2022 Hendry Street, Ft Myers, FL 33901
CPRTools.com | 239-464-3282

CPR Tools, Inc.

Evaluating Security Claims of the Cigent Secure SSD

Date

July 1, 2021

Document No: 070121-002

2022 Hendry Street, Ft Myers, FL 33901
CPRTools.com | 239-464-3282

Table of Contents

1 PURPOSE

The Cigent Secure SSD allows for operation in what is called 'dual mode'. This feature permits the user to configure and access their drive as two separate storage systems. This document will refer to the 'regular' storage volume as 'Side A' of the drive. The secure storage system will be referred to as 'Side B'. According to Cigent documentation neither of these storage systems is aware that the other exists and the host Operating System is only able to access one at a time.

CPR Tools was tasked to determine if data could be recovered from the 'hidden' storage system of the drive using commercially available and proprietary data recovery tools.

2 DRIVE UNDER TEST

- Manufacturer
  - Cigent Secure SSD™
- Model
  - K2 (testing Dual Mode™)
- Size
  - 1TB (960GB)
- Interface
  - PCIe (NVMe)
- Serial Number
  - AF710716104D00000156
- Firmware
  - ECFM13TO

3 TEST PREPARATION

The Operating System used for setup was Windows 10. Using the software tools provided commercially by Cigent the SSD was setup following the on-screen instructions. The drive was divided into two equal parts of 480GB and formatted. Once formatted 100 test text (.txt) files were added to Side B and Side B was closed. Upon reboot Side A was available through the Operating System and Side B was not detected using Explorer or Disk Management.

NOTE: CPR Tools lab personnel were not given any utilities to 'see' the secure area.

4 TEST PLAN

CPR Tools performed the following steps during testing of the device:

- Physical Examination of Subject and Exemplar drives
- Review SMART data
- Examine physical drive access with a hex editor
- Examine output of the SED Util utility
- Directly examine the FLASH Storage hardware

Each of these steps is detailed below.

5 PHYSICAL REVIEW OF SUBJECT AND EXEMPLAR DRIVES

As the capacity of the subject drive was unknown to the examiner upon presentation, a physical comparison to exemplar drives of varying capacities was made.

Figure 1 - Storage Chips Of Subject Drive

Figure 2 - Storage Chips From Exemplar 960GB Drive

Figure 3 - Storage Chips from Exemplar 480GB Drive

The examiner made note that the storage chip identifier from the exemplar 480GB drive did not match those of the target drive's storage chips, but the storage chips from the exemplar 960GB drive did match.

6 TEST – REVIEW OUTPUT OF S.M.A.R.T UTILITY

The CrystalDiskInfo utility identified the target drive as having a capacity of 480.0 GB . The same utility identified an exemplar 480GB drive as having a capacity of 480.1 GB. This 0.1GB difference is significant from a forensics standpoint, as any difference from an exemplar sample indicates a path worthy of further investigation. (See Figure 4 and Figure 5)

This seemingly minor discrepancy was an indication that while the subject drive was interpreted as 480GB capacity by the software, there was likely some kind of modification to the addressable capacity of the drive.

The utility also displays basic information derived from how the operating system, Windows 10, identifies the drive. This information includes normal S.M.A.R.T. values as well as drive capacity, the NVMe version, Firmware and Serial Number.

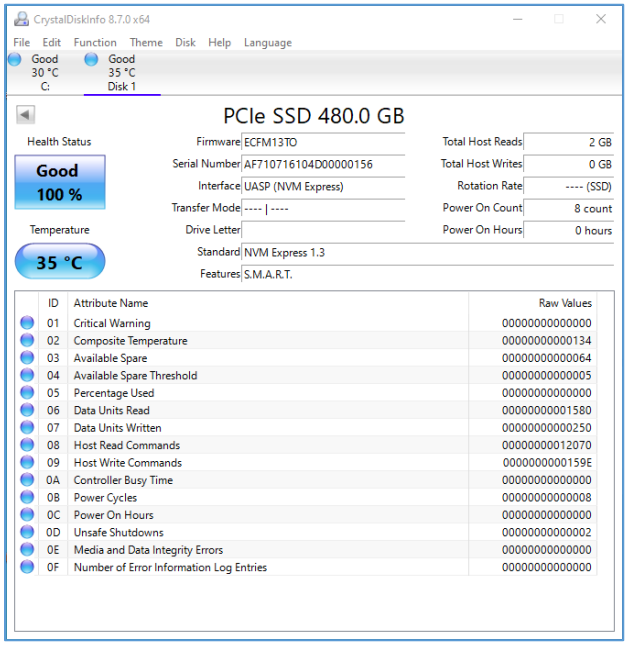

Figure 4 - Output of S.M.A.R.T. Utility Scan on Target Drive

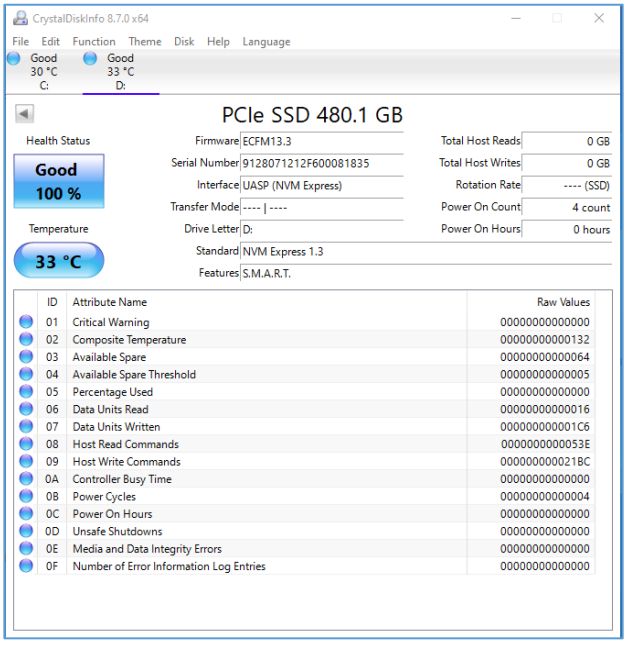

Figure 5 - Output of S.M.A.R.T. Utility Scan on Exemplar Drive

2022 Hendry Street, Ft Myers, FL 33901
CPRTools.com | 239-464-3282

7 EXAMINATION WITH HEX EDITOR

Using an industry standard Hex Editor, we found the drive to be accessible as a physical device. Scan of the device reported no errors but upon further examination, the only visible data was test data from Side A, no test data from Side B was viewable. Side A, as shown in the hex editor is depicted in Figure 6.

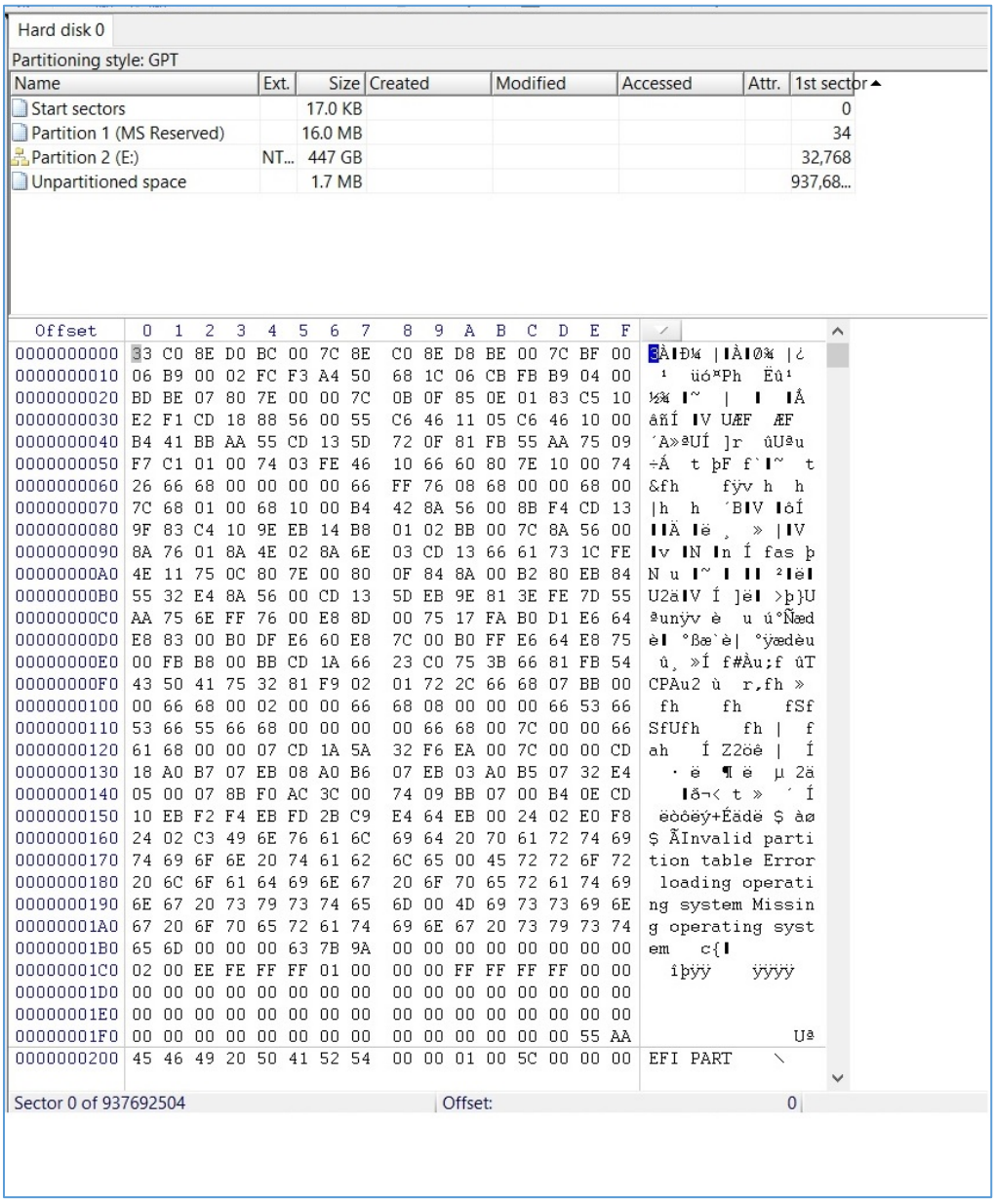

Figure 6 - Hex Editor display of Side A

8 EXAMINATION WITH SED UTIL

SED Util is a utility created by the Drive Trust Alliance and is a full featured command line interface for managing all aspects of drives which conform to the OPAL specification. The SED Util reports the locked or unlocked status for drives supported under the OPAL specifications seen in the Locking function (0x0002). Upon examination with SED Util, the software reported locked ranges and indicated that the drive conformed to the OPAL specification(s) for locked ranges.

Figure 7 depicts the output of the SED Util's review of the drive.

```
/dev/nvme1 NVMe PCIe SSD                                    ECFM13TO
AF710716104D00000156
TPer function (0x0001)
    ACKNAK = N, ASYNC = N. BufferManagement = N, comIDManagement  = Y, Streaming
= Y, SYNC = Y
Locking function (0x0002)
    Locked = N, LockingEnabled = Y, LockingSupported = Y, MBRDone = N, MBREnabled
= N, MediaEncrypt = Y
Geometry function (0x0003)
    Align = Y, Alignment Granularity = 8 (4096), Logical Block size = 512, Lowest
Aligned LBA = 0
SingleUser function (0x0201)
    ALL = N, ANY = N, Policy = Y, Locking Objects = 9
DataStore function (0x0202)
    Max Tables = 9, Max Size Tables = 10485760, Table size alignment = 1
OPAL 2.0 function (0x0203)
    Base comID = 0x07fe, Initial PIN = 0x0 , Reverted PIN = 0x0 , comIDs = 1
    Locking Admins = 4, Locking Users = 9, Range Crossing = N

TPer Properties:
  MaxComPacketSize = 16384  MaxResponseComPacketSize = 16384
  MaxPacketSize = 16364  MaxIndTokenSize = 16328  MaxPackets = 1
  MaxSubpackets = 1  MaxMethods = 1  MaxSessions = 1
  MaxAuthentications = 9  MaxTransactionLimit = 1  DefSessionTimeout = 0


Host Properties:
  MaxComPacketSize = 2048  MaxResponseComPacketSize = 2048
```

Figure 7 - Output of the SED Util's view of the target drive

It should be noted that the settings for *LockingEnabled* and *MediaEncrypt* show 'on' which provided an indication that one or more hidden partitions might exist on the target drive beyond the reported LBA range.

9 RECOVERY ATTEMPTS

Using industry standard and proprietary hardware and software utilities, several additional attempts to access user data were made, including attempts to read from sectors outside the reported LBA range (Side 2). These attempts were not successful.

Based on these experiences, we initiated more advanced recovery methodologies which directly target the hardware itself.

10 POST CHIP-OFF X-RAY OF STORAGE MEDIA

The FLASH chips were removed from the NVMe PCB. As part of our standard operating procedure when performing chip-off recoveries, we employ an X-RAY machine to review and ensure that no damage was done during the chip removal process. Figure 8 depicts the post chip-off X-RAY of the chip removed from the subject drive.

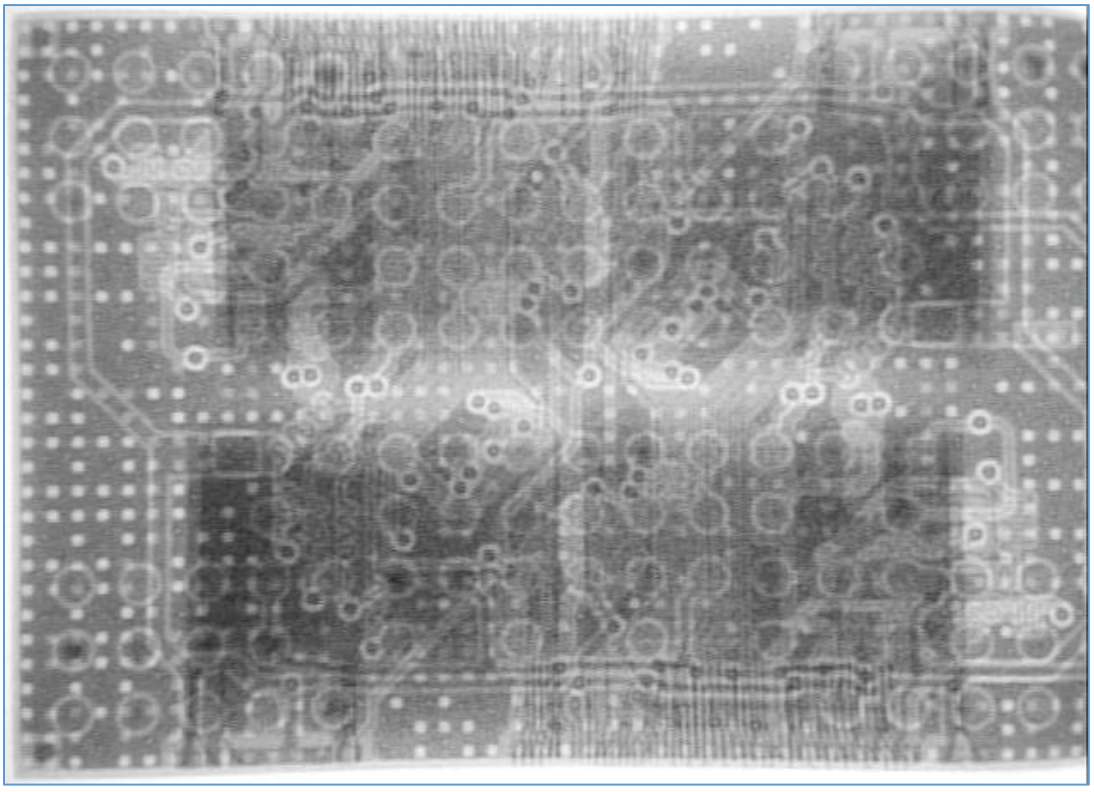

Figure 8 - X-RAY of Storage Chip Removed From Subject Drive

Examination of the X-RAY image revealed no damage to the bond wires or traces, indicating that the chip-off procedure was successful.

11 DIRECT EXAMINATION OF FLASH STORAGE

Once removed from the NVMe PCB the chips were examined directly using a BGA Chip Reader.

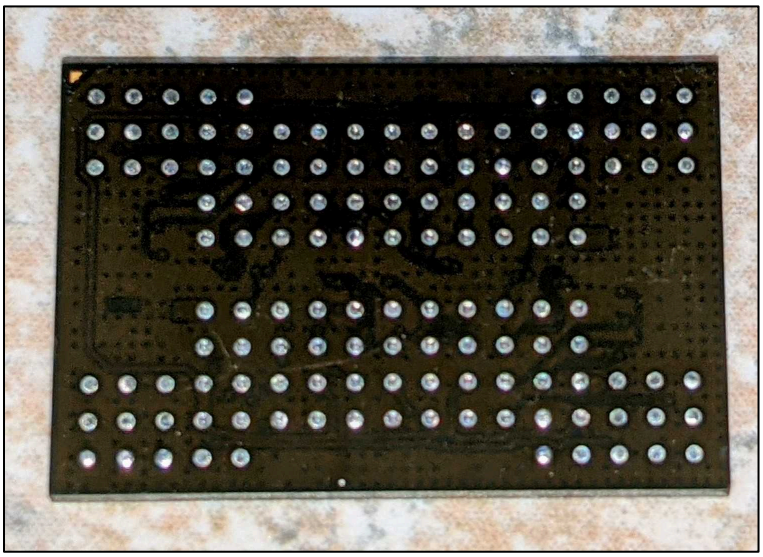

Figure 9 - BGA FLASH Chip

All data recovered from the chips were saved to binary ‘dumps’. The binary ‘dumps’ were then scanned for data. The scan did not reveal any recognizable data, nor did it reveal any ECC patterns. A sample of the output from these scans is depicted in Figure 10 and reveals nothing more than random data.

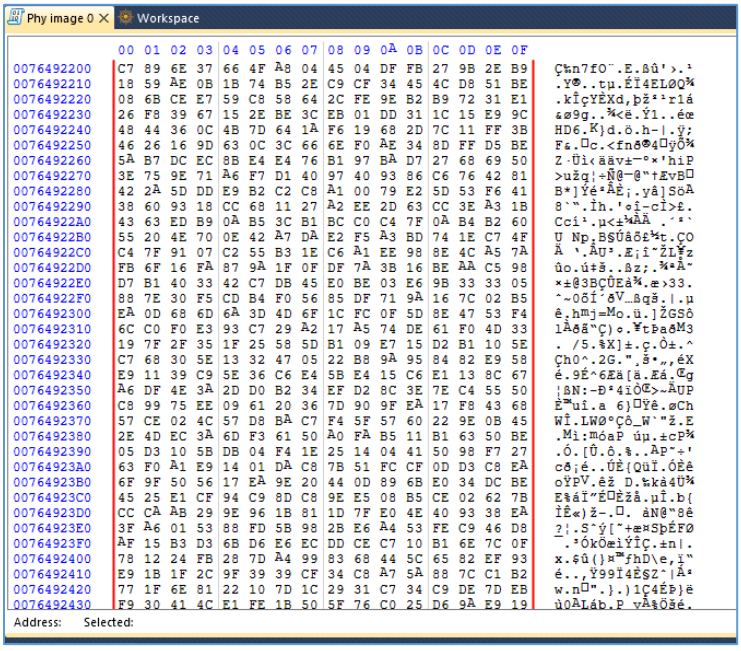

Figure 10 – Random Page Data pulled from Chip Dump

Figure 11 and Figure 12 depict "page bit" views of chip data. All white locations represent a value of zero; the locations in black represent a value of one.

Figure 11 was taken from the target drive. Given that there are no discernable patterns, we are confident that there is no viable data in this view. However, data may be present and encrypted.

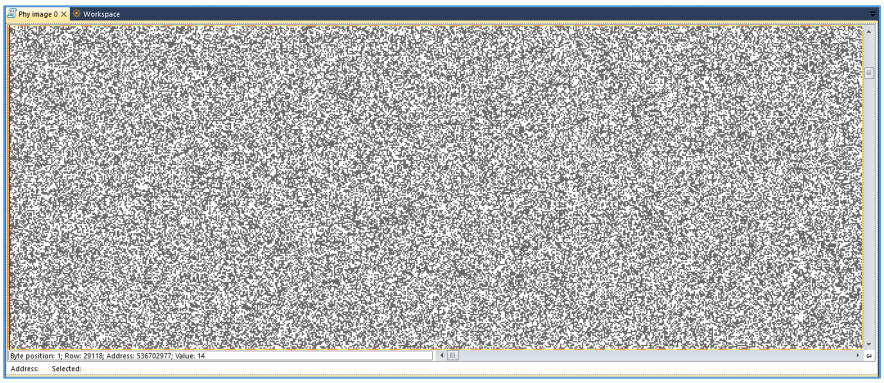

Figure 11 - A page bit view of the chip data displaying no discernable patterns

Figure 12 was taken from an exemplar drive. Even a cursory examination displays identifiable patterns which represent, from left to right, user data, Translator, ECC Data and more user data.

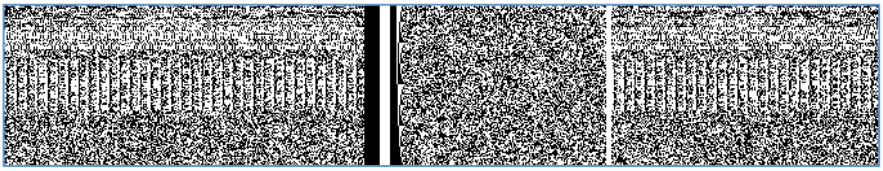

Figure 12 - A page bit view of chip data from the exemplar drive displaying user data.

12 SUMMARY OF FINDINGS

In evaluating the security measures on the Cigent Secure SSD, our engineers employed a number of techniques to obtain user data from the "hidden side" once the drive was in its "dual mode" state. Note: The target drive was presented without a drive information label.

The target drive reported a capacity of 480GB; the exemplar, known to be a 480GB drive, reported 480.1GB. This small discrepancy led to a more thorough physical comparison between the two. It was noted that the exemplar drive had fewer storage chips on the PCB than the target drive.

Employing an industry standard hex editor, we examined the target drive as a physical device. The device was able to be opened. A total of 937,692,504 (480GB) sectors were able to be displayed.

Next, we examined the target drive using the SED Util software. The software reported a value of 'on' for *LockingEnabled* and *MediaEncrypt*. This information, combined with the physical differences between the target and the exemplar drive, were indicators that one or more hidden partitions might exist on the drive beyond the drive's reported LBA range. As all traditional methods had been exhausted, we moved on to advanced methods by performing a chip-off recovery.

The FLASH storage chips were removed and examined under X-RAY to ensure that no damage was incurred during the chip removal process.

The FLASH storage chips were then accessed using a BGA chip reader. Scans of the chip did not reveal any recognizable data, nor did it reveal any ECC patterns. Next, page bit views of the data were rendered and examined. All data appeared to be random which led us to believe it was encrypted and we were unable to recover any user data from the chips.

13 CONCLUSION

After a thorough review utilizing both basic and advanced recovery and forensic techniques, no user data was able to be recovered from Side B of the Cigent Secure SSD.