Data Recovery Plan

Joshua Lopez

California Lutheran University

Digital Forensics IT-540

Wayne Snyder

January 15, 2025

Data Recovery Plan

When planning to recover data, it is strongly recommended that you have in-depth/specialized knowledge of the operating system to prevent further data damage/loss. Other considerations include cost, time of recovery, drive type and speed, and storage capacity, to name a few ((IT Asset Mangement Group [IT AMG], n.d.)). Best practices emphasize the critical importance of regular and frequent backups in an effort to minimize data losses. However, deleting unnecessary files on linux OS, such as logs, temp, and other unneeded files, is considered a maintenance task on a linux OS ((IT AMG, n.d.)). Accidental deletion, unauthorized, or deletion with malicious intent is not. For this type of incident, you need a Data Recovery Plan. It is important to note that a process may not work for your distribution due to the many Linux distributions.

Many types of users create data from the casual to CEOs of Corporations. One significant difference is that specific data can be mission/systems critical for a small business owner or CEO. Securing the availability of data is a high priority. Although there typically are built-in recovery tools, access to reliable data recovery software is the best practice to mitigate accidental data loss (Acronis, 2024). My experience with this report leaned more toward command-line tools. However, it was pleasant and efficient to work with robust applications. I prefer a command line as I seem to have more control(or illusion of) over the step-by-step process. Having this knowledge also carries over to the use of robust applications. If something goes wrong, it is crucial to understand what is going on underneath the hood. Cost saving is another benefit, as professional recovery services can be costly, depending on the loss/damage. Significantly, recovery isn’t 100% guaranteed when recovery depends on the loss scenario. For those with mission-critical data, it is a hard pill to swallow.

Recovery Plan

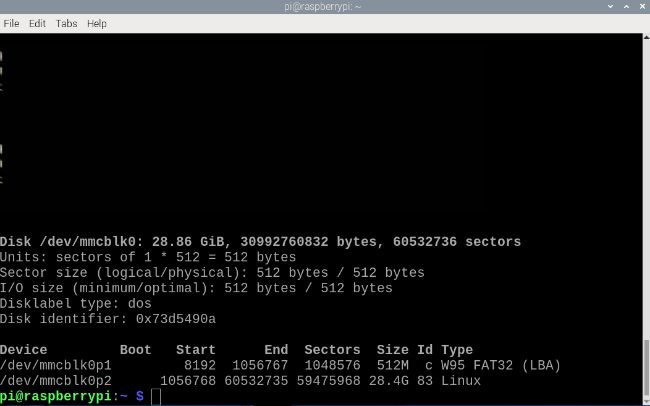
1. Linux: Recovery (IT AMG, n.d., Linux: Recover Using Terminal section)
   1. List Drives – View the structure to see what we are working with
      1. Command(s)
         1. lsblk
            1. Quick layout of drives – partitions – mount points
         2. fdisk -l
            1. Manage – Partitioning – View disk/partition size/file system type
2. Create A Snapshot
   1. Investigators should handle original data as little as possible.
      1. Make two copies. One to work with and the other as a backup
         1. Reasoning: Locard’s Principal Of Transference (Easttom, 2021, p. 66)
            1. Each time you touch the original data, there is a chance of altering it
   2. Forensic Imaging (Easttom, 2021, pp. 109–110)
      1. Forensically wipe the target drive you are going to copy the suspect drive to
         1. Sample Command
            1. dd if=/dev/zero of=/dev/hdb1 bs=2048

This command will overwrite everything on target with null values

* 1. Set Up Forensic Server To Listen For Copy
     1. Sample Command
        1. nc -l -p 8888 > evidence.dd
           1. Netcat command setup listen with “l” flag and port “p” flag, receives copy and writes it to evidence.dd file
  2. Bit Level Copy
     1. Sample Command
        1. dd if=/dev/hda1 | nc 192.168.0.2 8888 -w 3
           1. Run on the suspect machine to make a bit-level copy, output to netcat command, which then sends bits over the network to forensic computer

1. Data Recovery (Alibaba Cloud, n.d., Restore accidentally deleted data section)

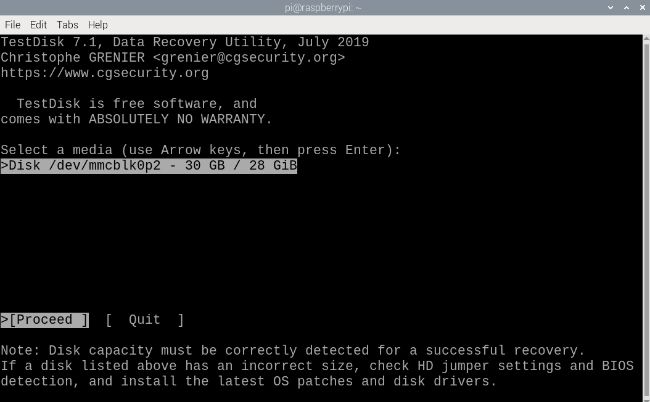
Figure 1  
  
Partitions View



*Note.* Disk mmcblk0 has two partitions. We will use the /dev/mmcblk0p2 partition.

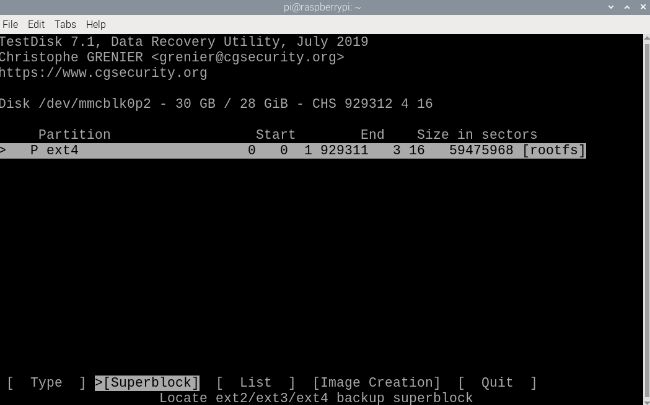
* 1. Linux Command Line Tool – Recover Data
     1. Command: sudo apt install -y testdisk
  2. Disk Structure
  3. Open Disk
     1. Command: sudo testdisk /dev/mmcblk0p2

Figure 2  
  
Partition Selection



*Note.* /dev/mmcblk0p2 selected for analysis.

Figure 3  
  
File System



*Note.* Partition is type ext4.

Figure 4  
  
File and Directory View

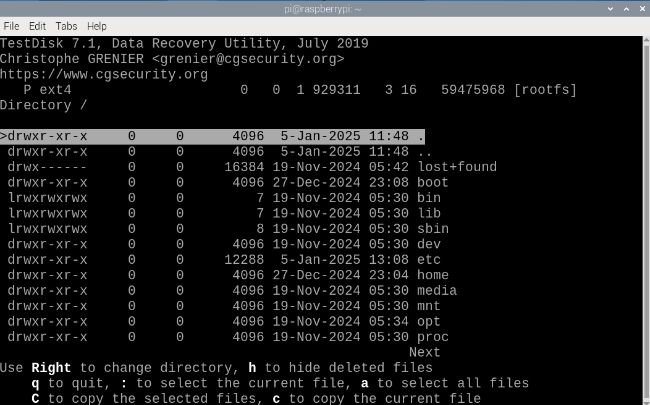
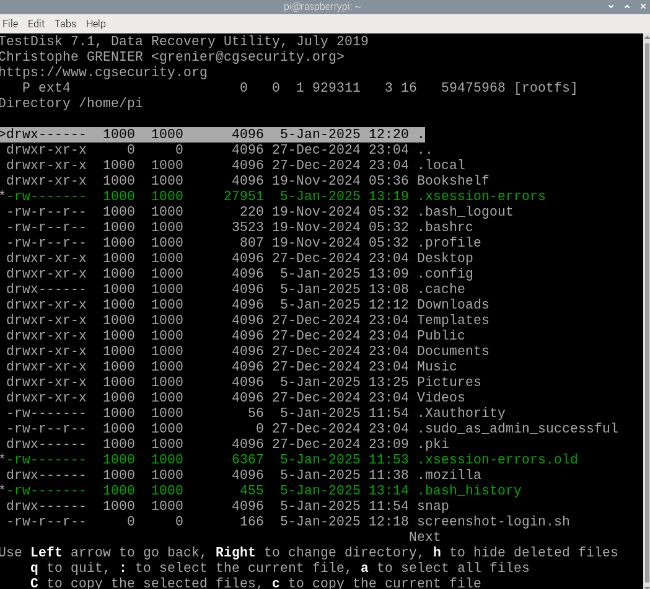
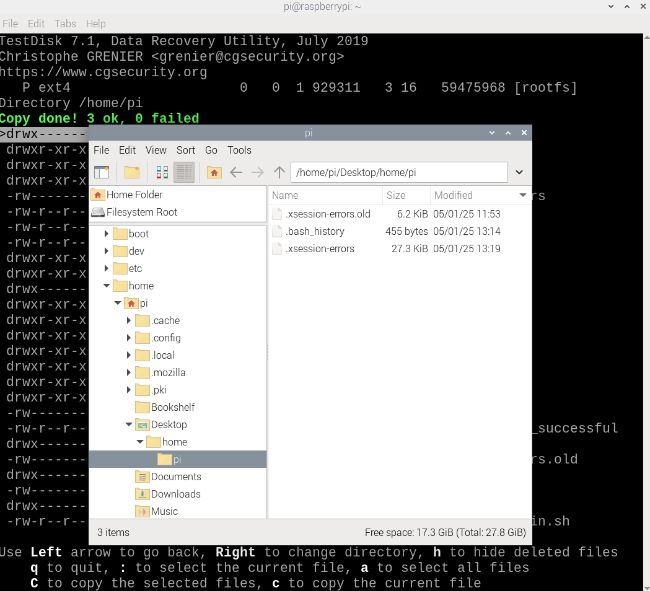


Figure 5  
  
Recovered Documents



*Note.* Targeted documents in green are highlighted.

Figure 6  
  
Copy Completed Successfully



*Note.* Confirmed targeted files received locally.

Recovery is complete

References

Acronis. (2024, March 5). How to restore a deleted file: A step-by-step guide. Retrieved January 5, 2025, from <https://www.acronis.com/en-us/blog/posts/how-to-restore-individual-files/#a1SkJgMpN0>

Alibaba Cloud. (n.d.). *Best practices for Linux instance data recovery*. Retrieved January 3, 2025, from <https://www.alibabacloud.com/help/en/ecs/use-cases/best-practices-for-linux-instance-data-recovery#5bdce0742evv9>

Easttom, C. (2021). *Digital forensics, investigation, and response* (4th ed.). Jones & Bartlett Learning.

IT Asset Mangement Group. (n.d.). *7 Steps To Recover Data From a Hard Drive: Windows, Mac and Linux*. IT AMG. Retrieved January 2, 2025, from <https://www.itamg.com/data-storage/hard-drive/recovery/>

Saive, R. (Ed.). (2017, August 8). *How to Boot into Single User Mode in CentOS/RHEL 7*. TechMint. Retrieved December 28, 2024, from <https://www.tecmint.com/boot-into-single-user-mode-in-centos-7/>