the experiment was choosing the equipment for the study. The environment consisted of one laptop (Dell Latitude 5591) with two separate hard drives. The first hard drive (HDD) was the one being examined, and the second solid-state drive (SSD) was the one containing the examination software. The hard drives were altered in the laptop based on the need and were never in the laptop at the same time. This is to ensure no cross-contamination of the data. The solid-state drive containing the necessary software did not need any additional setup, where the HDD (Hitachi 100 GB) had to be wiped, and the new Microsoft Windows 11 required installation. Since the HDD was not a new unit, a complete wipe was performed. This step was completed utilizing Ultimate Boot CD (Version5.3.8) [20] and Darik's Boot and Nuke (2.3.0) [21] software. The wipe method used the 'DoD Short' option with three rounds of wiping. Upon wiping, the next step was to install Windows 11 Pro and update.

Once the drivers and operating system was up to date, the updates and driver updates were paused for a month, so there would not be any additional traffic interfering. In addition to the pausing updates, a modified script [22] was run to stop any unnecessary services. The last step before transferring the files to the laptop was to open the Microsoft Edge browser and set it up. The default setup was followed. The specifications of the Hitachi HDD that is being examined is presented in Table 1.

Table 1. Hitachi Hard Drive Information

Manufacturer	HITACHI
Serial Number	MPCZN7Y0HGP1ML
Model Number	HTS721010G9SA00
Capacity	100 GB
Date of Creation	January 2007
RPM	7200
P/N	0A27318
MLC	DA1373
CHS	16383/16/63
F/W	C10H

3.2 Data Creation

In order to control the environment as best as possible, 24 separate files were created with three different categories text, images, and videos. Each category consisted of eight files, four that were placed in the documents folder and four for the downloads folder. The naming scheme was followed by the folder placement, type of the file, and file number. For example, image three that was placed in the downloads folder was named *downloads_image_3.jpg*.

The text files had four different sizes starting with around 1 KB, 1 MB, 100 MB, and 500 MB. This strategy ensured the range of multiple text files. Since the files were created by the researchers manually and the custom text was in each of the files, the exact sizes (e.g., 100 MB, or 500 MB) were not possible to achieve. Nevertheless, the sizes are close to the ones referenced. The first text file had 30 lines of the following text *documents_file1_column_A_row_1* except where the row number would increase for the each row added. The reason for allocating columns and rows in the text files was so if a partial recreation of the file was possible, the researchers would know exactly what part of the file was recovered.

Just like the text files, the four images created for the study were of different sizes. Since the size of the photos is harder to predict, a different approach was used. For the creation of the photos, the Nikon D5200 D-SLR camera with

various modes created different size images. The first and the smallest images in both documents and downloads folder were taken using 'BASIC' image quality and 'Small' image size equaling to around 430 KB. The second image settings were 'NORM' image quality and 'Medium' image size adding to around 3.5 MB for each folder. The third image had 'FINE' and 'Large' settings for the image quality and the image size, respectively equaling to around 8.1 MB. Lastly, the fourth image, 'RAW' image quality, and 'Large' image size adding up to around 25 MB. The content of the photo was the name of the photo with a white background. For example, the second photo placed in the downloads folder (*downloads_ image_ 2.jpg*) had the content showing *downloads image 2*. All of the photos were shot in the same environment, from the same place, and the mode of the pictures was set to auto.

Lastly, the videos were taken with the same camera (Nikon D5200) following the same naming scheme as the photos, except having video instead of an image. The process of creating the videos differed from creating the photos. The quality settings of each video was the same; movie quality set to 'high', and frame size/frame rate set to '1920 × 1080 and 60'. The microphone was set to auto sensitivity, and the automatic focus was left on. Background audio was generic beeping noise which was the same for all videos. To differentiate the sizes of the videos the first video was 5 s long, the second was the 60 s, the third was 300 s, and the last video was 600 s long, equaling to sizes of around 15 MB, 164 MB, 817 MB, and 1.5 GB respectively.

Presented in Table 2 are all of the created files for this experiment. For the full MD5 and SHA256 values of the files created, please reference the A. Appendix, Tables 6 and 5.

3.3 Data Population and Collection

Data population and the data collection for this experiment was conducted in five different phases. Each of the phases was built upon the previous and linked together to complete the study. After each phase, an image of the Hitachi HDD was captured.

Consequent to the creation of the files, the researchers placed Hitachi HDD into the laptop, powered it on, and copied the files in the already predesignated folders (documents and downloads). Once the files were copied, the laptop was powered off, and the HDD was pulled out from the laptop. Meanwhile, the SSD with the examination software was put back on the laptop. In order to create an image of the Hitachi HDD, a write blocker presented in Fig. 1 was used. This was to eliminate any potential writing to the HDD. Software utilized to create the RAW (dd) image of the physical device (Hitachi HDD) was AccessData's FTK Imager (Version 4.2.1.4) [23]. The created image was named *image_ 01_ BI*, BI abbreviating the base image. The base image was used as the reference to the other images and in checking hash values of the files.

The second phase of the data population and collection consisted of reinstalling the Hitachi HDD and powering on the laptop. In this phase of the experiment, all the files previously copied (total of 24) were deleted from the

Table 2. Created Files for the Examination

File Name	Size
documents_file_1.txt	1011 bytes (1,011 bytes)
documents_file_2.txt	1.04 MB (1,098,892 bytes)
documents_file_3.txt	106 MB (111,666,573 bytes)
documents_file_4.txt	528 MB (554,332,869 bytes)
documents_image_1.JPG	431 KB (442,055 bytes)
documents_image_2.JPG	3.37 MB (3,537,995 bytes)
documents_image_3.JPG	7.95 MB (8,346,930 bytes)
documents_image_4.NEF	24.7 MB (25,959,999 bytes)
documents_video_1.MOV	14.7 MB (15,432,643 bytes)
documents_video_2.MOV	159 MB (166,766,872 bytes)
documents_video_3.MOV	793 MB (832,085,550 bytes)
documents_video_4.MOV	1.54 GB (1,662,377,424 bytes)
downloads_file_1.txt	1009 bytes (1,009 bytes)
downloads_file_2.txt	1.04 MB (1,098,892 bytes)
downloads_file_3.txt	106 MB (111,666,573 bytes)
downloads_file_4.txt	528 MB (554,332,869 bytes)
downloads_image_1.JPG	434 KB (444,917 bytes)
downloads_image_2.JPG	3.42 MB (3,596,578 bytes)
downloads_image_3.JPG	7.97 MB (8,358,210 bytes)
downloads_image_4.NEF	24.4 MB (25,648,008 bytes)
downloads_video_1.MOV	14.7 MB (15,420,553 bytes)
downloads_video_2.MOV	160 MB (168,357,406 bytes)
downloads_video_3.MOV	798 MB (837,483,431 bytes)
downloads_video_4.MOV	1.54 GB (1,662,532,158 bytes)

laptop (SHIFT + Del), and the laptop was powered off. The second image of the HDD was taken, again using a write blocker and FTK Imager. The name of the image was *image_ 02_ AD*, referring to after the delete process.

In the third phase, the laptop was powered on, and the laptop was left idling for 60 min (±3 min). The idling process did not involve any user interaction besides powering on and off the laptop and opening the task manager to monitor the 'up time' of the machine. After an hour, the laptop was powered off, and the HDD was extracted once more. The third image was taken from the extracted HDD using the same methods as before. The image was named *image_ 03_ ADI*, abbreviating after delete and idling period.

The fourth image followed the same procedure for installing the HDD and powering on the laptop. The purpose of this phase was to create an image of the HDD after an hour of browsing the internet, mimicking the everyday activity of a user. For the browsing activity, the researchers have chosen not to use

Fig. 1. Write Blocker with HDD Attached

more than five tabs at the time, with one of the tabs dedicated to the timer on YouTube.com, showing the time spent on browsing. The browser used for this activity was Microsoft Edge (Version 90.0.818.66). The rest of the tabs were used for searching news and articles on stocks, technology, science, etc. For the full browsing history, please refer to the B. Appendix. When the 60 min (±3 min) mark elapsed, the laptop was turned off, and the same procedure for imaging the HDD was repeated. The name of the fourth image was *image_04_ADW*, W standing for the web.

Lastly, the fifth activity of the last phase was to download a file that is larger than 10% of the entire size of the HDD. In this case, the file needed to be over 10 GB. In order to download a known file, the researchers have created and uploaded the file to Microsoft's OneDrive using a different computer. The name of the file was *download_file_test.zip* and the size was 10.4 GB. For the last time the HDD was extracted from the laptop for the imaging process. The same procedure was followed as in the previous steps for obtaining the image.

3.4 Data Processing and Analysis

Data processing for this experiment started when the five images were taken. Since the images were in the RAW (dd) format, it allowed both examining software to use the files. The machine used for the examination was the same laptop used for the experiment, except the hard drives were swapped. Instead of Hitachi HDD, which was pulled out of the laptop after the fifth image, the SSD with examination software was installed back in the laptop. The specifications of the laptop with the examination software are as follow:

- Processor: Intel(R) Core(TM) i7-8850H CPU @ 2.60 GHz 2.59 GHz
- RAM: 16.0 GB
- Graphics Card: NVIDIA GeForce MX130

- Integrated Graphics: Inte(R) UHD Graphics 630
- Examination SSD: NVMe CA3-8D512-Q11 NV
- BaseBoard: Dell Inc. 0DVVG1 A00
- Operating System: Windows 10 Pro (Version: 21H1, OS Build: 19043.1348)

Magnet Forensics Suite [10], more specifically Magnet AXIOM Process (v5.6.0.26839) and Magnet AXIOM Examine (v5.6.0.26839) was the commercial tools of choice for the project. The examination of the RAW (dd) images followed the same procedure for all five of the images captured and involved both tools. The first tool, the Magnet AXIOM Process, was used to acquire the evidence. For the examination all of the artifacts were selected except the memory, which was grayed out and not allowed to be selected. An additional step was taken before the acquisition process started, a custom keyword search. The custom keyword search included all 24 file names without their extensions (e.g.,*documents_image_1*). This added an additional layer of search. Once the acquiring process was finished, Magnet AXIOM Examine was used to analyze the cases.

The procedure followed for creating the case in Autopsy (version 4.19.1) was very similar to Magnet AXIOM Process, except some of the features of the Autopsy were turned off. The ingests that were not included were Email Parser, Encryption Detection, Virtual Machine Extractor, Android Analyzer (aLEAPP), DJI Drone Analyzer, Plaso, iOS Analyzer (iLEAPP), Android Analyzer. It is important to note that the custom keyword search list was created for the Autopsy with the names of all 24 files created for the experiment.

The analysis process involved two stages in five different phases. The first stage was analyzing five different cases utilizing Magnet AXIOM Examine. The second phase involved the same process, just using Autopsy. In addition, cases from the same RAW (dd) image were compared with both Magnet AXIOM and Autopsy. This process ensured the best evaluation of the tools and eliminated any potential bias since two different tools were used. Given that there was nothing deleted on the first image, both applications should produce the same results giving it a good starting point for the rest of the analysis. In the last phase of the analysis, the five different images were observed using the methods from [13,14] showing the persistence of files throughout different stages of the research.

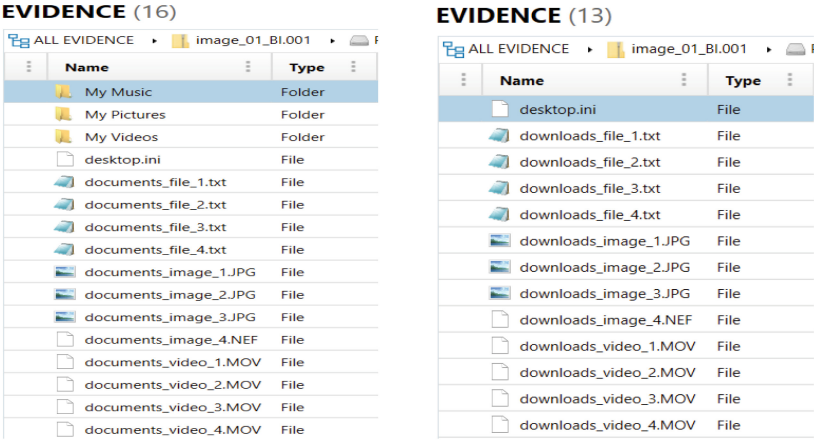
4 Discussion of the Results and Analysis

Reading the literature and observing that there was not a lot of updated documentation on evaluating digital forensics tools gave us an idea to do just that. Part of the reason for this gap could be the releasing of the frequent updates for the tools. This section discusses the experimental results and analyzes the findings. The first part of this section discusses the reasoning of the experiment, and the second part takes a look into the results organized by the RAW (dd) images taken of the Hitachi HDD.

The five different stages selected for the analysis of the project were chosen based on the daily use of an average user. The usage included file transfer, file delete, not performing any tasks for an hour after the delete, an additional hour of web search after the delete and the idle, and lastly, a large file download. The progression of the activities goes from basic to where comprehensive writing was introduced to the hard drive.

4.1 First Image - Base Image

During the analysis of the first image, the 24 files previously created were just transferred onto the laptop, and the laptop was turned off shortly after. The files were copied from the USB into two folders, documents and downloads. Once the cases were created, it was expected for the files to be present. As this image was referenced as the base image, the researchers wanted to observe how the programs processed the RAW (dd) image and be able to compare the images in the future. As it can be seen in Fig. 2, the files were found and located in the dedicated folders utilizing Magnet AXIOM Examine.



(a) Documents Folder (b) Downloads Folder

Fig. 2. Base Image - Magnet AXIOM

All file sizes matched when compared to the initial files. Additionally, the MD5 hash values of the files matched as well, except for the *documents_file_4.txt, documents_video_3.MOV, documents_video_3.MOV* and *downloads_file_4.txt, downloads_video_3.MOV, downloads_video_4.MOV* in the downloads folder. Magnet AXIOM for these files was not able to calculate the hash values.

For the analysis in the Autopsy, the process did not change compared to the Magnet AXIOM, and also the results did not differ greatly. All files were

in the designated folders and the sizes matched to the original sizes of the files. Unlike Magnet AXIOM, all of the hash values were matching and showing. Despite the hash values being correct for the files, Autopsy flagged *documents_video_3.MOV, documents_video_4.MOV, downloads_video_3.MOV, downloads_video_4.MOV* with the message, 'Hash an unlikely notable analysis result score'. Figure 3 shows the files found by Autopsy.

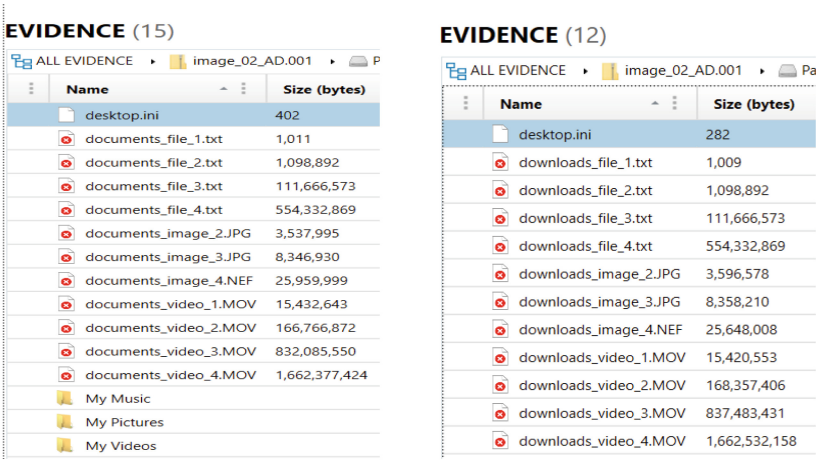
(a) Documents Folder (b) Downloads Folder

Fig. 3. Base Image - Autopsy

4.2 Second Image - After Delete

The analysis of the second image took place after all 24 files previously transferred were deleted using 'SHIFT + Delete' method and turning off the laptop. The process consisted of the same procedures as analyzing the first image. As it can be seen in Fig. 4, the results show *documents_image_1*, and *downloads_image_1* are missing from the list.

The files that were not missing are marked as deleted. The contents of those files were the same as in the first image except for the (*documents_file_1, downloads_file_1*). This is also confirmed by hash values not matching compared to the base image. The files where the hash values matched were able to display the contents without any issues. The two text files missing, additional information about them was found in *$LogFile Analysis* and *$UsnJrnl*. The analysis was performed by utilizing a previously created keyword search. The messages presented by Magnet AXIOM in the update sequence number journal ($UsnJrnl) of the related files were:



(a) Documents Folder (b) Downloads Folder

Fig. 4. After Delete - Magnet AXIOM

- The data in the file or directory is overwritten.
- The file or directory is extended (added to).
- The file or directory is created for the first time.
- A user has either changed one or more files or directory attributes (for example, the read-only, hidden, system, archive, or sparse attribute), or one or more time stamps.
- The file or directory is closed.

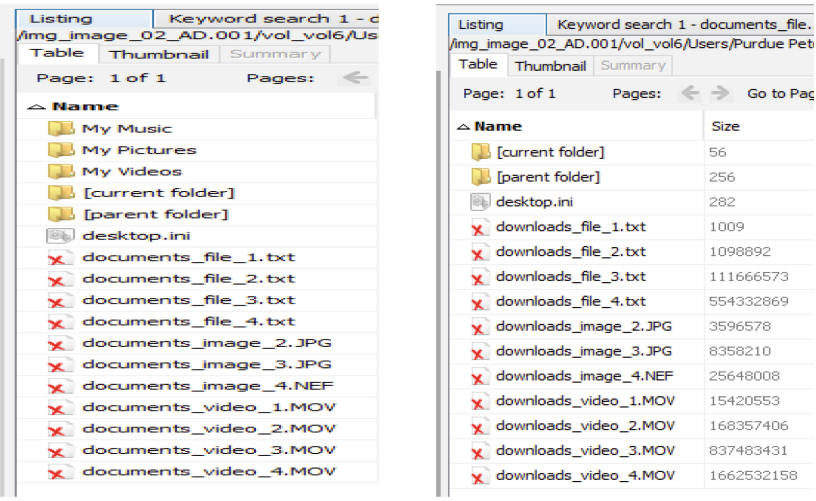
For the files that were not showing, the only locations where the names of the files (*documents_image_1, downloads_image_1*) were found are the same locations as for the *documents_file_1, downloads_file_1*, giving the same reason as previously stated.

The analysis utilizing Autopsy shows a different results but not by much. Like Magnet AXIOM tools, Autopsy could not show the (*documents_image_1, downloads_image_1*) files in the original folder as seen in Fig. 5. Moreover, hash values of the *documents_file_1, downloads_file_1* did not match also and the text files were unreadable. Keyword search for the two files showed presence showed in Table 3.

Traces of the two files (*documents_image_1, downloads_image_1*) that were not appearing in the initial folders were found in *$LogFile* and *$UsnJrnl:$J*. Lastly, compared to the base image only *images_2*, *images_3*, and *images_4* did not have the flag 'Hash an unlikely notable analysis result score' given by Autopsy.

4.3 Third Image - After Delete and Idle

After the process of creating the second image using FTK Imager, the third phase consisted of powering on the laptop and letting it idle for 60 min (±3 min) and



(a) Documents Folder (b) Downloads Folder

Fig. 5. After Delete - Autopsy

turning the laptop off before taking the third image. Upon opening the created case in Magnet AXIOM and navigating to the designated folders (Documents and Downloads), there were no files showing. Keyword search showed the only traces of the file names were in *$LogFile Analysis* and *$UsnJrnl*. Reasons for the files shown are the same as in the previous analysis of the second image, right after the delete.

The autopsy showed similar results to Magnet AXIOM, where the files did not show in either of the folders, and the traces were only found in *$LogFile*, *$MFT* and *$UsnJrnl:$J*.

4.4 Fourth Image - After Delete and Web Browsing

The fourth image was after the files were deleted, the idle of the laptop for an hour, and an additional hour of web browsing. Following the process and case creation, Magnet AXIOM was not able to recognize any files in the designated folders of the deleted files. The only location where the keyword search was able to find a match was in *$UsnJrnl*. The keyword search found all 24 file names, and the messages presented by Magnet AXIOM in the update sequence number journal ($UsnJrnl) of the related files showed the same reasons as before.

The report from the Autopsy and the keyword search shows the traces of all 24 files in *$UsnJrnl:$J*. In the *MpWppTracing-20211119-195058-00000003-ffffffff.bin* are found traces of the *documents_file_1.txt*. Lastly in the *$MFT file*, keyword search found *downloads_video_4.MOV* and *downloads_file_1.txt* but no other information was able to be presented.

Table 3. Keyword Search

Name	Location
MpWppTracing-20211119-195058-00000003-ffffffff.bin	/img_image_02_AD.001/vol_vol6/ProgramData/Microsoft/Windows Defender/Support/MpWpp Tracing-20211119-195058-00000003-ffffffff.bin
U snJrnl :J	/img_image_02_AD.001/vol_vol6/Extend/U snJrnl : $J
$LogFile	/img_image_02_AD.001/vol_vol6/$LogFile
$MFT	/img_image_02_AD.001/vol_vol6/$MFT
documents_file_1.txt	/img_image_02_AD.001/vol_vol6/Users/******Pete/Documents/documents_file_1.txt
documents_file_1.txt-slack	/img_image_02_AD.001/vol_vol6/Users/******Pete/Documents/documents_file_1.txt-slack
U snJrnl :J	/img_image_02_AD.001/vol_vol6/Extend/U snJrnl : $J
downloads_file_1.txt	/img_image_02_AD.001/vol_vol6/Users/******Pete/Downloads/downloads_file_1.txt
downloads_file_1.txt-slack	/img_image_02_AD.001/vol_vol6/Users/******Pete/Downloads/downloads_file_1.txt-slack
$LogFile	/img_image_02_AD.001/vol_vol6/$LogFile
$MFT	/img_image_02_AD.001/vol_vol6/$MFT

4.5 Fifth Image - After Delete and Download

In the last image we wanted to download a large file that was over 10% of the whole size of the disk. In our case that was a file over 10 GB in size. Upon the download of the file, the laptop was turned off and the RAW (dd) image was taken. Magnet AXIOM once more was not able to show the deleted files and the only place where the traces of the files were found are in *$UsnJrnl*. Same as in the step four, the keyword search was able to find all 24 names in the *$UsnJrnl*. Autopsy showed the traces only in *$UsnJrnl:$J* for all 24 files.

4.6 Persistence of Deleted Files

For the last test we wanted to ensure that the results we got from both, commercial and free software were accurate and no data was overlooked. This is often seen due to the software limitations which can cause issues when the evidence is presented in courts or just resolved with the newer updates. The Table 4 shows the persistence of all files throughout five images utilising persistence of deleted files script. Additionally, the table shows the percentage of the files left after each of the five actions. Magnet AXIOM Process and Autopsy were able

to see files right after they have been deleted (image 2) with the exceptions of *documents_image_1.JPG* and *downloads_image_1.JPG*. Magnet AXIOM Process and Autopsy were not able to decipher any usable files in images 3, 4, and 5. On the other hand, persistence analysis script for some of the files was not able to recognise any persistence left (e.g., *documents_file_1*) while showing lot more persistence on other files such as *documents_file_4*. Note that for both *documents_image_1.JPG* and *downloads_image_1.JPG* files were not created. It is suspected that the proprietary software was not able to pick it up for an unknown reason to the researchers.

Table 4. Persistence of Deleted Files after Each Image

Name of the file	Base Image (image 1)	After Delete (image 2)	After Delete and Idle (image 3)	After Delete and Web Browsing (image 4)	After Delete and Download (image 5)
documents_file_1	100%	0%	0%	0%	0%
documents_file_2	100%	100%	100%	0%	0%
documents_file_3	100%	100%	100%	30%	0%
documents_file_4	100%	100%	100%	100%	0%
documents_image_1	100%	unknown	unknown	unknown	unknown
documents_image_2	100%	100%	100%	0%	0%
documents_image_3	100%	100%	100%	0%	0%
documents_image_4	100%	100%	100%	80%	0%
documents_video_1	100%	100%	100%	100%	0%
documents_video_2	100%	100%	100%	0%	0%
documents_video_3	100%	100%	100%	100%	0%
documents_video_4	100%	100%	100%	100%	0%
downloads_file_1	100%	0%	0%	0%	0%
downloads_file_2	100%	100%	100%	0%	0%
downloads_file_3	100%	100%	100%	80%	0%
downloads_file_4	100%	100%	100%	100%	0%
downloads_image_1	100%	unknown	unknown	unknown	unknown
downloads_image_2	100%	100%	100%	0%	0%
downloads_image_3	100%	100%	100%	1–5%	0%
downloads_image_4	100%	100%	100%	100%	0%
downloads_video_1	100%	100%	100%	0%	0%
downloads_video_2	100%	100%	100%	100%	0%
downloads_video_3	100%	100%	100%	100%	0%
downloads_video_4	100%	100%	100%	100%	0%

5 Conclusion and Future Works

The main goal of this paper was to study and evaluate two different tools for digital forensics investigators on the deleted files. One commercial and one free tool was evaluated on Windows 11 Pro operating system utilizing a spinning hard drive. This analysis and evaluation included five different scenarios, each of which gave the experiment different steps after the files were deleted.

In this experiment both tools performed equally well with some minor differences. Acquisition time of Magnet AXIOM Process was significantly less compared to Autopsy. The acquisition process of the RAW (dd) image utilizing

Magnet AXIOM Process on average took 55 min, and using Autopsy with multiple injests unchecked took on average around 5 h. Moreover, Magnet AXIOM Examine showed more reasons for the possibilities of the files being deleted. Despite the difference of the software no different information was found once compared. Both software solutions were able to recognize the deleted files in the second image and were not able to see it in the rest of the experiment. A possible explanation for the lack of evidence given the nature of NTFS structure could be due to the two programs used in the study are not able to read the remnants of deleted files. In contrast the persistence analysis throughout all files on all images has shown that deleted files mostly survived until the third image.

Continuation of this project will follow, analysis of the *$MFT* files and *$UsnJrnl* files on all images to understand the metadata. Moreover, adding more tools to be examined for both commercial and open source. Some of the questions that can also be answered during the future works are how does the poweroff preserve the files, probabilities of the smaller size files being preserved longer. Finally, in the future works is to utilize different methods of data storage and different file structures and types. The approach will allow for greater data set for the future use, aiding digital forensics investigators and digital forensics enthusiasts.

A Appendix - Hash Values of the Created Files

Table 5. SHA256 Values of the Files

File Name	SHA256
documents_file_1.txt	D1BEA1EA1FE26B7D550CC7E6C5295C3A41AE98EADE9D837B9FEDF0ADBD79CFB2
documents_file_2.txt	F6E5BEEEB604AC2701356BD46DBF34F367D83651F9AFB25E0F503EA5239D609B
documents_file_3.txt	D9ECBB1E43031E588FD5C75B551F0BE1277BAACB93EF10C5267DCCF4A90BD511
documents_file_4.txt	3714966D123BC9832342BDA5D84250FE73C8F0E1423386587531462O7B7AA866
documents_image_1.JPG	B42CECE6F5E6280A07012358DAF88A7FE42D3A0E574CCD9384A8BB0E043170D5
documents_image_2.JPG	6B26FB548EDE7F9E06C1619CEE9CD273914A2FCE491671C1C542AD794FA35C5E
documents_image_3.JPG	3E4AA3C286B74C6DF4EDBE2AF4D5D44F358ACE938B7CA87C2D1C993817AED583
documents_image_4.NEF	0929F4747218CE984CB51ACA22A22C0C06DD7DE335761A38DEC80C6AEEFAB4F4
documents_video_1.MOV	347471C37D0358B93055A8B459AE17E29ACEBCC11EA051EDB0EE52DE79187A28
documents_video_2.MOV	8B853A3FEB09D1D53971649BBAC10621AC4C8564D9AD0D243E7C700D1ECB0D5B
documents_video_3.MOV	4434D6FC562E459EF527B396FFCF23DFB7644678BC319B29F5075CC36A5CC64C
documents_video_4.MOV	586DEF420099C97A0D3A1E39CD0A3BA54421033EFD8094E12974D4556B837E09
downloads_file_1.txt	9F1D88A8AC810659C6B0560AD35E4DB7ACDBB19B8AA1B2645165D3190D2BE636
downloads_file_2.txt	8AA0DCA4B1EC2AE16371F8046422B202E842EA0E386541FD86E384052DB0F29C
downloads_file_3.txt	7C27BA8A3AC7CA54C6ECCC8C11B330C13CAF824C21E7D47A767FEDB862F4102B
downloads_file_4.txt	8380874C6EEFAFC9016D4F6D980B27586814320C273005B81CBF5478FC92588C
downloads_image_1.JPG	7B04459AADEEFCC0BE4EFD35AA11ACD8282970C401022AB8BF16C3976DFC6131
downloads_image_2.JPG	92213B800D5A9D5793523DC1DD5DFFF86FC497774F216E8AE5935BA0FCEF0332
downloads_image_3.JPG	409D62F6DECB10B496986C769A1056A3FA0E6E8760CE14400BE0C8C6D3419086
downloads_image_4.NEF	AFA4C90D1C08F20687AA6C20B30F626E41FF5C06C81D0624A231A2966DCBAAC3
downloads_video_1.MOV	038F6C8793893936129C2C41768E9B86F93CB9BE97B23032BD84D67F189B973E
downloads_video_2.MOV	6EC3E100E72B45242A26D899B93C104CA818227000BB784304405267B51E0F08
downloads_video_3.MOV	32FA70ADF0FAC8EF6DEBC22032184E8C5CB19C121837E777A011D93C552B0EEA
downloads_video_4.MOV	F44CCAC646A5C685444BDA79816F6A2D71A6BBE80744B5BF3979FF2683115A8A

Table 6. MD5 Values of the Files

File Name	MD5 Value
documents_file_1.txt	18E9B2B48C85038F40FF56FAB92CCFE7
documents_file_2.txt	A6C813724F90A6DEDC9E90CC85420692
documents_file_3.txt	8012575698CC73C2271CBEAF1509E53D
documents_file_4.txt	91A699C84D1FB777CF8770BFBF0C0CA5
documents_image_1.JPG	4E71D99F41DED0496B4A662E130A640B
documents_image_2.JPG	F2DD9996CE24B8D018F1EC2CB908517F
documents_image_3.JPG	8D678D9168016CB1DF0D78CF5401DA08
documents_image_4.NEF	6EFDD9F736F595B66D24D041C39DA13A
documents_video_1.MOV	FE8AE4FB0B41BBDA2C660C4A8718F8AF
documents_video_2.MOV	7B8B826B20DEB6213EF56E7ADAF39B10
documents_video_3.MOV	EAB8A5C9692449EAEA6357BDF26AED84
documents_video_4.MOV	40A034E5602103161551A812C6FDBF4A
downloads_file_1.txt	C2565A04AE5846A1B240AF64FDCB083F
downloads_file_2.txt	CD2390F4531F00BC4C46AEFA544004B9
downloads_file_3.txt	981D64297FCD6E48011DD0BCA9445A64
downloads_file_4.txt	E95A2322DF03855B609A3375586EB13F
downloads_image_1.JPG	9B41B370F3F68661E02392E175089223
downloads_image_2.JPG	82481249AA00504C36021C1A2179AB92
downloads_image_3.JPG	9F6512743155F1D639D94E40EC9E65B2
downloads_image_4.NEF	11C865193ECBB083A9D576D218E66156
downloads_video_1.MOV	25000B37CA3619D0307BDA2563323D4B
downloads_video_2.MOV	FB38471A126C94ED04B7D122F9D8B7E4
downloads_video_3.MOV	C0930EA581932DB24DAB957E3F9882F9
downloads_video_4.MOV	188A26DA51F8C9A499E71E7E2CE4C56D

B Appendix - Microsoft Edge Browsing History

The items below are listed in the chronological order by browsing activity. The format follows **Title | Time (UTC+0) | URL**.

1. YouTube | 11/21/2021 17:15 | http://www.youtube.com/
2. YouTube | 11/21/2021 17:16 | https://www.youtube.com/
3. 60 min timer - YouTube | 11/21/2021 17:16 | https://www.youtube.com/results?search_query=60+minute+timer
4. 60 min video - YouTube | 11/21/2021 17:16 | https://www.youtube.com/results?search_query=60+minute+video

5. AUTUMN 60 min TIMER, no music #60minutetimer - YouTube | 11/21/2021 17:16 | https://www.youtube.com/watch?v=QRjSongCKkM
6. stocks - Bing | 11/21/2021 17:16 | https://www.bing.com/search?q=stocks&cvid=86ab3c620a934928aa8e1e67a2efb5a3&aqs=edge.0.0l9.2100j0j1&pglt=2083&FORM=ANNTA1&PC=U531
7. Google | 11/21/2021 17:17 | https://www.google.com/
8. news - Google Search | 11/21/2021 17:17 | https://www.google.com/search?q=news&source=hp&ei=K3-aYfH7KNbVtAabjYugAg&iflsig=ALs-wAMAAAAAYZqNO6Vlx2uhjMZ4JLj8S5Z7fNhmRNql&ved=0ahUKEwixveD3-qn0AhXWKs0KHZvGAiQQ4dUDCAk&uact=5&oq=news&gs_lcp=Cgdnd3Mtd2l6EAMyCwgAEIAEELEDEIMBMgsIABCABBCxAxCDATIICAAQgAQQsQMyBQgAEIAEMgUILhCABDIICC4QgAQQsQMyBQgAELEDMggIABCxAxCDATIFCAAQgAQyBQgAELEDOg4IABCPARDqAhCMAxDlAjoOCC4QjwEQ6gIQjAMQ5QI6CwguEIAEELEDEIMBOg4ILhCABBCxAxDHARDRAzoOCC4QgAQQsQMQxwEQowI6EQguEIAEELEDEIMBEMcBENEDOgsILhCABBDHARCvAVC8CFjlDWDGD2gBcAB4AIABeogB1QKSAQMzLjGYAQCgAQGwAQo&sclient=gws-wiz
9. Google News | 11/21/2021 17:18 | https://news.google.com/
10. Google News | 11/21/2021 17:18 | https://news.google.com/topstories?hl=en-US&gl=US&ceid=US:en
11. Google News - Technology - Latest | 11/21/2021 17:18 | https://news.google.com/topics/CAAqJggKIiBDQkFTRWdvSUwyMHZNRGRqTVhZU0FtVnVHZ0pWVXlnQVAB?hl=en-US\&gl=US\&ceid=US\%3Aen
12. Ferrari Introduces the Daytona SP3, an 828-HP Tribute to the '60s - autoevolution | 11/21/2021 17:19:16 | https://news.google.com/articles/CAIiEOKi16f4Pv4pSWm8Q5nkEQIqMwgEKioIACIQFloNoavzTzBvP2PfEiuO2yoUCAoiEBZaDaGr808wbz9j3xIrjtswx-StBw?hl=en-US&gl=US&ceid=US%3Aen
13. Ferrari Introduces the Daytona SP3, an 828-HP Tribute to the '60s - autoevolution | 11/21/2021 17:19:16 | https://www.autoevolution.com/news/ferrari-introduces-the-daytona-sp3-an-828-hp-tribute-to-the-60s-174687.html
14. https://www.bing.com/search?q=krebs+on+security&cvid=4b58f3d343ac4148bb07f3270f3c769a\&aqs=edge..69i57.4000j0j1\&pglt=2083\&FORM=ANNTA1\&PC=U531 | 11/21/2021 17:21:22 | https://www.bing.com/search?q=krebs+on+security\&cvid=4b58f3d343ac4148bb07f3270f3c769a\&aqs=edge..69i57.4000j0j1\&pglt=2083\&FORM=ANNTA1\&PC=U531
15. n/a | 11/21/2021 17:21:22 | https://www.bing.com/newtabredir?url=https%3A%2F%2Fkrebsonsecurity.com%2F
16. Krebs on Security – In-depth security news and investigation | 11/21/2021 17:21:23 | https://krebsonsecurity.com/

17. Can You Jailbreak Your iPhone Running iOS 15 to iOS 15.1? Everything You Need to Know | 11/21/2021 17:31:44 | https://news.google.com/articles/CBMiamh0dHBzOi8vd2NjZnRlY2guY29tL2Nhbi15b3UtamFpbGJyZWFrLXlvdXItaXBob25lLXJ1bm5pbmctaW9zLTE1LXRvLWlvcy0xNS0xLWV2ZXJ5dGhpbmcteW91LW5lZWQtdG8ta25vdy_SAW5odHRwczovL3djY2Z0ZWNoLmNvbS9jYW4teW91LWphaWxicmVhay15b3VyLWlwaG9uZS1ydW5uaW5nLWlvcy0xNS10by1pb3MtMTUtMS1ldmVyeXRoaW5nLXlvdS1uZWVkLXRvLWtub3cvP2hsPWVuLVVTJmdsPVVTJmNlaWQ9VVMlM0Fl
18. Can You Jailbreak Your iPhone Running iOS 15 to iOS 15.1? Everything You Need to Know | 11/21/2021 17:31:44 | https://wccftech.com/can-you-jailbreak-your-iphone-running-ios-15-to-ios-15-1-everything-you-need-to-know/
19. 6 incredible Apple deals on Amazon ahead of Black Friday | 11/21/2021 17:35:07 | https://news.google.com/articles/CAIiECDYkClfUpv1m44PIS2Shw4qFQgEKg0IACoGCAow9ckFMIBVMJCfBA?hl=en-US\&gl=US\&ceid=US\%3Aen
20. 6 incredible Apple deals on Amazon ahead of Black Friday | 11/21/2021 17:35:07 | https://appleinsider.com/articles/21/11/20/6-epic-apple-deals-on-amazon-599-m1-mac-mini-99-apple-pencil-2-189-airpods-with-magsafe-more
21. Google News - World - Latest | 11/21/2021 17:36:01 | https://news.google.com/topics/CAAqJggKIiBDQkFTRWdvSUwyMHZNRGx1YlY4U0FtVnVHZ0pWVXlnQVAB?hl=en-US\&gl=US\&ceid=US\%3Aen
22. Google News - Sports - Latest | 11/21/2021 17:36:25 | https://news.google.com/topics/CAAqJggKIiBDQkFTRWdvSUwyMHZNRFp1ZEdvU0FtVnVHZ0pWVXlnQVAB?hl=en-US\&gl=US\&ceid=US\%3Aen
23. Google News - Science - Latest | 11/21/2021 17:36:45 | https://news.google.com/topics/CAAqJggKIiBDQkFTRWdvSUwyMHZNRFp0Y1RjU0FtVnVHZ0pWVXlnQVAB?hl=en-US\&gl=US\&ceid=US\%3Aen
24. NASA's DART Mission To Crash a Spacecraft Into an Asteroid Is Set To Launch – Watch It Live | 11/21/2021 17:36:56 | https://news.google.com/articles/CBMicmh0dHBzOi8vc2NpdGVjaGRhaWx5LmNvbS9uYXNhcy1kYXJ0LW1pc3Npb24tdG8tY3Jhc2gtYS1zcGFjZWNyYWZ0LWludG8tYW4tYXN0ZXJvaWQtaXMtc2V0LXRvLWxhdW5jaC13YXRjaC1pdC1saXZlL9IBdmh0dHBzOi8vc2NpdGVjaGRhaWx5LmNvbS9uYXNhcy1kYXJ0LW1pc3Npb24tdG8tY3Jhc2gtYS1zcGFjZWNyYWZ0LWludG8tYW4tYXN0ZXJvaWQtaXMtc2V0LXRvLWxhdW5jaC13YXRjaC1pdC1saXZlL2FtcC8?hl=en-US&gl=US&ceid=US%3Aen
25. NASA's DART Mission To Crash a Spacecraft Into an Asteroid Is Set To Launch – Watch It Live | 11/21/2021 17:36:57 | https://scitechdaily.com/nasas-dart-mission-to-crash-a-spacecraft-into-an-asteroid-is-set-to-launch-watch-it-live/

26. https://www.bing.com/search?q=zdnet&cvid=e5e4121259b54fefb3b3bd6ecd0daac1\&aqs=edge.0.0l9.1355j0j4\&FORM=ANAB01\&PC=U531 | 11/21/2021 17:39:11 | https://www.bing.com/search?q=zdnet&cvid=e5e4121259b54fefb3b3bd6ecd0daac1\&aqs=edge.0.0l9.1355j0j4\&FORM=ANAB01\&PC=U531
27. n/a | 11/21/2021 17:39:11 | `https://www.bing.com/newtabredir?url=https%3%2F%2Fwww.zdnet.com%2F`
28. Technology News, Analysis, Comments and Product Reviews for IT Professionals ZDNet | 11/21/2021 17:39:11 | https://www.zdnet.com/
29. FBI warning: This zero-day VPN software flaw was exploited by APT hackers | ZDNet | 11/21/2021 17:39:45 | https://www.zdnet.com/article/fbi-warning-this-zero-day-vpn-software-flaw-was-exploited-by-apt-hackers/
30. Nylas | Universal Email API | 11/21/2021 17:40:39 | https://www.nylas.com/products/email-api/?gclid=EAIaIQobChMIx8jSg4Cq9AIVi8D2Ah1X_gKBEAEYASAAEgJFSvD_BwE
31. Palo Alto Networks raises FY22 revenue guidance | ZDNet | 11/21/2021 17:41:08 | https://www.zdnet.com/article/palo-alto-networks-raises-fy22-revenue-guidance/
32. Dark web crooks are now teaching courses on how to build botnets | ZDNet | 11/21/2021 17:41:56 | https://www.zdnet.com/article/college-for-cyber-criminals-dark-web-crooks-are-teaching-courses-on-how-to-build-botnets/
33. Security | ZDNet | 11/21/2021 17:48:01 | https://www.zdnet.com/topic/security/
34. Cloud security firm Lacework secures $1.3 billion in new funding round | ZDNet | 11/21/2021 17:48:07 | https://www.zdnet.com/article/cloud-security-firm-lacework-secures-1-3-billion-in-series-d-funding-round/
35. n/a | 11/21/2021 17:52:43 | https://www.bing.com/newtabredir?url=http%3A%2F%2Fwww.foxnews.com%2F
36. Fox News - Breaking News Updates | Latest News Headlines | Photos & News Videos | 11/21/2021 17:52:43 | https://www.foxnews.com/
37. Fox News - Breaking News Updates | Latest News Headlines | Photos & News Videos | 11/21/2021 17:52:43 | http://www.foxnews.com/
38. NBC News - Breaking News & Top Stories - Latest World, US & Local News | NBC News | 11/21/2021 17:54:13 | https://www.nbcnews.com/
39. n/a | 11/21/2021 17:54:13 | https://www.bing.com/newtabredir?url=https%3A%2F%2Fwww.nbcnews.com%2F
40. n/a | 11/21/2021 17:57:27 | https://www.bing.com/newtabredir?url=https%3A%2F%2Fwww.cnn.com%2F
41. CNN - Breaking News, Latest News and Videos | 11/21/2021 17:57:27 | https://www.cnn.com/
42. n/a | 11/21/2021 18:00:33 | https://www.bing.com/newtabredir?url=https%3A%2F%2Fabcnews.go.com%2F
43. ABC News – Breaking News, Latest News, Headlines & Videos - ABC News | 11/21/2021 18:00:34 | https://abcnews.go.com/

44. https://www.bing.com/search?q=news&cvid=5b6fa467060a443d88ffe736905bde5c\&aqs=edge..69i57j0l4j69i60l4.1971j0j4\&FORM=ANAB01\&PC=U531 | 11/21/2021 18:07:12 | https://www.bing.com/search?q=news&cvid=5b6fa467060a443d88ffe736905bde5c\&aqs=edge..69i57j0l4j69i60l4.1971j0j4\&FORM=ANAB01\&PC=U531
45. n/a | 11/21/2021 18:07:12 | https://www.bing.com/newtabredir?url=https%3A%2F%2Fnypost.com%2Fnews%2F
46. New York Post – Breaking News, Latest US & World Headlines | 11/21/2021 18:07:12 | https://nypost.com/news/
47. n/a | 11/21/2021 18:08:27 | https://www.bing.com/newtabredir?url=%3A%2F%2Fmoney.cnn.com%2Fdata%2Fmarkets%2F
48. Stock Market Data - Dow Jones, Nasdaq, S&P 500 - CNNMoney | 11/21/2021 18:11:48 | https://money.cnn.com/data/markets/
49. https://www.bing.com/search?q=stock&qs=n&form=QBRE&sp=-1&pq=stock&sc=8-5&sk=&cvid=5209CCE60D7448CB9FB5488184E0944B | 11/21/2021 18:12:50 | https://www.bing.com/search?q=stock&qs=n&form=QBRE\&sp=-1\&pq=stock\&sc=8-5\&sk=\&cvid=5209CCE60D7448CB9FB5488184E0944B
50. Stock Market Data with Stock Price Feeds | Nasdaq | 11/21/2021 18:12:50 | https://www.nasdaq.com/market-activity/stocks
51. n/a | 11/21/2021 18:12:50 | https://www.bing.com/newtabredir?url=https%3A%2F%2Fwww.nasdaq.com%2Fmarket-activity%2Fstocks

References

1. Riley, T.: The cybersecurity 202: Cybercrime skyrocketed as workplaces went virtual in 2020, new report finds, February 2021 (2021)
2. Brooks, C.: Alarming cybersecurity stats: what you need to know for 2021. Forbes, March 2021 (2021)
3. Staff, D.: Data breach costs: calculating the losses for security and it pros, February 2021 (2021)
4. Gill, M.: 10 shocking data loss and disaster recovery statistics, August 2021 (2021)
5. Nabity, P., Brett, L.: Recovering deleted and wiped files: a digital forensic comparison of FAT32 and NTFS file systems using evidence eliminator, no. 2007, pp. 1–10 (2009)
6. Lazaridis, I., Arampatzis, T., Pouros, S.: Evaluation of digital forensics tools on data recovery and analysis. In: The Third International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM2016), p. 67 (2016)
7. Buchanan-Wollaston, J., Storer, T., Glisson, W.: Comparison of the Data Recovery Function of Forensic Tools, pp. 331–347 (2017). To cite this version: HAL Id: hal-01460614
8. Microsoft by the numbers windows devices. https://news.microsoft.com/bythenumbers/en/windowsdevices. Accessed Oct 2021
9. Alsop, T.: Shipments of hard and solid state disk (HDD/SSD) drives worldwide from 2015 to 2021, March 2020 (2020)
10. Magnet forensics. https://support.magnetforensics.com/s/. Accessed Oct 2021
11. Another set of amazing wins at the 2021 forensic 4:cast awards! Magnet Forensics Blog (2021)

12. Autopsy. https://www.autopsy.com/. Accessed Oct 2021
13. Jones, J.H., Khan, T.M.: A method and implementation for the empirical study of deleted file persistence in digital devices and media. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–7 (2017)
14. Khan, T.M.: Identifying factors affecting deleted file persistence through empirical study and analysis. Ph.D. thesis. George Mason University (2017)
15. AllisonShen. security_mft (2021). https://github.com/
16. Aggarwal, K., Garg, S.K.: Computer forensics: data recovery perspective over Windows and Unix, vol. 6, no. 8, pp. 6–8 (2021)
17. Duan, R., Zhang, X.: Research on computer forensics technology based on data recovery. J. Phys.: Conf. Ser. **1648**(3), 032025 (2020)
18. Cankaya, E.C., Kupka, B.: A survey of digital forensics tools for database extraction. In: FTC 2016 - Proceedings of Future Technologies Conference, December, pp. 1014–1019 (2017)
19. Al-Sabaawi, A., Foo, E.: A comparison study of Android mobile forensics for retrieving files system. Ernest Foo Int. J. Comput. Sci. Secur. (IJCSS) **13**, 2019–148 (2019)
20. Ultimate boot CD [software]. https://www.ultimatebootcd.com/. Accessed Oct 2021
21. DBAN, hard drive eraser & data clearing utility. [software]. DBAN Hard Drive Eraser & Data Clearing Utility. https://dban.org/. Accessed Oct 2021
22. Robertson, A.: [Software], September 2018. https://gist.github.com/alirobe/7f3b34ad89a159e6daa1file-reclaimwindows10-ps1. Accessed Oct 2021
23. Ftk imager. [software]. https://accessdata.com/. Accessed Oct 2021