



CPR Tools, Inc.

Evaluating Security Claims of the  
Cigent Secure SSD

Date

July 1, 2021

Document No: 070121-002



## Table of Contents

1	Purpose .....	3
2	Drive Under Test .....	3
3	Test Preparation.....	3
4	Test Plan.....	4
5	Physical Review of Subject and Exemplar Drives.....	4
6	Test – Review Output of S.M.A.R.T Utility .....	4
7	Examination with Hex Editor .....	6
8	Examination with SED Util.....	7
9	Recovery attempts .....	8
10	Post Chip-Off X-Ray of Storage Media .....	8
11	Direct Examination of FLASH Storage .....	9
12	Summary of Findings.....	10
13	Conclusion.....	11



## 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.

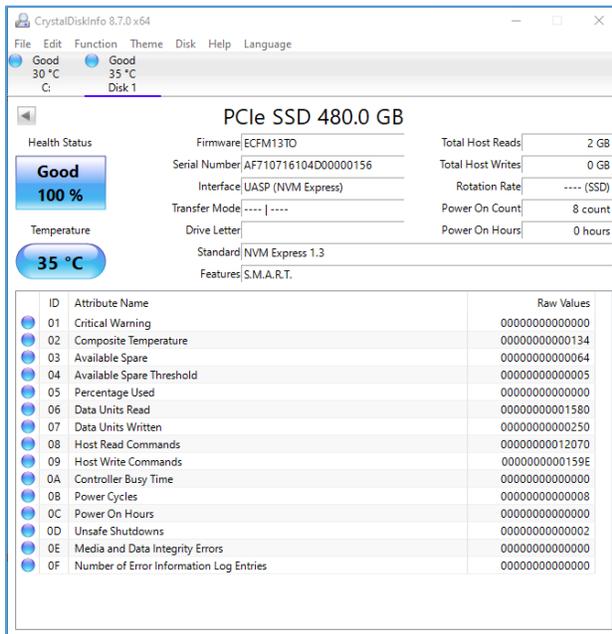


Figure 4 - Output of S.M.A.R.T. Utility Scan on Target Drive

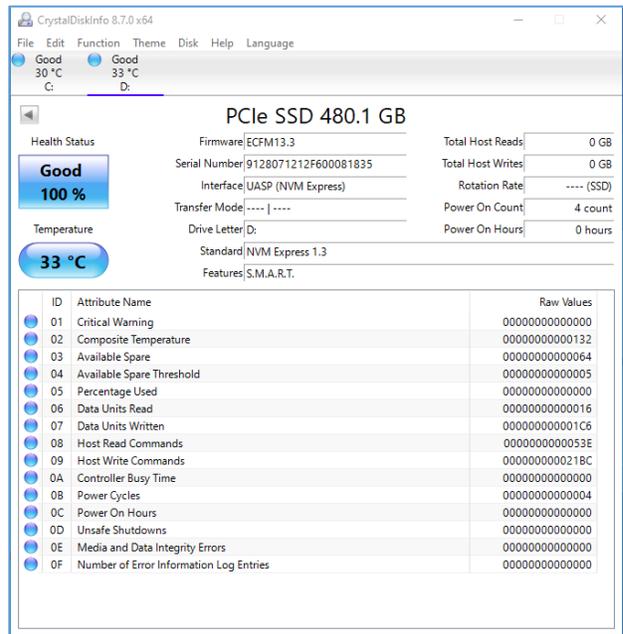


Figure 5 - Output of S.M.A.R.T. Utility Scan on Exemplar Drive

## 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.

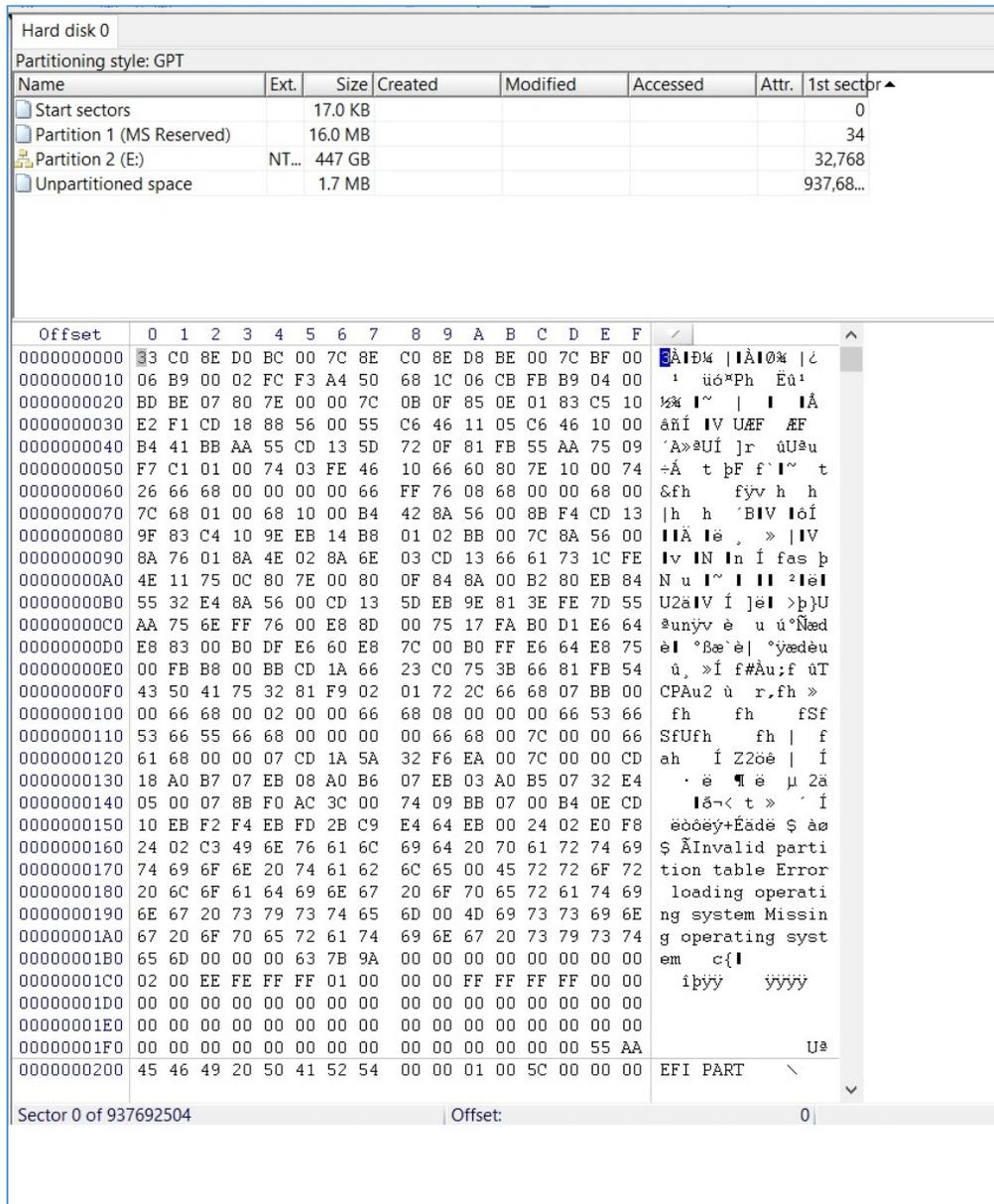


Figure 6 - Hex Editor display of Side A

## 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.

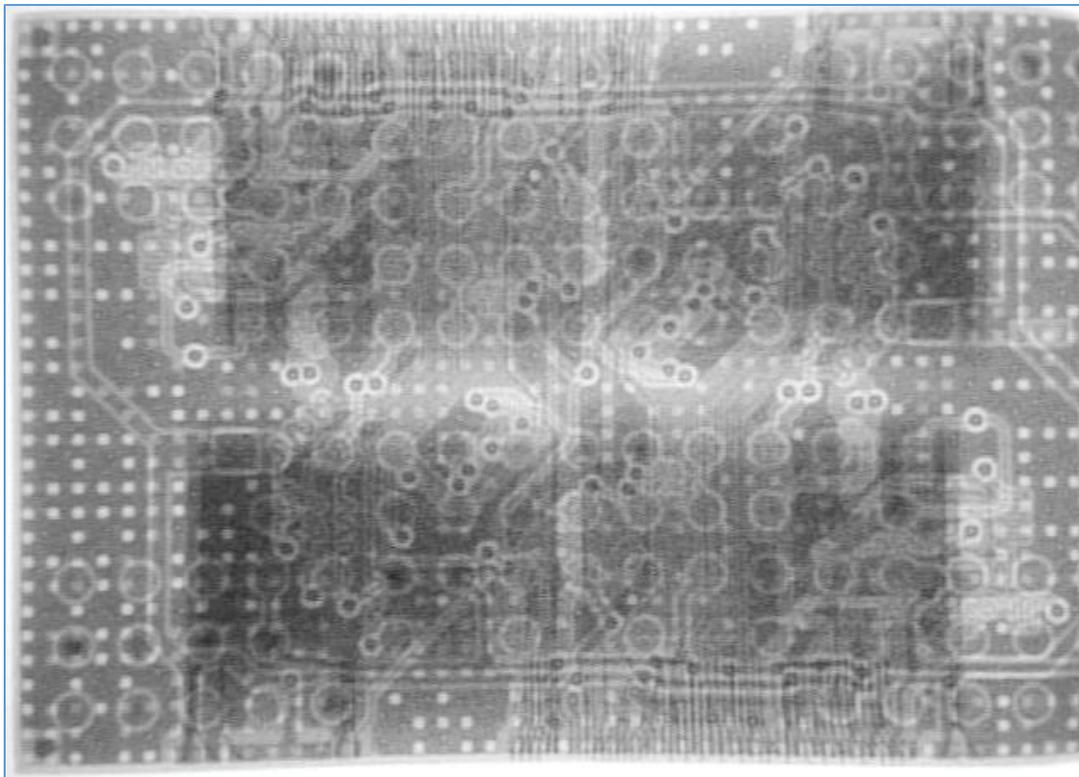


Figure 8 - X-RAY of Storage Chip Removed From Subject Drive

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.

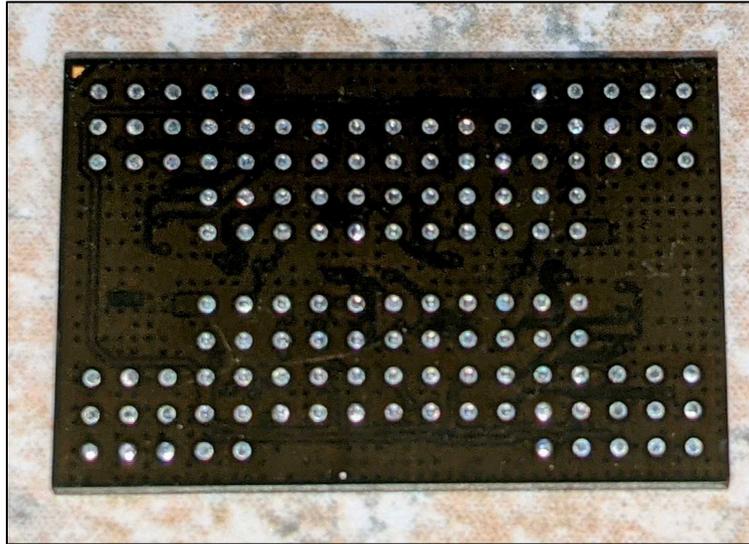


Figure 9 - BGA FLASH Chip

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.

```

Phy Image 0 X Workspace
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Ckn7f0".E.âù'>.-
0076492200 C7 89 6E 37 66 4F A8 04 45 04 DF FB 27 9B 2E B9 .Y0. tu.ÉI4ELOQK
0076492210 18 59 AE 0B 1B 74 B5 2E C9 CF 34 45 4C D8 51 BE .kfcYÈXd,pè'+rlâ
0076492220 08 6B CE E7 59 C8 58 64 2C FE 9E B2 B9 72 31 E1 .æ9g. %cê.Y1.ée
0076492230 26 F8 39 67 15 2E BE 3C EB 01 DD 31 1C 15 E9 9C æ9g. %cê.Y1.ée
0076492240 48 44 36 0C 4B 7D 64 1A F6 19 68 2D 7C 11 FF 3B HD6.Kjd.ô.h-l.ÿ;
0076492250 46 26 16 9C 83 0C 3C 66 6E F0 AE 34 8D FF D5 BE Fæ.Dc.<fn804Dy0K
0076492260 5A B7 DC EC 8B E4 E4 76 B1 97 BA D7 27 68 69 50 Z.Ûi.ääv±-°*hiP
0076492270 3E 75 9E 71 A6 F7 D1 40 97 40 93 86 C6 76 42 81 >uèq;=Ñ@-@"+EVB
0076492280 42 2A 5D DD E9 B2 C2 C8 A1 00 79 E2 5D 53 F6 41 B*ÿé+Äè; .yâ]s0A
0076492290 38 60 93 18 CC 68 11 27 A2 EE 2D 63 CC 3E A3 1B 8".In.'oi-c]S0A
00764922A0 43 63 ED B9 0A B5 3C B1 BC C0 C4 7F 0A B4 B2 60 Cci'.µ<+MÄÄ .'.*
00764922B0 55 20 4E 70 0E 42 A7 DA E2 F5 A3 BD 74 1E C7 4F U Np.BS0â8èMt.CO
00764922C0 C4 7F 91 07 C2 55 B3 1E C6 A1 EE 98 8E 4C A5 7A Ä .'.ÄU'.E; i-ZÿZ
00764922D0 FB 6F 16 FA 87 9A 1F 0F DF 7A 3B 16 BE AA C5 98 ùo.ú+s. .Bz;.%*Ä
00764922E0 D7 B1 40 33 42 C7 DB 45 E0 BE 03 E6 9B 33 33 05 *æ@3BÛ0EÄK.æ>33.
00764922F0 88 7E 30 F5 CD B4 F0 56 85 DF 71 9A 16 7C 02 B5 ~-0öI'èV.Bq8.l.µ
0076492300 EA OD 68 6D 6A 3D 4D 6F 1C FC 0F 5D 8E 47 53 F4 è.hmj=Mo.ü.]ZGS6
0076492310 6C 0D F0 E3 93 C7 29 A2 17 A5 74 DE 61 F0 4D 33 lÄâ~C)ø.ÿtba8M3
0076492320 19 7F 2F 35 1F 25 58 5D B1 09 E7 15 D2 B1 10 5E . /5.%X]±.ç.0±.
0076492330 C7 68 30 5E 13 32 47 05 22 88 9A 95 84 82 E9 58 Çh0^-.2G.".â*.,èX
0076492340 E9 11 39 C9 5E 36 C6 E4 5B E4 15 C6 E1 13 8C 67 é.9È-6Zâ[æ.Éâ.Cg
0076492350 A6 DF 4E 3A 2D 0D B2 34 EF D2 8C 3E 7E C4 55 50 ;AN:-D*4IOE>..ÄUP
0076492360 C8 99 75 EE 09 61 20 36 7D 90 9F EA 17 F8 43 68 E"ui.a 6)ÛYè.øCn
0076492370 57 CE 02 4C 57 D8 EA C7 F4 5F 57 60 22 9E 05 45 Wl.LM9ç0_W""Z.E
0076492380 2E 4D EC 3A 6D F3 61 50 A0 FA B5 11 B1 63 50 BE .Mi:R0aP üu.æoP
0076492390 05 D3 10 5B DB 04 F4 1E 25 14 04 41 50 98 F7 27 .ó.[Û.ô.â.ÄP'+
00764923A0 63 F0 A1 E9 14 01 DA C8 7B 51 FC CF OD D3 C8 EA c8;é.ÛÈ(QüY.óÈK
00764923B0 6F 9F 50 56 17 EA 9E 20 44 OD 89 6B E0 34 DC BE oVpV.èè D.kkâ4U
00764923C0 45 25 E1 CF 94 C9 8D C8 9E E5 08 B5 CE 02 62 7B EâI'èÛÈZâ.üi.b[
00764923D0 CC CA AB 29 9E 96 1B 81 1D 7F E0 4E 40 93 38 EA iÈæ)Z-.D. AN0'8è
00764923E0 3F A6 01 53 88 FD 5B 98 2B E6 A4 53 FE C9 46 D8 ?; .S'ÿ[ '+æSpEÛ0
00764923F0 AF 15 B3 D3 6B D6 E6 EC DD CE C7 10 B1 6E 7C 0F .'.0x0æiÿÿC.anl.
0076492400 78 12 24 FB 28 7D A4 99 83 68 44 5C 65 82 EF 93 x.âù{)M"fhDve,i
0076492410 E9 1B 1F 2C 9F 39 39 CF 34 C8 A7 5A 88 7C C1 B2 é...ÿ99I4ÈS2'IA+
0076492420 77 1F 6E 81 22 10 7D 1C 29 31 C7 34 C9 DE 7D EB w.nÛ.).)1ç4ÈB)è
0076492430 F9 30 41 4C E1 FE 1B 50 5F 76 C0 25 D6 9A E9 19 ù0ALâb.P.vâ0èé.
Address: Selected:
  
```

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 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.

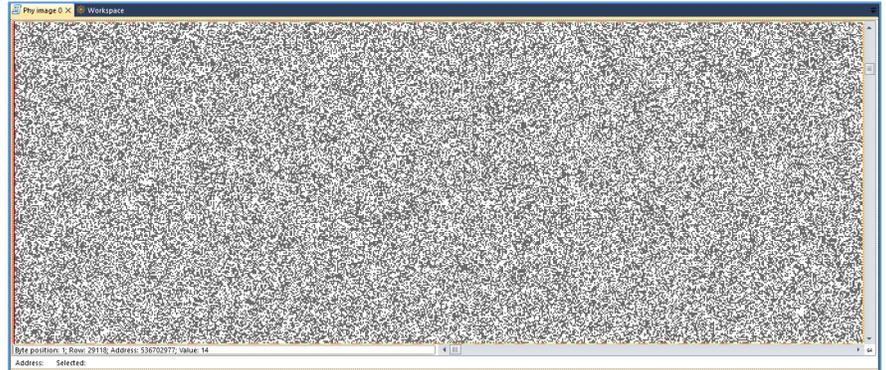


Figure 11 - A page bit view of the chip data displaying no discernable patterns

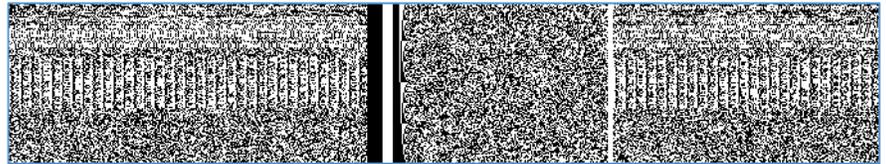


Figure 12 - A page bit view of chip data from the exemplar drive displaying user data.

## 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.