Chapter 3
SSD Forensic Investigation Using Open Source Tool

Hepi Suthar
Rashtriya Raksha University, India

Priyanka Sharma
Rashtriya Raksha University, India

ABSTRACT

According to the CIA triad, Cyber Forensic Investigation judicial point of view is the data integrity of volatile memory kinds of data storage devices. This has long been a source of concern, and it is critical for the chain of custody procedure. As an outcome result, it is a substantial advancement for the measured examination cycle to safeguard unstable data from SSD. In this study provides the easiest way to preserve potentially volatile based memory digital proof, store on SSDs, and generate forensically bit-streams, also known as bit-by-bit copies. The challenge of protecting the data integrity of an electronic piece of evidence that has been arrested at a crime scene frequently faces analysts. This academic article primarily suggests a process method and a few steps for carrying out forensic investigations on data obtained from solid state drives all the while avoiding the TRIM characteristic and garbage series from running lacking user input or interaction, preserving the data integrity of the facts as usable digital evidence.

DOI: 10.4018/978-1-6684-6864-7.ch003

INTRODUCTION

A SSD is a type of solid-state secondary types of storage device that stores data using integrated circuit (IC) assemblies as memory. Although SSDs do not contain physical disks, they are sometimes known as solid-state drives. SSDs can be utilised with conventional tough disk force shape elements and protocols, which include Serial superior era attachment and SAS, notably simplifying their integration into laptop systems. New shape elements, just like the M.2 shape factor, and new I/O protocols, such NVM Express, were evolved to satisfy the current technological wishes of the Flash reminiscence era utilized in SSDs (Geier, 2015; Kang et al., 2018). SSDs lack mechanical transmitting components. This separates them from ordinary electromechanical devices with moving R/W heads and rotating disks, like as Hard disk drives or floppy disks (Templeman & Kapadia, 2012). SSDs are regularly more injury resistant, operate silently, have quicker get right of entry to times, and have decreased latency when in contrast to electromechanical units (Suthar & Sharma, 2022). Although the cost of SSDs has decreased over time, they're nevertheless greater costly than HDDs according to unit of garage in 2018 and are expected to hold so for the subsequent ten years.

The majority of SSDs used 3D Triple Level Cell NAND flash reminiscence (Geier, 2015). It is a type of non-volatile memory (similar to ROM) that maintains data even when the energy is switched off (Bunker et al., 2012). SSDs can be composed of random-access memory (RAM) for applications that demand quick access but no longer always facts persistence after a strength outage. When external electricity is lost, batteries can be employed as integrated power sources in such units to retain facts for a set size of time (Suthar & Sharma, 2022). If energy is lost, strong nation disks save facts as electrical charges, which steadily leak over time. This is why solid kingdom drives are unsuitable for archiving applications, as outdated drives (that have handed their patience rating) often begin to lose facts after being stored for one to two years (at 30 °C). Hybrid drives (SSHDs) combine a giant challenging disk power with a strong country drive cache to speed up frequently accessed data. A hybrid force is one that combines the advantages of SSDs and HDDs into a single device, such as Apple's Fusion Drive (Suthar & Sharma, 2022).

Composition structure of SSD - The solid-state drive is mainly composed of the main control chip, flash memory particles, a cache chip, and a SATA interface chip (Ko, 2019). Solid State Drive (SSD) is a large-capacity memory that uses solid-state semiconductor chips as storage media. According to the semiconductor chip used, it can be divided into flash memory (NAND flash) and volatile storage (DRAM)-based solid-state drives. The latter requires an independent power supply and can only be used in very special equipment. It is beyond the scope of this article.