Data Recovery and Digital Forensics Analysis for Flash Drive

Solo Author: Manichandra Ajit Aarya Kankipati
Computer Science. Old Dominion University
Norfolk, Virginia, United States
Email : mkank001@odu.edu

***Abstract*—Data is saved on a broad range of devices in the present day, which means it is also removed from a large variety of devices. Data storage disks are extremely prone to damage and failure. With typical use, many conventional hard drives die in less than a decade. Overheating and power surges are also major causes of damage. Data recovery from physically damaged or degraded storage devices necessitates the use of specialized techniques and abilities. Forensic Data Analysis (FDA) is a discipline of digital forensics that evaluates structured data in relation to financial crime situations. The goal is to identify and analyze patterns of fraudulent activity. This study provides a method for forensically examining flash memory and recovering data from it using market-available technologies.**

***Index Terms*—Digital Forensics, Data integrity, Data recovery, Memory, Forensics, Investigating**

I. Introduction

Nowadays, the use of portable digital devices is increasing at an exponential rate, paralleling the expansion of consumer electronics. Flash memory technology, particularly USB devices or Pen Drives, has dominated non-volatile storage and access. The electronic device USB flash drive forensics and pen drive forensics tools are useful in the study of embedded systems, which primarily involves the extraction of data on a logical level. The USB interface is one of the most widely used protocols for connecting devices to computers. This is a plug-and-play connection, which means that devices connected to the USB "broadcast" their presence to the computer so that it may setup them without any user input. The forensic investigation begins with data collecting methods of flash memory devices employing several ways.

It is not always feasible to recover all data from a storage device via logical data capture. Deleted data, for example, but also data that is not immediately relevant to the user, cannot be collected, and potentially important information may be ignored. As a result, data collection is desired at the lowest tier where evidence may be expected. It is typical practice for hard disk-based storage media to transfer all bytes from the source storage device to a target storage device and then do analysis on this copy. Advanced data recovery software is used by digital forensic investigators to retrieve data that suspects attempted to conceal. While criminals may initially save damning material on their computers or mobile devices, they may erase or conceal this data if they feel they are being observed by law authorities.

This research proposes a way to forensically examine flash memory and also to recover data from it by using different tools that are available in market.

II. Background

Like all technology, USB has evolved over time. Despite being a "Universal" Serial Bus, it has generated many variants with varying connection rates and a plethora of cables in its 18-or-so years on the market. With USB 2.0, USB truly matured, and USB 3.0's increased speed to 5Gbps has made it even more beneficial for all of the use cases stated above—it takes less time to do system backups or transport large video files around, and it alleviates a bottleneck for 802.11ac or gigabit Ethernet connections. It's extremely easy to run full operating systems from USB 3.0 hard drives or flash drives, which is especially beneficial when troubleshooting a machine or recovering data from it. USB ports are sometimes the sole ports offered in laptops, particularly now that Wi-Fi has decreased the necessity for specialized Ethernet connectors. The interface's ubiquity ensures compatibility from all major chipmakers, from Intel to Qualcomm to AMD.

Digital forensics is a branch of forensic science that focuses on locating, obtaining, processing, analyzing, and reporting on electronically stored data. Electronic evidence is present in practically all illegal acts, and digital forensics assistance is critical for law enforcement investigations. Computers, cellphones, remote storage, unmanned aerial systems, ship-borne equipment, and other devices can all be used to gather electronic evidence. The primary purpose of digital forensics is to collect data from electronic evidence, convert it into actionable information, and submit the results for prosecution. To guarantee that the findings are acceptable in court, all processes employ good forensic methodologies.

III. Tools

A. Autopsy

Autopsy is the leading open source digital forensics platform that is simple to use, rapid, and applicable in any computerized test. It examines hard disks, smart phones, media cards, and other devices. It is primarily designed for Microsoft Windows, however there is some support for Linux and macOS. Autopsy is a free and powerful hard drive investigation application that includes capabilities such as multi-user cases, timeline analysis, registry analysis, keyword search,

email analysis, video playback, EXIF analysis, malicious file detection, and much more.

B. FTK Disk Imager

FTK Imager is an open-source software program developed by AccessData that is used to create accurate copies of original evidence without altering it. The image of the original evidence remains unchanged, allowing us to copy data at a much faster rate, which can be quickly stored and evaluated further. The FTK imager additionally has an integrity testing function that creates a hash report that aids in comparing the hash of the evidence before and after making the image of the original Evidence.

C. Puran File Recovery

Puran File Recovery helps restore deleted/lost files/partitions. Files can also be retrieved from formatted hard drives. Almost any disk that Windows detects as a drive may be inspected, regardless of its file system. Whether it's hard disks, pen drives, memory cards, mobile phones, CDs, DVDs, or any other type of storage medium.

D. Recuva

Recuva is one of the most effective free file recovery software programs accessible. It's as simple to use as any other freeware or paid file recovery tool on the market. It is available in both installable and portable formats. It has a basic wizard as well as complex features, and it works with a variety of Windows operating systems. It is compatible with Windows 10, 8.1, 7, Vista, and XP.

IV. Approach

The approach is clear for recovering data by using digital forensics. After connecting the USB to the system, The USB needs to format. Performing different tools on the formatted disk to obtain all the data which was formatted will be successful after following all the steps explained in the Experimentation module.

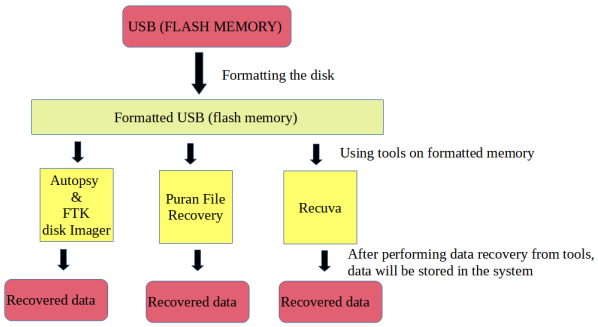

Fig. 1. Approach model data recovery from USB

V. Experiment Design

In the modern day, data is stored on a wide variety of devices, which means it is also deleted from a wide variety of devices. When someone engages in illegal activity, whether at work or in their personal life, it is usual for them to go out of their way to erase any proof of such behavior. In such circumstances, the data is frequently not simply erased, but further steps are taken to totally cleanse the storage device of the data. Such attempts may involve reformatting a hard disk, repeatedly rewriting fresh data over old data, or even purposefully harming the storage device. Computer Forensics Resources is aware with these techniques and can typically retrieve data that has been destroyed on purpose.

After analyzing the recovered data from different tools, we will categorize which tool is efficient by checking its data integrity. As we are using four different tools, there's three ways of recovering data from autopsy, FTK disk imager, recuva and puran file recovery tool. Every step of performing the project explained with the help of screenshots. First, I performed the process with the help of autopsy and FTK disk imager and later, I also used recuva tool for performing same operation. And at last, I performed the experimentation with the help of puran.

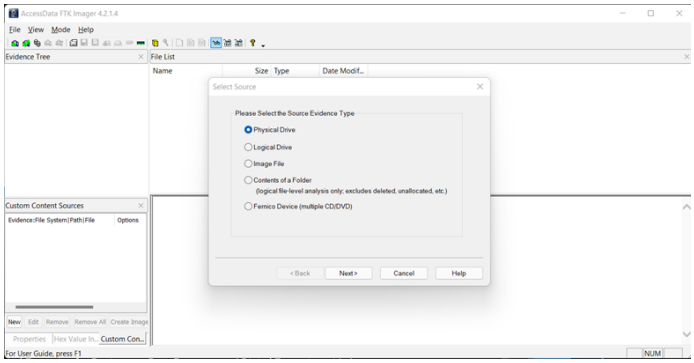

Fig. 2. Creating disk image and giving needed details for the process

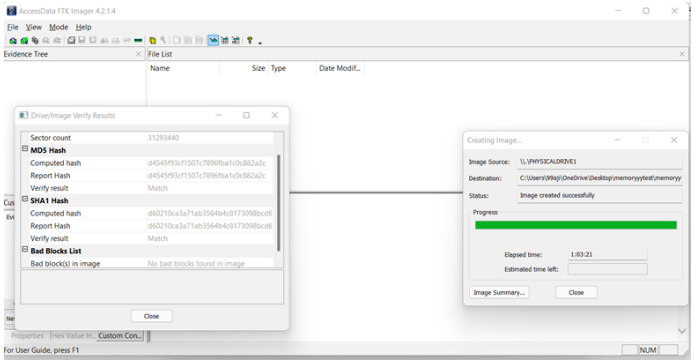

Fig. 3. FTK disk image output

For Autopsy, there's a chance of needing disk image for experimentation. With the help of FTK disk imager, it is easy to create a disk image file. After creating and storing them in

autopsy tool for analyzing, it gives all the files that are stored throughout its lifetime.

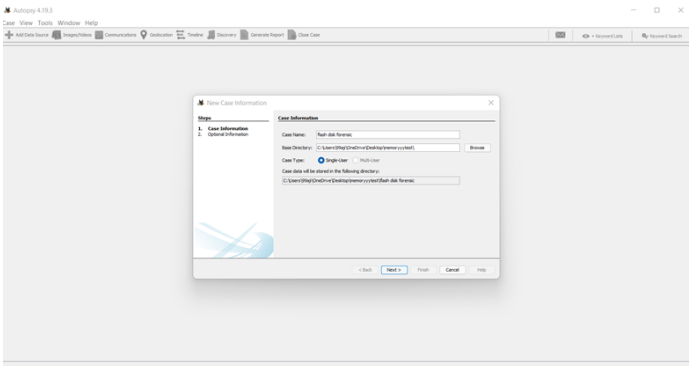

Fig. 4. Autopsy: Uploading disk image to autopsy for performing data recovery

And with puran file recovery and recuva, we can analyze all the files that are stored throughout its lifetime in the drive. Those recovered files from the tools are also stored in PC for the research and for analysis. In puran and recuva, Deep scan plays a major role. In Puran, Normal scan can only obtain some files, but deep scan will give every data file that once stored in the Flash disk in it's lifetime.

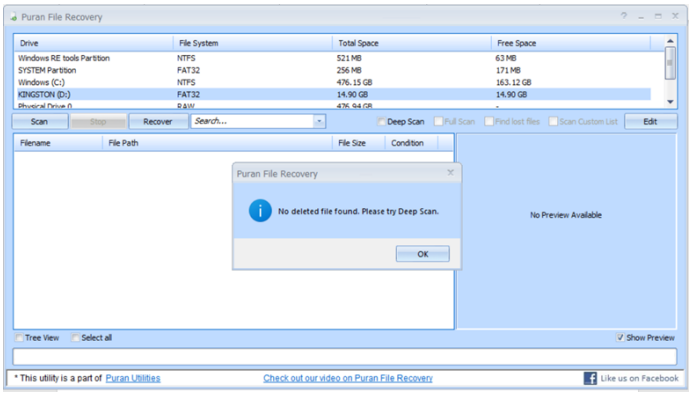

Fig. 5. Puran: Deep scan will find results that are not found by normal scan

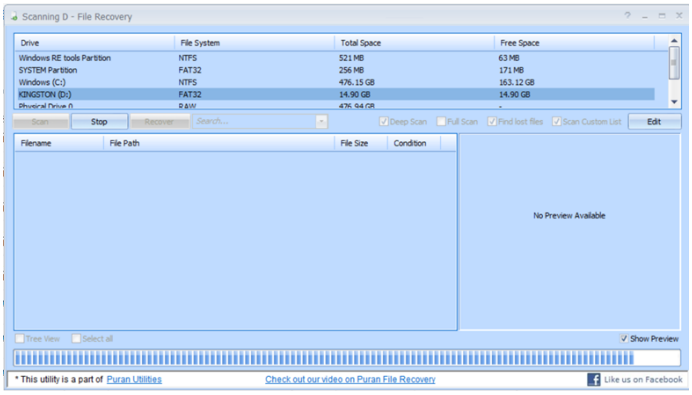

Fig. 6. Puran: Deep scanning the USB

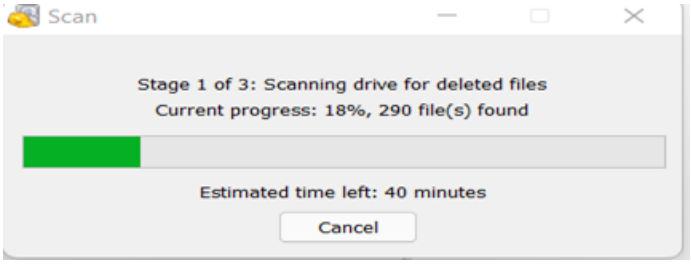

Fig. 7. Recuva: Performing Recuva

VI. Results

After experimenting with the formatted flash drive with these tools, All the files which are stored once in that flash drive are available to recover. All these tools work differently but they all give data files for analysis. An autopsy is the most well-known tool for performing digital forensics and it will also report the case professionally.

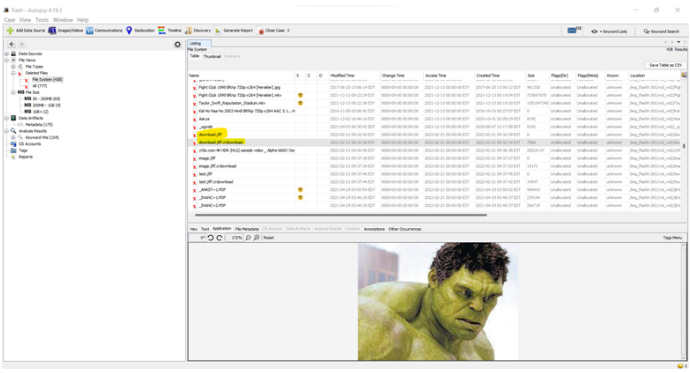

Fig. 8. Autopsy: All the data files which are previously stored in the formatted USB are available to recover

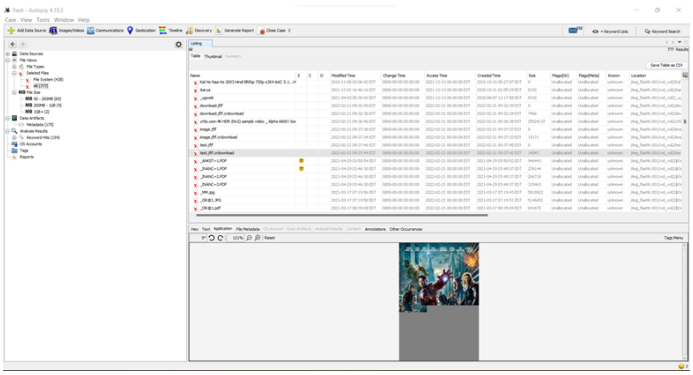

Fig. 9. Autopsy: Some of the Data has been compromised

Here, Some of the data files have been compromised which means they have less data integrity. And for the experimentation, I used a Kingston Flash disk with the FAT32 file system which is meant to be a memory of 16GB but the actual memory size of it is 14.90GB because the remaining memory will be maintained for system files.

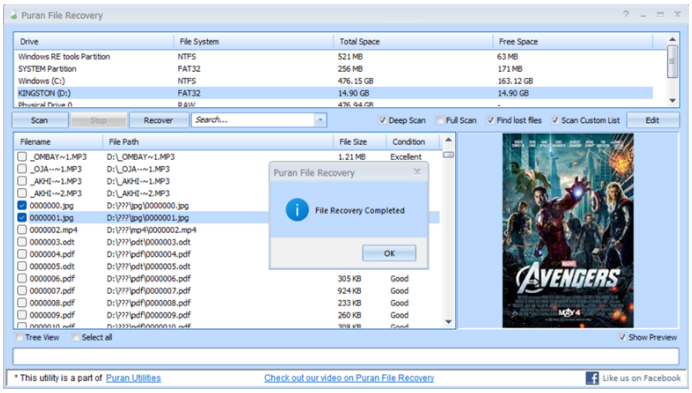

Fig. 10. Puran: All the data files which are previously stored in the formatted USB are available to recover

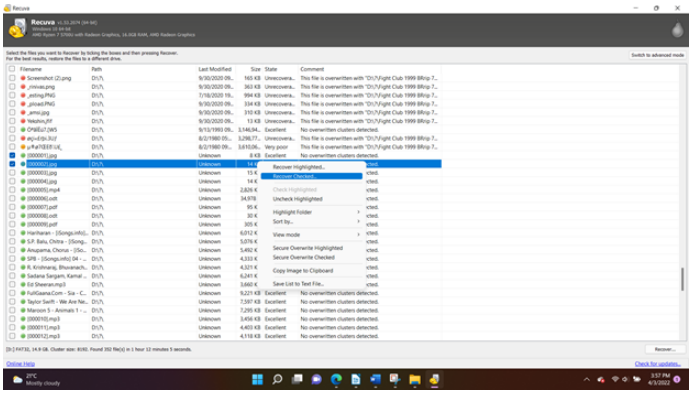

Fig. 11. Recuva: All the data files which are previously stored in the formatted USB are available to recover

Deleted files count from the tools is 438, 352 and 415 which are from Autopsy, Recuva, and Puran respectively. The time take for performing this process for every tool is minimum of 60 min for 14.90GB flash disk.

Tool	Time	Deleted files count
Autopsy	65 Minutes	438
Puran	70 Minutes	415
Recuva	72 Minutes	352

Fig. 12. Comparing tools performance

The time taken for completing the entire process from different tools is 65 minutes, 70 minutes, and 72 minutes for Autopsy, Puran, and Recuva. From this, We know that autopsy is taking less time and Recuva taking more time to complete the data recovery process. And also the output files which are recovered from these tools are having original file sizes.

VII. Summary

Data recovery is the process of recovering data from media that has been corrupted or physically destroyed. This procedure might be rather costly. Hard drives, for example, may be destroyed by water or fire, compact discs may have their reflective surfaces scratched, and USB drives may have their connections physically broken. Data recovery from damaged media frequently involves the dismantling of the media and repair of damaged sections. Furthermore, data might become unrecoverable by the user if it has been damaged in any way. Data recovery professionals can occasionally locate and restore the data.

For one case, a user mistakenly removed files from a storage media. Typically, the contents of deleted files are not instantly wiped from the physical disk; instead, references to them in the directory hierarchy are removed, and the space used by the deleted data is made available for subsequent data overwriting. End users believe that deleted files cannot be found using a typical file manager, while the erased data actually persists on the physical drive. Meanwhile, the original file contents are preserved, frequently in a series of unconnected pieces, and may be recovered if not overwritten by other data files. Hard disks that have been logically damaged, which indicates that the data has been corrupted or accidentally erased. When it comes to logically damaged hard disks, someone with computer experience can download software and do the recovery themselves by following the instructions, however certain applications can actually be worse for your computer's hard drive and cause you to lose everything forever. This software only works with logically damaged hard disks, which implies that the machine is still operational; you only have a deleted or corrupt file or files.

VIII. Conclusion

Most data recovery applications use metadata analysis methods, the raw recovery method based on known file content, or a mix of the two ways. Metadata is information about hidden services that is stored in the file system. Its examination enables the software to find the primary structures on the storage that maintain track of the location of files, their contents, their attributes, and the directory hierarchy. This data is then analyzed and used to repair the damaged file system.

This approach is preferable to raw recovery since it enables for the recovery of files with their original names, directories, date and time stamps. If the information was not severely distorted, it may be feasible to recreate the complete folder structure, depending on the characteristics of the file system's procedures for removing unneeded entries.

This study provides digital forensics testing with several tools to compare which is better for data recovery. According to the results, Autopsy is a more powerful tool for digital forensics, particularly data recovery, since it detects 438 lost system files and a total of 777 files in 65 minutes. Puran file recovery and Recuva both required a minimum of 70 minutes to process 415 and 352 data files, respectively. However, Autopsy has low data integrity since data from one of the outputs is corrupted. Some data files are lost in data integrity as it takes less time and detects more files. All of the recovered data files have the same memory size, which is also the same

as the original file before formatting. After recovering from the tools, the memory size may be lowered. Because we were looking for a photo with a size of 14KB, the recovered data files are similarly 14KB in size. Regardless of device failure or damage, data recovery is always a top priority. Future forensic techniques may be able to increase the power and efficiency of flash drives as a result of the findings of this study.

REFERENCES

[1] Breeuwsma, Marcel Jongh, Martien Klaver, Coert Knijff, Ronald Roeloffs, Mark. (2007). Forensic Data Recovery from Flash Memory. Small Scale Digital Device Forensics Journal. 1.

[2] S. Tomer, A. Apurva, P. Ranakoti, S. Yadav and N. R. Roy, "Data recovery in Forensics," 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), 2017, pp. 188-192, doi: 10.1109/IC3TSN.2017.8284474.

[3] Q. Yao and C. Gu, "Research and Implementation of Data Recovery Technology Based on WINDOWS FAT," 2010 International Conference on Machine Vision and Human-machine Interface, 2010, pp. 549-552, doi: 10.1109/MVHI.2010.214.

[4] M. A. Caloyannides, N. Memon and W. Venema, "Digital Forensics," in IEEE Security Privacy, vol. 7, no. 2, pp. 16-17, March-April 2009, doi: 10.1109/MSP.2009.34.

[5] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," in IEEE Access, vol. 10, pp. 11065-11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[6] A. K. Shrivastava, N. Payal, A. Rastogi and A. Tiwari, "Digital Forensic Investigation Development Model," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 532-535, doi: 10.1109/CICN.2013.115.

[7] A. Jones, S. Vidalis and N. Abouzakhar, "Information security and digital forensics in the world of cyber physical systems," 2016 Eleventh International Conference on Digital Information Management (ICDIM), 2016, pp. 10-14, doi: 10.1109/ICDIM.2016.7829795.

[8] M. Alhussein, A. Srinivasan and D. Wijesekera, "Forensics filesystem with cluster-level identifiers for efficient data recovery," 2012 International Conference for Internet Technology and Secured Transactions, 2012, pp. 411-415.

[9] L. A. Herrera, "Challenges of acquiring mobile devices while minimizing the loss of usable forensics data," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116458.

[10] P. Dibb and M. Hammoudeh, "Forensic Data Recovery from Android OS Devices: An Open Source Toolkit," 2013 European Intelligence and Security Informatics Conference, 2013, pp. 226-226, doi: 10.1109/EISIC.2013.58.

[11] S. Žulj, D. Delija and G. Sirovatka, "Analysis of secure data deletion and recovery with common digital forensic tools and procedures," 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), 2020, pp. 1607-1610, doi: 10.23919/MIPRO48935.2020.9245197.

[12] P. Ravindra, R. Kalal, Soumya and V. Mandal, "Logical data recovery technique for USB devices," 2013 International Conference on Emerging Trends in Communication, Control, Signal Processing and Computing Applications (C2SPCA), 2013, pp. 1-6, doi: 10.1109/C2SPCA.2013.6749447.

[13] G. C. Kessler, "Advancing the Science of Digital Forensics," in Computer, vol. 45, no. 12, pp. 25-27, Dec. 2012, doi: 10.1109/MC.2012.399.

[14] N. A. Aziz, M. S. M. Yusof, M. H. B. A. Malik, A. Rasyad Hanizam and L. H. Abd Rahman, "Acquiring and Analysing Digital Evidence - a Teaching and Learning Experience in Class," 2018 Cyber Resilience Conference (CRC), 2018, pp. 1-4, doi: 10.1109/CR.2018.8626819.

[15] C. Yang and P. Yen, "Fast Deployment of Computer Forensics with USBs," 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, 2010, pp. 413-416, doi: 10.1109/BWCCA.2010.106.