Data and Device Recovery Using Forensic Tools and Practices

ISSC458 – Digital Forensics: Investigating Data and Image Files

APUS University

Corbin Osman

Brian Burnett

02/19/2023

In today’s age of technological advances there are large amounts of data and information constantly being transmitted and stored around the world. Much of this data contains personal and confidential information, whether it belongs to a business, an organization, or an individual person. The consequences could prove to be negative if this information were to be lost, stolen, or misused, which is why there are many efforts focused on the recovery of digital information.

One field that works to recover lost or deleted information is the field of digital forensics. In forensics, the goal is to find evidence that can help to provide insight into a scenario or incident, such as finding proof that an individual was involved in a recently committed crime. With technology being a large part of our everyday lives there is a lot of information recorded and stored about our interactions in the digital world, a few examples being the messages and emails we send, the picture or videos we take and share, and the things we may purchase online. Forensic investigators are able to search for these interactions, including those that may have been deleted or lost, and understand how an individual or group has used technology.

This paper will focus on and explore the recovery of data and information through the use of forensic tools and practices. First, we will look at the uses of data and device recovery and why they are important for a forensic investigator or examiner. Second, we will explore different types of digital data that one may want to recover and following a few data recovery examples will be shared. In the next section we will continue looking at additional data that can be recovered in the form of a drive or partition that may have been lost, deleted or damaged. In the final two sections we will explore some tools that are available for use in data recovery across different operating systems along with strong practices to develop and employ in forensic data recovery.

**The Importance of Data and Device Recovery in Forensics**

Knowing how to recover data and information that may have been deleted, lost, or stolen can be useful for anyone who utilizes technology. For the everyday user it can be common to delete a message, a photo, or a file and then later realize that you wanted to keep it. Understanding how to find and recover this data can be useful for personal benefit as well as for those working in the field of data recovery.

The act of recovering data and information, whether lost, stolen, or deleted, has proven to be useful in many situations. One such scenario is following the loss of a system that contained important information and data. While a common method to prevent loss of data in this instance is through regular backup creation, this is not always performed and may not be able to recover one hundred percent of the information that was lost. Another scenario is following natural or electrical disaster, such as a power outage or tornado. Both these and other disasters can result in systems and information being damaged or lost entirely, and knowing how to quickly recover from these catastrophes can be invaluable to businesses. A final scenario to consider is data that is damaged or stolen by an attacker. It is important that businesses and corporations have strong security measures in place to prevent and mitigate loss from attacks, though a plan and process for recovery should also be prepared if prevention is not successful.

Shifting the focus to forensics and crime, there are many reasons an investigator may work with recovering data. For forensic investigators, searching for and locating data that can be used as evidence is important to be able to understand what the data proves. Deleted or lost data can provide a lot of information, such as who last viewed or modified the data, who it may have been shared with, and the contents of the data itself. This knowledge can help law enforcement know how an individual or group may be affiliated with a crime in question and provide the evidence needed to convict them of having committed the crime.

When this data is recovered through forensic operations, it is important that processes and evidence be handled appropriately. Arkady Bukh shares a few points to consider in regard to data recovery in the forensic field. For starters, the evidence needs to be admissible. This requires investigators and examiners to thoroughly document all actions taken during the time a piece of digital evidence is handled so that its integrity can be proven. Similarly, it can be beneficial to form a timeline of events, or a reconstruction of the events that took place, to show what actions were performed, when they occurred, and what effects they had. Finally, ensuring that the evidence collected and presented is of high quality will help to ensure that the conclusions reached will be understood and made clear by the evidence shown (Bukh).

With a better understanding of what data recovery is and how it is important to forensic investigators, let us now look at the different types of data one may want to recover and some scenario examples.

**File and Data Types in Data Recovery**

As technology has advanced, so have the number of different data and file types we interact with and utilize on our technological devices. Whether they be text messages, email communications, photos, videos, word documents, or any other type of digital media, all files consist of data that can prove useful to users and investigators alike. Modern systems help to make recovery of this information a simple task should a file or communication be deleted by relocating it to a location commonly referred to as “trash” or the “trash / recycling bin”. For some services such as email accounts, this information is held for a period after deletion, such as a month, where it is then removed from the account and inaccessible to the user. No matter when or how data is deleted, it is almost always recoverable through tools and forensic procedures.

In the field of digital forensics, it is important to recognize what types of files and data one should search for and attempt to recover. Common types of digital evidence that investigators will search for are communications between parties such as text messages or emails, audio, photo or video files that allow investigators to hear or see what occurred during an event, and documents or files that contain confidential and sensitive information. All of these types of files and data can help investigators better understand the five W’s of a scenario, such as who was involved, why was a crime committed, and when and where it occurred.

While this information can be found easily and quickly at times, evidence may have been deleted or destroyed intentionally by the imposing party to hide their involvement in the incident. Knowing what data to look for can now allow us to start searching for digital evidence.

**The Process of Data Recovery**

Forensic investigators have many tools and techniques at their disposal to search drives and devices for data that may have been deleted, lost, or stolen. Exploring three example scenarios will help us understand how data is recovered by investigators.

For the first scenario, we will suppose that an important document file containing evidence of employee confidential information has been erased from a hard drive. An investigator would begin by creating a backup of the data and working on this copy to ensure the original evidence is not affected in any way. The investigator could then look through the contents of the hard drive to see if there are any currently remaining data files that could be used as evidence. If the suspect document is not found on the drive, the investigator can then turn to a data recovery software, such as Recuva or Disk Drill, and scan the hard drive for data that may have been deleted. If all goes well, the data recovery software should be able to locate the document and allow the investigator to restore it to its original state, then allowing it to be reviewed in order to determine if it did in fact contain the alleged employee information.

The second scenario involves recovering data that appears to have been corrupted in some way. Joel Lockard shares a process to recover corrupted files, and states that file corruption can occur when the computer system structure is damaged or interrupted. Some common occurrences of this are through power outages, power surges, and computer crashes (Lockard, 2021). After the same steps of backing up and working on a copy of the data there are a few techniques that can be attempted for recovering corrupted data. For one, an investigator can check the file integrity though utilizing the Chkdsk utility on a Windows system. For Windows and other systems that regularly create backups of data an investigator can attempt to restore the data from the backup to a previous functioning state. An alternative solution can be to use repair software such as Repair Toolbox to help fix the corrupt state of certain files (Lockard, 2021).

For the final scenario we will look at recovering text message or email communications that may have been deleted. A common source for these files is a mobile device such as a smartphone, which often houses hundreds of different communications. Similar to the previously explored techniques one may be able to restore their phone to a previous state where the deleted communications can then be read. When this is not possible, other methods may be of use to locate and recover the information. Data and files that are deleted normally remain stored in the drive found on the device, but they become hard to find as the system does not have a link pointing to where the data is after deletion. Through manually searching or using tools and software that automatically scans and searches for information, these text and email communications can too be recovered and of use to forensic investigators.

With an understanding of how data and files can be recovered following deletion or corruption, let us now look at how the devices and drives that house this data can also be recovered in the instance of drive and partition deletion or damage.

**Recovery of Drives and Partitions**

All technological devices utilize some sort of file storage system. These are commonly referred to as drives, such as the hard drive you might find inside of a PC. On these drives one can have multiple storage areas, or partitions as they are often known. Within the drives and partitions, you will find most of the data that resides on a system. As with all technology, there can come a time when these drives or partitions experience issues or are damaged, lost, or stolen. Seeing as they contain a lot of important system information and data, it is valuable to know how to recover drives and partitions and the data they house.

There are many scenarios where it may become necessary to attempt to recover a drive or partition and its data. An article on partition data recovery by Jyoti Prakash helps us understand ways to go through the recovery process along with reasons it may be needed. The author shares that partition loss is usually caused by human error, though it can occur on its own as well. Partition table loss or damage can be caused by power outages, virus attacks, and other issues and make it difficult to view and create new partitions. Partition issues can also arise by cause of virus or malware attacks, which can be designed to target partition tables or the partitions and drives themselves. Each of these, on top of the possibility of human error, can cause problems with partitions and drives and require work to be done to restore them to their prior working state.

Prakash offers several suggestions and practices to employ when attempting to recover damaged or deleted partitions. First, it is important to stop using the drive or partition and the system it is located on to ensure no further damage is done. Second, you can attempt to run system operations, such as Chkdsk for Windows operating systems, to check the status of a partition and fix any potential issues. If there is no apparent progress being made, one can turn to recovery software that is designed to recover partitions and their data. Tools can be used to scan the damaged partition for the data it contains or previously contained, and while it may not be possible to fully restore the partition one may be able to restore much of the data it had contained (Prakash, 2023).

**Tools and Software for Data Recovery**

There are many different tools and software at our disposal that can be used to aid in the recovery of data and information. These have been designed to help make the data recovery process quick and simple with easy to follow prompts and good system interfaces that allow users to understand the process and see all of the data being recovered.

Within the Windows Operating System there are several software that can be used to help recover lost or deleted data and information. EaseUS Data Recovery Wizard is software that is easy to use for all users and provides a wizard that guides the user through the recovery process. Ontrack Easy Recovery is software that can be of great benefit to both home and business interactions, as it is great at recovering data that may have been deleted or damaged by viruses or malware. Recuva is software that offers a lot of helpful tools, such as being able to scan removable drives and creating backups of disk images (Lishchuk, 2023).

For Mac Operating Systems, there are many similar software that work the same as other data recovery software. Cisdem data recovery is easy to use for all system users and offers features such as different scan types and the ability to search for and restore over two hundred different file types. Disk Drill is a more advanced recovery software that offers a large variety of tools one may need to extensively search for and recover data. Disk Drill also happens to have a Windows counterpart, so those familiar with the Mac software can find similar success in using the Windows version (Henline, 2023).

Linus Operating System users have the bonus of having access to natively built-in recovery tools. These are often found on the operating system and used through a command line interface allowing for quick and easy data recovery. Among these are a few notable tools, namely TestDisk, PhotoRec, and Foremost. TestDisk allows for easy partition recovery and helps to re-build information and data such as the partition table. PhotoRec, which was created by the same company that helped to make TestDisk, makes the recovery of images and other graphic style data simple and quick. Foremost comes pre-installed on the Linux distribution Kali Linux, but can be installed on other distributions as well, and offers data retrieval for multiple file type formats (Ninad, 2022).

**Conclusion**

No matter what type of data or information needs to be recovered, it is important to follow steps and procedures to ensure that data and devices are kept as intact as possible. Forensic investigators can find a lot of success in utilizing the many tools available to aid in recovery of data that has been deleted or damaged, which in turn allows for evidence to be found that can show one’s involvement in a particular incident. Studying and learning how to use the tools and software available will allow all users, whether working in the field of forensics or not, to better understand what occurs when data is deleted or damaged and what can be done to restore it to a previous state.

Resources

Bukh, A. (n.d.). Data Recovery and Forensic Analysis. *Cybersecgroup.info*. http://cybersecgroup.info/incident-response/computer-forensics/data-recovery-and-forensic-analysis

Henline, J. (2023, January 9). The Best Mac Data Recovery Software 2023 for Every Kind of User. *Cisdem.com*. https://www.cisdem.com/resource/best-data-recovery-software-mac.html

Lishchuk, R. (2023, January 5). 10 Best Windows Data Recovery Software 2023. *Stellarinfo.com*. https://www.stellarinfo.com/article/windows-data-recovery-software.php

Lockard, J. (2021, December 22). How to Recover Corrupted Files on Windows. *7DataRecovery.com*. https://7datarecovery.com/blog/recover-corrupted-files/

Ninad. (2022, August 3). Top 20 Best Linux Data Recovery Tools to Recover Deleted / Corrupted Files. *Digitalocean.com*. https://www.digitalocean.com/community/tutorials/top-best-linux-data-recovery-tools

Prakash, J. (2023, January 6). How to Recover Data from Deleted Partition. *Stellarinfo.com*. https://www.stellarinfo.com/blog/recover-data-with-deleted-partition-recovery-software/