THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 16

Article 3

April 2021

Viability of Consumer Grade Hardware for Learning Computer Forensics Principles

Lazaro A. Herrera
Nova Southeastern University, lh1490@mynsu.nova.edu

Recommended Citation

Herrera, Lazaro A. (2021) "Viability of Consumer Grade Hardware for Learning Computer Forensics Principles," *Journal of Digital Forensics, Security and Law*: Vol. 16 , Article 3.
Available at: https://commons.erau.edu/jdfsl/vol16/iss1/3

Viability of Consumer Grade Hardware for Learning Computer Forensics Principles

Cover Page Footnote

This paper and the research behind it would not have been possible without the exceptional support of the Miami-Dade Police Department Digital Forensic Unit for providing the loaner forensics hardware, the knowledge on how to best utilize the hardware and being reachable for all questions. Additionally, Benjamin Livelsberger of the NIST's Computer Forensics Tool Testing Program (CFTT) was of key importance to ensure consistent testing of all of the consumer grade tools, providing updates on CFTT's Version 5 with Forensic Wipe testing and troubleshooting issues with our setup. Last, but not least, Dr James Kiper for continuously encouraging and supporting me to take on research into fringe and underserved topics within the field of computer forensics. His mentorship of his students to continously apply scientific methodologies derived from the forensics field to bring scientific ideals to the computer forensics field is an example to be followed.

VIABILITY OF CONSUMER GRADE HARDWARE FOR LEARNING COMPUTER FORENSICS PRINCIPLES

Lazaro A Herrera
Nova Southeastern University
lh1490@mynsu.nova.edu

ABSTRACT

We propose utilizing budget consumer hardware and software to teach computer forensics principles and for non-case work, research and developing new techniques. Consumer grade hardware and free/open source software is more easily accessible in most developing markets and can be used as a first purchase for education, technique development and even when developing new techniques. These techniques should allow for small forensics laboratories or classroom settings to have the tooling and framework for trying existing forensics techniques or creating new forensics techniques on consumer grade hardware. We'll be testing how viable each individual piece of hardware is as well as combinations along with seeing at which point utilizing forensics-grade hardware becomes necessary in order to proceed.

Keywords: component, formatting, style, styling, insert

1. INTRODUCTION

Developing countries worldwide still have a disparity in education opportunities with the "percentage of adults with a primary education is 42 percent in low developing countries, compared with 94 percent in very high developing countries" Press (2019). As these countries "bring household internet (15%), access to computers (9.7%) and broadband knowledge (0.7%)" Press (2019) to their citizens, there will be more and more high technology job opportunities. As computers become more prevalent, cybercrime will eventually become a concern and having a trained population that can take on the work that is ahead will become more and more critical since cybercrime does not tend to respect geographical borders.

Growing local talent for computer forensics and cybersecurity work is a long term endeavour that requires access to a lot of technology and knowledge. The internet can provide the knowledge but the question is, who will provide the technology? Computer forensics knowledge and principles require more hardware even for a beginner digital forensics lab Lawrence et al. (2018) than most of other disciplines and as explored, the cost of getting access to this technology is far larger than expected.

There is a serious need for budget-friendly forensics hardware that can be used in classroom settings and even research settings if we want developing countries to take part in forensics research and become a part of the greater worldwide forensics body. This hardware must be price competitive, must have educational value and should provide the maximum amount of forensics value with reproducible results.

As can be seen in Figure 1 even the used hardware that was used for this project for SATA imaging costs in excess of $110 (without any of the cables to attach SATA media to it). Adding in a SATA / IDE bridge in Figure 2 like the one used for IDE imaging (without cables for IDE media) adds an extra $90. Although $200 is not a prohibitive amount to a large university in the United States or a large police department, ensuring the hardware is accessible to a wider audience is in the industry's best interest.

As can be seen in Table 1, that $200 price point can sting when looking at what the monthly adult wages in USD for some of the Latin American countries currently entering a developed or developing status FinancialRed (2018) compared to adult US wages Bureau of Labor Statistics (2019).

Table 1 shows how many working days an average adult could be expected to spend in order to save enough money to purchase the hardware that was used for testing here.

2. PROPOSED TESTING PLAN

2.1 Hardware Platform

The selection of consumer-grade hardware and software were derived from online searches on budget hardware and software for outfitting a beginner forensics lab. A mixture of this hardware and software should be able to: create a forensics image from IDE or SATA hard drive; clone disk from an IDE or SATA hard drive; and write an image from an image file to a disk. These tasks can illustrate the importance of minimizing spoilage of evidence and hashing in an educational environment.

The hardware outlined in Table 4 and Table 5 was used to validate the forensic value provided by the hardware in Table 2 and Table 3. Items in Table 4 and Table 5 were either purchased, existing hardware or loaned in order to be tested.

Cinolink's Dual Bay has a hardware based cloning function that does not require a connection to a computer and minimizes the odds of accidentally contaminating the underlying evidence and can double as a forensic wiper when paired with some open source software listed in the Software Platform section. Large disks up to 10TB are natively supported and the hardware is USB 3.0 capable.

CoolGear's 'Write Protect' hardware includes all of the hardware to be able to mount one 2.5" / 3.5" SATA and IDE device (at the same time) and dedicated switches for write protect for both SATA and IDE allowing for use as both a read-only or read-write device. There are additional safeties that make it impossible to disable write blocking without powering off and powering the device back on but the manufacturer only supports write blocking under Windows-based systems. For 2.5" devices, it is also possible to power the device directly from the USB 3.0 connection without carrying external power; this can be useful in a classroom setting where power may not be able to all desks.

2.2 Software Platform

In order to make testing feasible at this scale, flash drives were used to hold the test suites that would validate the hardware. In order to make this possible, YUMI Multiboot Pendrivelinux.com (2020) was used to load multiple versions of different Linux and Windows operating systems unto three separate flash drives (Windows to Go, MBR-based and UEFI-based). Only software that was used during testing is listed under Table 6, 7

Table 1. Time to Purchase Hardware

Country	***Monthly Wages USD***	***Time To Purchase****
United States	$3,744	2 days
Argentina	$340	18 days
Brazil	$295	21 days
Bolivia	$300	20 days
Chile	$413	15 days
Colombia	$262	24 days
Costa Rica	$512	12 days
Cuba	$29	213 days
Dominican Republic	$288	21 days
Ecuador	$386	16 days
El Salvador	$300	20 days
Guatemala	$380	16 days
Honduras	$341	18 days
Mexico	$141	43 days
Nicaragua	$115	53 days
Panama	$731	8 days
Paraguay	$368	16 days
Peru	$283	21 days
Urugay	$431	14 days
Venezuela	$37	167 days

*Lower Values are Better for this Metric

Table 2. Consumer Grade Software

Name	***Purpose***	***Price***
Roadkil's Diskwipe	Forensic wipe	Free
Roadkil's Diskimage	Imaging/Clone	Free

Table 3. Consumer Grade Hardware

Name	***Purpose***	***Price***
Cinolink Dual Bay	Clone/R/W for SATA	$29.99
CoolGear SATA/IDE	Write Protect SATA/IDE	$49.99
ULTRA SATA/IDE	IDE Writing	$20.00*

*Not used for testing, just for setup

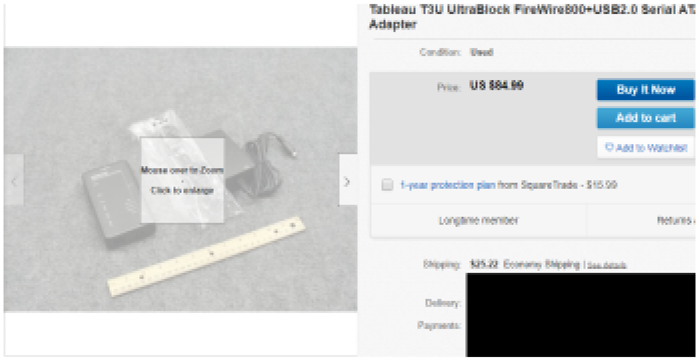


Tableau T3U UltraBlock FireWire800+USB2.0 Serial AT
Adapter

Condition: Used

Price: US $84.99

□ 1-year protection plan from SquareTrade - $15.99

Longtime member | Returns

Shipping: $25.22 Economy Shipping | See details

Delivery: [redacted]

Payments:

Figure 1. Cost of Tableau T3U

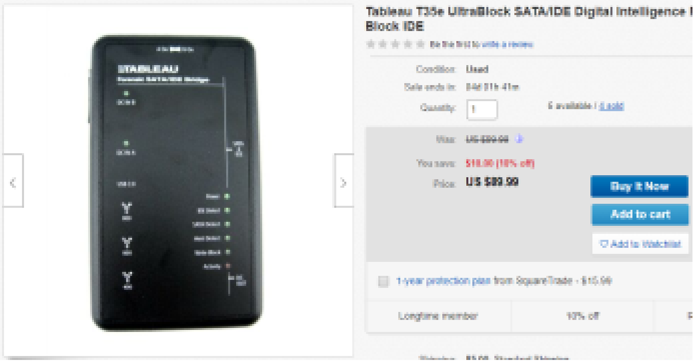


Tableau T35e UltraBlock SATA/IDE Digital Intelligence
Block IDE

☆☆☆☆☆ Be the first to write a review

Condition: Used

Sale ends in: 04d 01h 41m

Quantity: 1 6 available / 1 sold

Was: ~~US $99.99~~

You save: $10.00 (10% off)

Price: US $89.99

□ 1-year protection plan from SquareTrade - $15.99

Longtime member | 10% off

Shipping: $5.00 Standard Shipping

Figure 2. Cost of Tableau T35e

and 8. All tools are listed in the order they were used.

2.3 Testing Criteria

Due to the severe cost disparity of the hardware ($70 for consumer grade, $200 for forensics grade) and different speeds of the hardware under test (USB 3.0 for consumer grade, USB 2.0 for forensics grade), read / write performance will not be tested. The main criteria tested is the ability to take forensics images of media (or duplicating media) with a focus on ensuring checksums match between consumer and forensics gear. This criteria targets how reproducible the results are.

2.4 Testing Plan

Before any work was performed, all of the media used was forensically wiped using Roadkil's Diskwipe to write a basic single pass of zeros on each drive. The NIST's CFTT Federated Testing Thelma.allen@nist.gov (2020) suite was used after testing completed to validate the forensic wiping capabilityof Homeland Security (DHS) Science & (ST) (2020c). The Evidence Storage drive was formatted to NTFS for storage of any media while live booting Linux. The Suspect drive and Clone drives were left in their forensically wiped state. The CoolGear device in question was tested using the Hardware Write Block test under the NIST's CFTT Federated Testing Thelma.allen@nist.gov (2020) suite and CRU's Writeblocker Validation Utility in Windows before performing any tests. Reports on this testing were given to NIST for publication.

In order to ensure a realistic test scenario, a Windows 10 environment was prepared

Table 4. Storage Media

Name	***Purpose***	***Price***
Sandisk CZ48 128Gb Flash	Linux MBR Live Suites	$18.99
Spare 16Gb Flash	Linux EUFI Live Suites	Pre-owned
Samsung Fit 64Gb Flash	Windows To Go	$13.00
Seagate 1TB Expansion	Evidence Storage	Pre-owned
Inland 120Gb SSD	Suspect Drive (SATA)	Pre-owned
Seagate Momentus 320Gb HDD	Clone Drive (SATA)	Pre-owned
Maxtor DiamondMax 10 160GB	Clone Drive (IDE)	$14.95

Table 5. Forensics Grade Hardware

Name	***Purpose***	***Price***
Tableau T3U	SATA Write Blocker	Loaned
Digital Intel. UB	IDE Write Blocker	Loaned

Table 6. Linux MBR Flash Drive

OS	***Tool***	***Purpose***	***Price****
NIST CFTT v4 / v5	Validation	Validation	Open Source
Caine 11	Guymager	Imaging	Open Source
Kali Linux 2020 (forensic)	Guymager	Imaging	Open Source
Kali Linux 2020 (live)	Guymager	Imaging	Open Source
Parrot 4.7 (forensic)	Guymager	Imaging	Open Source
Parrot 4.7 (live)	Guymager	Imaging	Open Source
OSFClone 1.2.1000	Clone	Imaging	Open Source

Table 7. Linux UEFI Flash Drive

OS	***Tool***	***Purpose***	***Price****
Deft 8.2	Guymager	Imaging	Open Source
Paladin 7 (read only)	Imager	Imaging	Donationware*
Paladin Edge 64 (read only)	Imager	Imaging	Donationware*
Paladin 7 (read / write)	Imager	Imaging	Donationware*
Paladin Edge 64 (read / write)	Imager	Imaging	Donationware*

*Recommended donation: $25

Table 8. Windows To Go Flash Drive

Tool	***Install Type***	***Purpose***	***Price****
CRU WriteBlocking	Installer	Validation	Free*
Lightscreen Portable	Portable	Screenshots	Open Source
MouseJiggle Portable	Portable	Jiggler	Open Source
Notepad++ Portable	Portable	Note taking	Open Source
Belkasoft RAM Capturer	Portable	RAM Capture	Free*
MAGNET RAM Capture	Portable	RAM Capture	Free*
ofview	Portable	Open files	Free
MAGNET EDD	Portable	Encryption	Free*
wirelesskeyview	Portable	Credentials	Free
vaultpasswordview	Portable	Credentials	Free
dataprotectiondecryptor	Portable	Credentialss	Free
credentialsfileview	Portable	Credentials	Free
FTK Imager Lite	Portable	Imaging	Free
Belkasoft Acq. Tool	Portable	Imaging	Free
Roadkil Disk Image	Portable	Imaging	Free
MAGNET Acquire	Installer	Imaging	Free*
Tableau Imager	Installer	Imaging	Free*
FTK Imager 4.2.1	Installer	Imaging	Free*

*Must Provide Email to Download

with some common relevant forensics artifacts (browser history, credentials) on the Suspect drive.

In this hypothetical Case B451C, a search warrant has been served to a person and their hard drive was seized. Forensics specialists on the scene have started a case file containing some of the pictures and procedures that were taken on site.

Case Notes include some of the steps taken in this case (including but not limited to): taking pictures of any screens when arriving at the suspect's computer, taking pictures of any media attached to the target computer by the forensic specialist, output of any tools executed on the suspect's computer and ending with pulling the power cable out of the suspect's machine and retrieving the internal drives.

The existence of information on the suspect's computer screen lead the forensics specialists to suspect there was an email account being used; some live tools were run on the suspect's system and data was stored on an attached Evidence drive. Pictures of the setup were taken at the scene and are attached in Appendix A.

Process Explorer was used to take a dump of the currently active Microsoft Edge web browser. OpenedFileView was used to look at any files that were being used at the time and a dump was captured.Three RAM captures were taken at the scene using Belkasoft's RAM Capturer, MAGNET Ram Capture and DumpIt with the results in Appendix A.

Since there was evidence suggesting the suspect had an email account, forensics specialists ran a series of credentials finding software (CredentialsFileView, VaultPasswordView, WirelessKeyView, DataProtectionDecryptor) to extract any credentials that could be useful during the investigation.

After all data was stored in the case file, both the evidence drive and the tools flash drive were ejected safely and the power was pulled. A picture of the suspect's drive inside of the machine was taken before bagging and tagging the evidence.

2.5 Itemized Test Plan

- Image initial drive using FTK Image, Belkasoft Captureand Roadkil Disk Image.
- Create a clone using the Cinolink Drive Dock (SATA to SATA).
- Create a clone using Roadkil Disk Image (Image to IDE).
- Validate the cloning results using NIST's CFTT Federated Testing.
- Take forensic images using Windows 10 with professional hardware.
- Take forensic images using Windows 10 with consumer hardware.
- Take forensic images using Windows To Go with professional hardware.
- Take forensic images using Windows To Go with consumer hardware.
- Take forensic images using various Linux distributions with professional hardware.
- Take forensic images using various Linux distributions with consumer hardware.

Most of the testing taking place was around imaging so we began by taking a basic forensic image using the professional grade Tableau T3U SATA bridge of the Suspect Drive. After taking the images using our three target tools (FTK Imager Lite, Belkasoft Capture and Roadkil Disk Image), we made sure the hashes for all three are consistent. After these images are taken, the CinoLink duplicator was used to make a clone from the Suspect Drive to the Clone Drive (SATA). After cloning is complete, images of the Suspect Drive were retaken using the Tableau T3U SATA bridge with the same three tools (FTK Imager Lite, Belkasoft Capture and Roadkil Disk Image) and additional images were taken of the Clone Drive (SATA) using the same methodology. Roadkil Disk Image has additional functionality to write an image back to a disk so we used this tool with the CoolGear (set to non-write protect mode) to make a forensics clone using the original Suspect Drive unto the Clone

Drive (IDE). After cloning is complete, images of the Clone Drive (IDE) were taken using the same methodology as the Clone Drive (SATA). After all images have been taken, the NIST's CFTT Federated TestingThelma.allen@nist.gov (2020) was used to validate the cloning capabilities of the tools used (CinoLink Duplicator and Roadkil Disk Image).

This testing completed the setup phase for all followup tests and the hashes extracted from these were considered the canonical truth for all followup tests; any deviation from the results acquired at this stage was be considered to be a test failure against the consumer grade hardware or software. Roadkil Disk Image was be used in a test failure to attempt to reset the media back to the original state before continuing on.

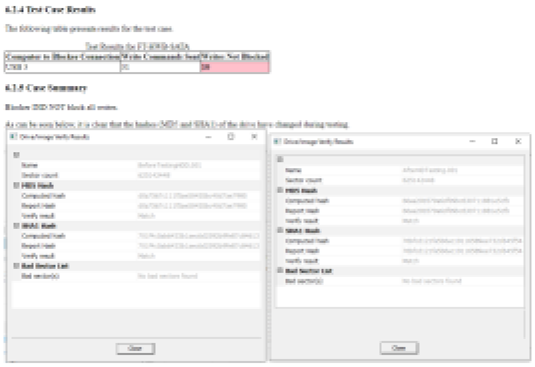
After setup has been completed, the following tests were be performed for each scenario outlined: forensic image of Suspect Drive using CoolGear hardware, forensic image of Clone (SATA) using CoolGear hardware, forensic image of Clone (IDE) using CoolGear hardware.

The following scenarios were be tested: Examiner Windows Machine containing FTK Imager, Belkasoft Capture, Roadkil Disk Image; Windows to Go Flash Drive containing Magnet Acquire, Tableau Imager, FTK Imager v4.2.1; Caine 11 containing Guymager; Kali Linux 2020 (forensics mode) containing Guymager; Kali Linux 2020 (live mode) contating Guymager; Parrot 4.7 (forensics mode) containing Guymager; Parrot 4.7 (live mode) containing Guymager; OSFClone 1.2.1000 containing Image Drive options; Deft (UEFI) containing Guymager; Paladin 7 (read only) containing Imager; Paladin Edge 64 (read only) containing Imager; Paladin 7 (read-write) containing Imager; Palading Edge (read-write) containing Imager.

3. TESTING

3.1 Setup Phase

Hardware Write Blocker testing under the NIST's CFTT Federated TestingThelma.allen@nist.gov (2020) suite shows that the the CoolGear device does not adequately protect the writes on disk from Linux in both the Suspect SSD and Clone Drive connected through SATA (Figure 8 and Figure 9). These results were passed to NIST and will included in an unpublished future report.



6.1.4 Test Case Results

The following table presents results for the test case.

Test Results for FT-HWB-SATA

Computer to Blocker Connection	Write Commands Sent	Writes Not Blocked
USB 3	[illegible]	[illegible]

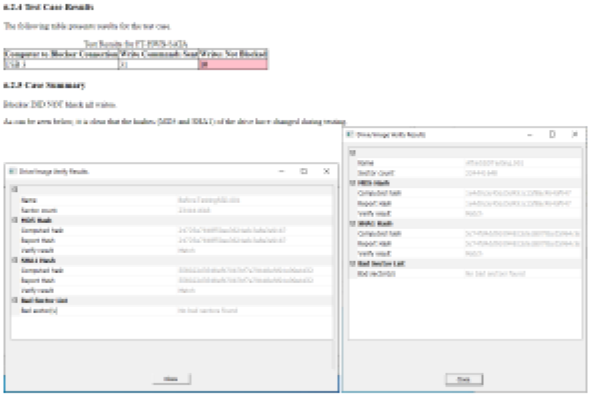
6.1.5 Case Summary

Blocker DID NOT block all writes.

As can be seen below, it is clear that the hashes (MD5 and SHA1) of the drive have changed during testing.

Figure 3. CoolGear Write Block SATA SSD Linux

Hardware Writer Blocker testing using CRU's Write Blocker Validation Utility shows that the the CoolGear device does not adequately protect the writes on disk from Win-



6.2.4 Test Case Results

The following table presents results for the test case.

Test Results for FT-HWB-SATA

Computer to Blocker Connection	Write Commands Sent	Writes Not Blocked
USB 3	[illegible]	[illegible]

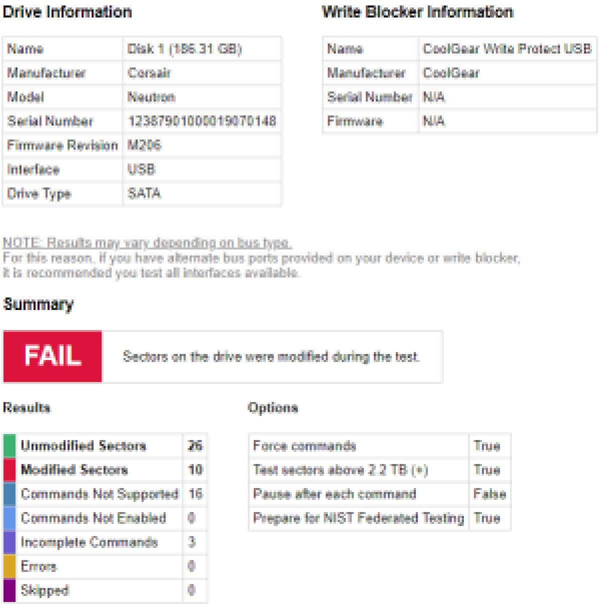
6.2.5 Case Summary

Blocker DID NOT block all writes.

As can be seen below, it is clear that the hashes (MD5 and SHA1) of the drive have changed during testing.

Figure 4. CoolGear Write Block SATA HDD Linux

dows in three instances (Figures 5, 6 and 7) of testing (two SSDs and one HDD)



Drive Information

Name	Disk 1 (186.31 GB)
Manufacturer	Corsair
Model	Neutron
Serial Number	12387901000019070148
Firmware Revision	M206
Interface	USB
Drive Type	SATA

Write Blocker Information

Name	CoolGear Write Protect USB
Manufacturer	CoolGear
Serial Number	N/A
Firmware	N/A

NOTE: Results may vary depending on bus type.
For this reason, if you have alternate bus ports provided on your device or write blocker,
it is recommended you test all interfaces available.

Summary

FAIL Sectors on the drive were modified during the test.

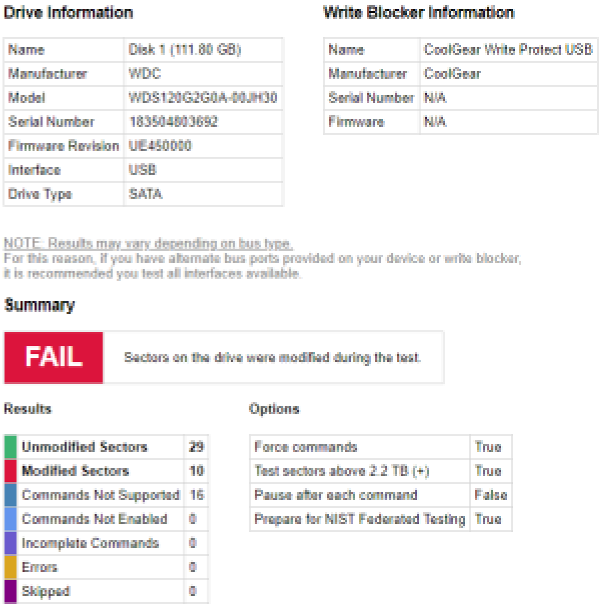
Results

🟩	Unmodified Sectors	26
🟥	Modified Sectors	10
🟦	Commands Not Supported	16
🟦	Commands Not Enabled	0
🟪	Incomplete Commands	3
🟧	Errors	0
🟪	Skipped	0

Options

Force commands	True
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	True

Figure 5. CoolGear Write Block SATA SSD Windows



Drive Information

Name	Disk 1 (111.80 GB)
Manufacturer	WDC
Model	WDS120G2G0A-00JH30
Serial Number	183504803692
Firmware Revision	UE450000
Interface	USB
Drive Type	SATA

Write Blocker Information

Name	CoolGear Write Protect USB
Manufacturer	CoolGear
Serial Number	N/A
Firmware	N/A

NOTE: Results may vary depending on bus type.
For this reason, if you have alternate bus ports provided on your device or write blocker,
it is recommended you test all interfaces available.

Summary

FAIL Sectors on the drive were modified during the test.

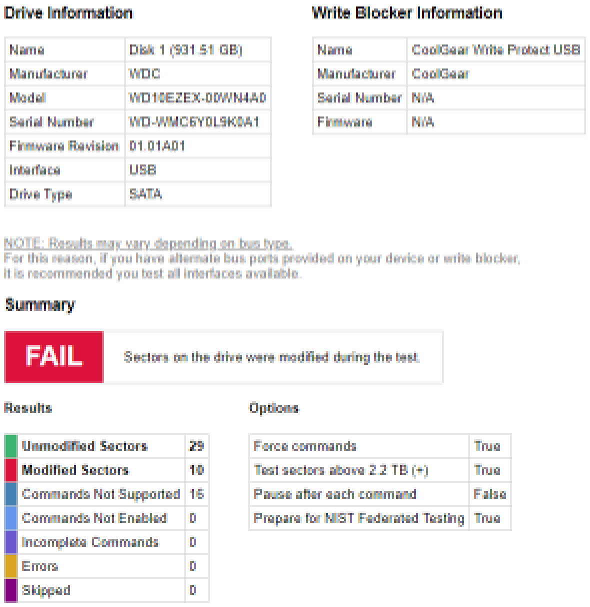
Results

🟩	Unmodified Sectors	29
🟥	Modified Sectors	10
🟦	Commands Not Supported	16
🟦	Commands Not Enabled	0
🟪	Incomplete Commands	0
🟧	Errors	0
🟪	Skipped	0

Options

Force commands	True
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	True

Figure 6. CoolGear Write Block SATA SSD Windows



Drive Information

Name	Disk 1 (931.51 GB)
Manufacturer	WDC
Model	WD10EZEX-00WN4A0
Serial Number	WD-WMC6Y0L9K0A1
Firmware Revision	01.01A01
Interface	USB
Drive Type	SATA

Write Blocker Information

Name	CoolGear Write Protect USB
Manufacturer	CoolGear
Serial Number	N/A
Firmware	N/A

NOTE: Results may vary depending on bus type.
For this reason, if you have alternate bus ports provided on your device or write blocker,
it is recommended you test all interfaces available.

Summary

FAIL Sectors on the drive were modified during the test.

Results

🟩	Unmodified Sectors	29
🟥	Modified Sectors	10
🟦	Commands Not Supported	16
🟦	Commands Not Enabled	0
🟪	Incomplete Commands	0
🟧	Errors	0
🟪	Skipped	0

Options

Force commands	True
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	True

Figure 7. CoolGear Write Block SATA HDD Windows

At this point, an image of the original was made before any of the testing using the three tools (Figures 14, 15 and 16). Pictures of the setup (Figure 13) and results (Table 9 and 10) as well as an issue found with Diskimage being unable to capture an image for this.

The first set of problems is encountered here as Roadkil's Diskimage is unable to image the drive through the Tableau T3U (Figure 17). The actual images are different by 24kb so it appears to have stopped near the end of the capture (Figure 18).

After capturing the images, NIST's suite was used to initialize the disks for testing. The first of the consumer grade tests was performed taking a 'forensic copy' using the Cinolink hardware (Figure 21 and 22). After cloning was completed, the NIST suite validated the clone and results were passed to NIST's CFTT Federated TestingThelma.allen@nist.gov (2020) as well as validating using FTK Imager and Belkasoft (Figure 23, 24 and 25) and using the hashes (Table 12 and 13).

At this moment, AccessData revoked the certificates for FTK Imager Lite and we were unable to use it for further testing. We retake

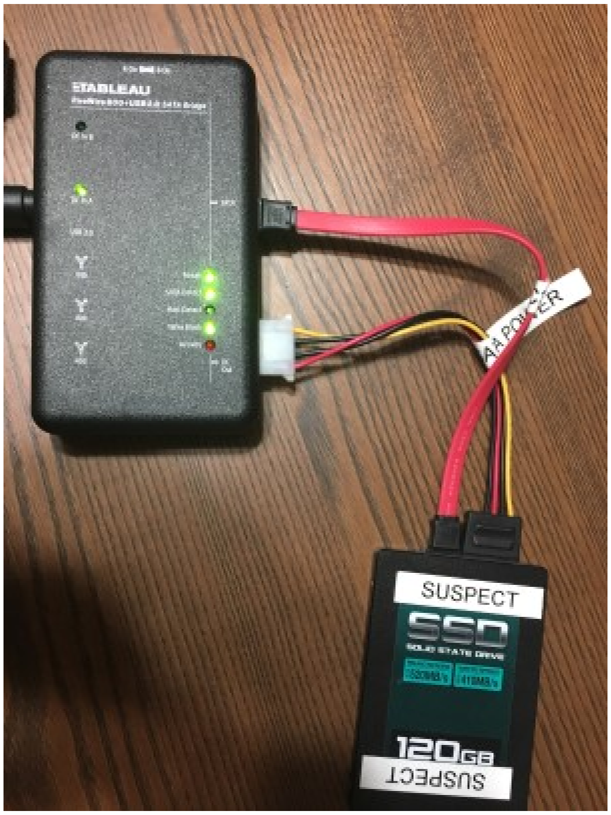


Figure 8. Initial Image Setup

Table 9. Initial Images MD5*

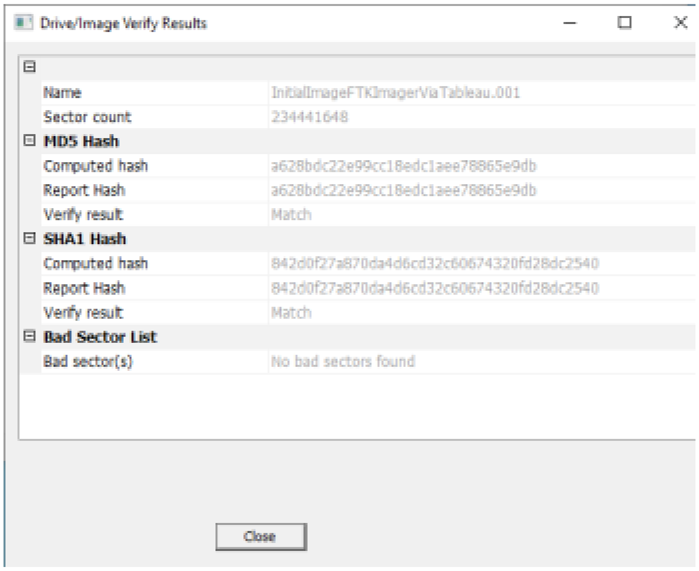
Tool Used	**Results**
	MD5
FTK Imager Lite	a628bdc22e99cc18edc1aee78865e9db
Belkasoft Capturer	a628bdc22e99cc18edc1aee78865e9db*
Roadkill Diskimage	Fail To Capture

*Hash Adjusted To Lowercase

Table 10. Initial Images SHA1

Tool Used	**Results**
	SHA1
FTK Imager Lite	842d0f27a870da4d6cd32c60674320fd28dc2540
Belkasoft Capturer	842d0f27a870da4d6cd32c60674320fd28dc2540*
Roadkill Diskimage	Fail To Capture

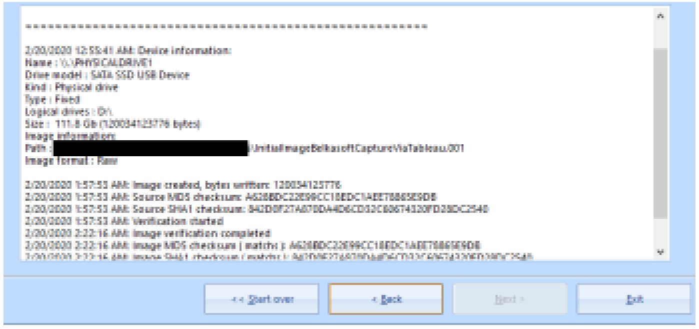
*Hash Adjusted To Lowercase



Drive/Image Verify Results

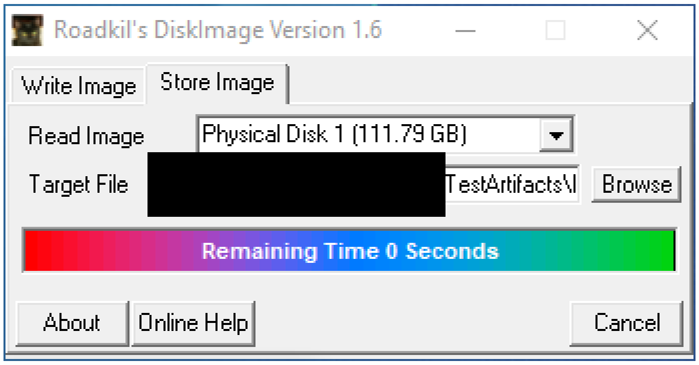
Name	InitialImageFTKImagerViaTableau.001
Sector count	234441648
MD5 Hash	
Computed hash	a628bdc22e99cc18edc1aee78865e9db
Report Hash	a628bdc22e99cc18edc1aee78865e9db
Verify result	Match
SHA1 Hash	
Computed hash	842d0f27a870da4d6cd32c60674320fd28dc2540
Report Hash	842d0f27a870da4d6cd32c60674320fd28dc2540
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Figure 9. Initial FTK Image Verification



```
************************************************************

2/20/2020 12:55:41 AM: Device information:
Name : \\.\PHYSICALDRIVE1
Drive model : SATA SSD USB Device
Kind : Physical drive
Type : Fixed
Logical drives : D:\
Size : 111.8 Gb (120034123776 bytes)
Image information:
Path : [redacted]\InitialImageBelkasoftCaptureViaTableau.001
Image format : Raw

2/20/2020 1:57:53 AM: Image created, bytes written: 120034123776
2/20/2020 1:57:53 AM: Source MD5 checksum: A628BDC22E99CC18EDC1AEE78865E9DB
2/20/2020 1:57:53 AM: Source SHA1 checksum: 842D0F27A870DA4D6CD32C60674320FD28DC2540
2/20/2020 1:57:53 AM: Verification started
2/20/2020 2:22:16 AM: Image verification completed
2/20/2020 2:22:16 AM: Image MD5 checksum ( match ): A628BDC22E99CC18EDC1AEE78865E9DB
2/20/2020 2:22:16 AM: Image SHA1 checksum ( match ): 842D0F27A870DA4D6CD32C60674320FD28DC2540
```

Figure 10. Initial Belkasoft Capture Image Verification



Roadkil's DiskImage Version 1.6

Read Image: Physical Disk 1 (111.79 GB)

Target File: [redacted]TestArtifacts\I

Remaining Time 0 Seconds

Figure 11. Roadkil's Diskimage at 100%

the same images as before of the Suspect Drive with FTK Imager and Belkasoft.

This test shows that this drive duplicator is capable of operating without contaminating data for this specific drive (Table 11).

Table 11. Suspect Drive Images CinoLink after Cloning

Tool Used	Results	
	MD5 Match	*SHA1 Match*
FTK Imager	Yes	Yes
Belkasoft Capturer	Yes	Yes

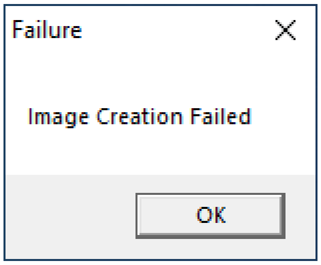

Failure

Image Creation Failed

Figure 12. Roadkil's Diskimage Error

After this point, images of the cloned drive were supposed to be taken but the Tableau T3U did not recognize the cloned drive (note the SATA detect light is not detecting the drive on Figure 26) so images had to be taken with the Coolgear 'write protect' hardware (note both IDE and SATA have been switched to the 'lock' providing write blocking capability on Figure 27) using the same tools. The clones were validated using FTK Imager and Belkasoft (Figure 28 and Figure 29).

At this point, the CoolGear 'write protect' hardware was supposed to be used to write an image back to the IDE drive, but it appears there is a glitch under Windows which does not allow IDE drives to be written to even if write protection is disabled. This information was passed to the manufacturer via support ticket.

An existing consumer product (ULTRA USB 2.0 to IDE / SATA adapter) was used to forensically wipe the drive using Roadkil's Diskwipe. After wiping the drive, NIST's suite was used to initialize the disks for testing. The second of the consumer grade tests was performed by writing a 'forensic image' using Roadkil's Diskwipe (Figure 30).

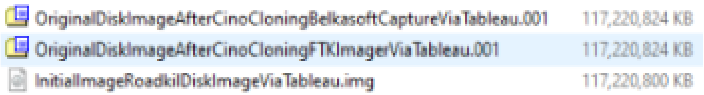
After cloning was completed, the NIST suite validated the clone and results were passed to NIST's CFTT Federated TestingThelma.allen@nist.gov (2020) and using FTK Imager and Belkasoft (Figure 31, 32 and 33). We validated the hashes again (Table 14) to ensure there was no spoilage and the hashes afterwards (Table 16 and 17)

3.2 Imaging Phase

All testing in the Imaging Phase will occur using the CoolGear 'write protect' hardware. All of the initial drives (Suspect, Clone, Clone IDE) was imaged using the hardware and any failures were reset using Roadkil' DiskImage.

Tests for Windows Live Tools were performed using FTK Imager Lite, Belkasoft Capturer and Roadkil's DiskImage randomizing the order in which the tools are run, and hashing (MD5 and SHA1) was performed on the output to validate whether the media was modified (Table 17, 18 and 19). Before beginning the Live Tools testing under Windows, signtool.exe from the Windows 10 SDK was used to remove the revoked certificate from AccessData on FTK Imager Lite (Figure 36). This will allow for testing to be performed using FTK Imager Lite until there is a long term fix for this issue.

Tests for Windows To Go Tools were performed using FTK Imager 4.2.1.4, Magnet ACQUIRE and Tableau Imager randomizing the order in which the tools are run (Table 20, 21 and 22). Tableau Imager failed to capture



```
OriginalDiskImageAfterCinoCloningBelkasoftCaptureViaTableau.001   117,220,824 KB
OriginalDiskImageAfterCinoCloningFTKImagerViaTableau.001          117,220,824 KB
InitialImageRoadkilDiskImageViaTableau.img                        117,220,800 KB
```

Figure 13. Image Size Differences*

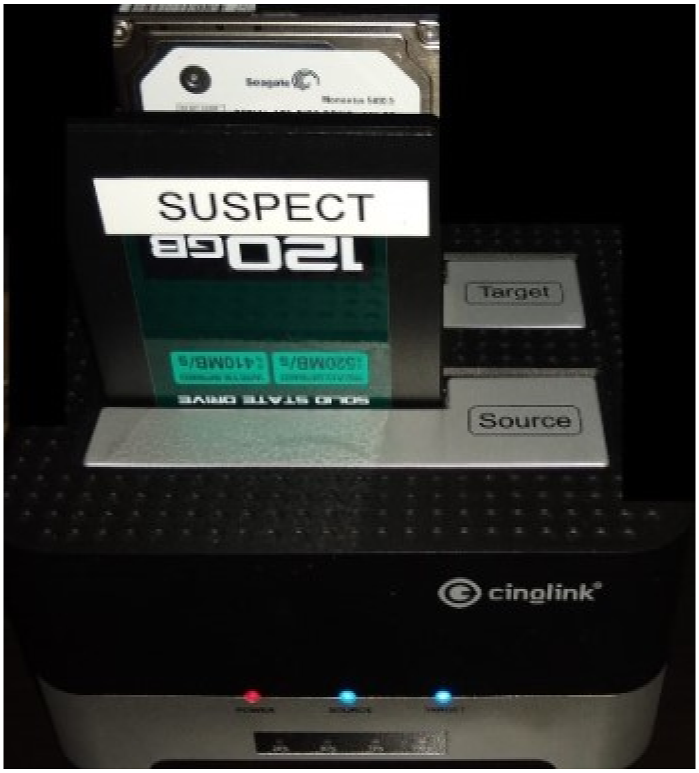


Figure 14. Cino Link Setup

Table 12. CinoLink Clone Images MD5*

Tool Used	Results
	MD5
FTK Imager	5ad9ae0912793248c8ba8d7c31a5bd6f
Belkasoft Capturer	5ad9ae0912793248c8ba8d7c31a5bd6f*

*Hash Adjusted To Lowercase

the images as it was not connected using a Tableau Forensic Bridge Tilbury (2010) (Figure 30).

After Windows To Go Imaging was completed, work began on Linux-based imaging solutions to validate the write blocking capabilities of the CoolGear Write Protect.This hardware has issues blocking some of the writes under the CFTT Testing SuiteThelma.allen@nist.gov (2020), so this testing was critical to find any flaws. CAINE 11, Kali Linux 2020 (forensics), Kali Linux 2020 (live), Parrot 4.7 (forensics), Parrot 4.7 (live), BackBox 6 (live) OSFClone 1.2.1000,

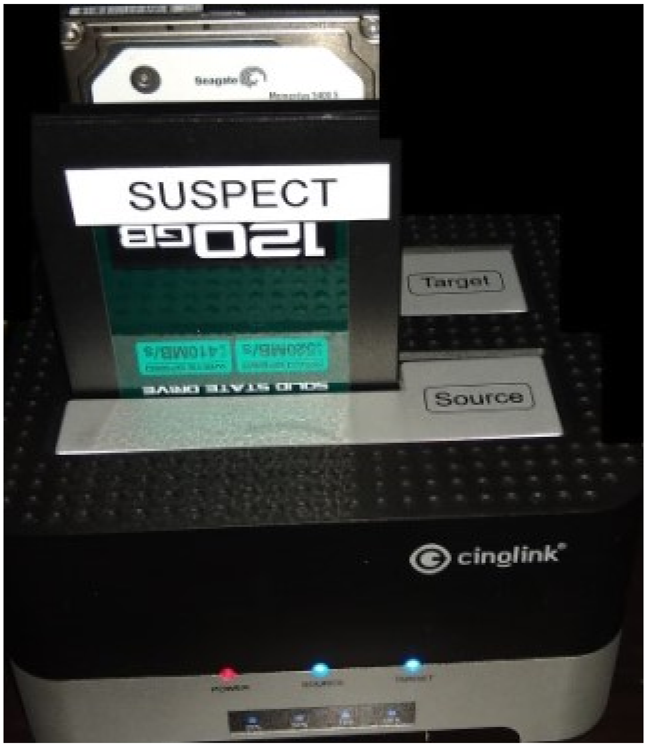
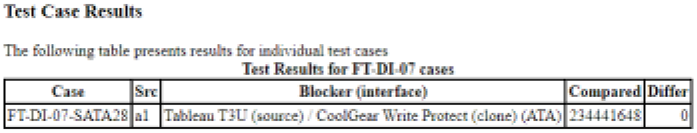


Figure 15. Cino Link 100% Cloned



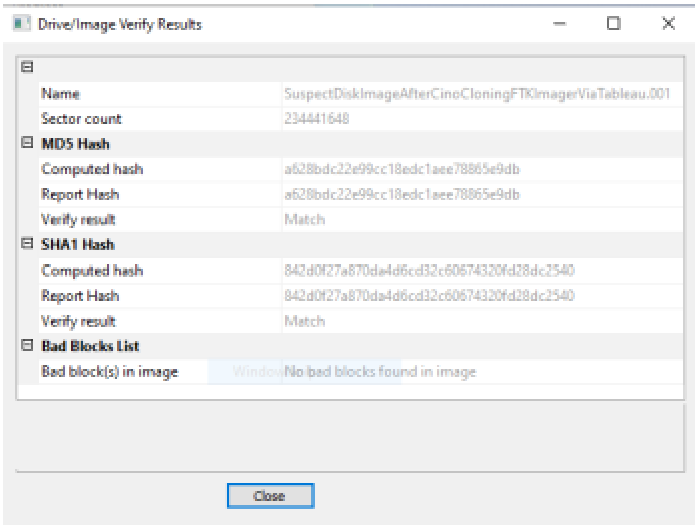
Test Case Results

The following table presents results for individual test cases

Test Results for FT-DI-07 cases

Case	Src	Blocker (interface)	Compared	Differ
FT-DI-07-SATA28	a1	Tableau T3U (source) / CoolGear Write Protect (clone) (ATA)	234441648	0

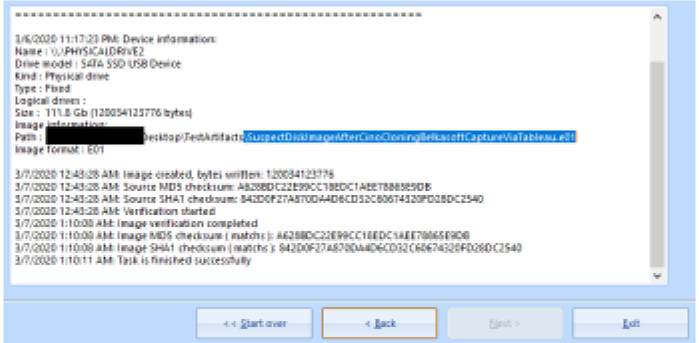
Figure 16. NIST CinoLink Cloning Results



Drive/Image Verify Results

Name	SuspectDiskImageAfterCinoCloningFTKImagerViaTableau.001
Sector count	234441648
MD5 Hash	
Computed hash	a628bdc22e99cc18edc1aee78865e9db
Report Hash	a628bdc22e99cc18edc1aee78865e9db
Verify result	Match
SHA1 Hash	
Computed hash	842d0f27a870da4d6cd32c60674320fd28dc2540
Report Hash	842d0f27a870da4d6cd32c60674320fd28dc2540
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 17. After Cloning Suspect FTK Imager Image Verification



```
==========================================================

3/6/2020 11:17:23 PM: Device information:
Name : \\.\PHYSICALDRIVE2
Drive model : SATA SSD USB Device
Kind : Physical drive
Type : Fixed
Logical drives :
Size : 111.8 Gb (120034123776 bytes)
Image information:
Path : [redacted]Desktop\TestArtifacts\SuspectDiskImageAfterCinoCloningBelkasoftCaptureViaTableau.e01
Image format : E01

3/7/2020 12:43:28 AM: Image created, bytes written: 120034123776
3/7/2020 12:43:28 AM: Source MD5 checksum: A628BDC22E99CC18EDC1AEE78865E9DB
3/7/2020 12:43:28 AM: Source SHA1 checksum: 842D0F27A870DA4D6CD32C60674320FD28DC2540
3/7/2020 12:43:28 AM: Verification started
3/7/2020 1:10:08 AM: Image verification completed
3/7/2020 1:10:08 AM: Image MD5 checksum ( matchs ): A628BDC22E99CC18EDC1AEE78865E9DB
3/7/2020 1:10:08 AM: Image SHA1 checksum ( matchs ): 842D0F27A870DA4D6CD32C60674320FD28DC2540
3/7/2020 1:10:11 AM: Task is finished successfully
```

Figure 18. After Cloning Suspect Belkasoft Capture Image Verification

Table 13. CinoLink Clone Images SHA1*

Tool Used	**Results**
	SHA1
FTK Imager	4efbe81336e50241c59dacc0f88988e17b0325dd
Belkasoft Capturer	4efbe81336e50241c59dacc0f88988e17b0325dd*

*Hash Adjusted To Lowercase

Table 14. Suspect Drive Images After Roadkil's DiskImage after Cloning

Tool Used	**Results**	
	MD5 Match	***SHA1 Match***
FTK Imager	Yes	Yes
Belkasoft Capturer	Yes	Yes

Table 15. Roadkil's DiskImage Clone Images MD5

Tool Used	**Results**
	MD5
FTK Imager	b03151f0cf812257e71a0d1d9cc60c17
Belkasoft Capturer	b03151f0cf812257e71a0d1d9cc60c17*

*Hash Adjusted To Lowercase

DEFT 8, Padalin Edge and Paladin 7 were used in these set of tests. Each distribution was booted using YUMI Multiboot Pendrivelinux.com (2020) and used to take the same images (Suspect, Clone SATA and Clone IDE) from the test media using the CoolGear Write Protect hardware and hashing (MD5 and SHA1) was performed on the output to validate whether the media was modified (Table 23, 24 and 25).

Table 16. Roadkil's DiskImage Clone Images SHA1*

Tool	**Results**
Used	***SHA1***
FTK Imager	25d97f03dae9607ae7206e7f82be78ca17c317d5
Belkasoft Capturer	25d97f03dae9607ae7206e7f82be78ca17c317d5*

*Hash Adjusted To Lowercase

Table 17. Windows Live Imaging - Suspect

Tool	**Results**	
Used	***MD5 Match***	***SHA1 Match***
FTK Imager Lite	Yes	Yes
Belkasoft Capturer	Yes	Yes
Roadkil's DiskImage	Fail to Capture	Fail to Capture

Table 18. Windows Live Imaging - Clone SATA

Tool	**Results**	
Used	***MD5 Match***	***SHA1 Match***
FTK Imager Lite	Yes	Yes
Belkasoft Capturer	Yes	Yes
Roadkil's DiskImage	Fail to Capture	Fail to Capture

Table 19. Windows Live Imaging - Clone IDE

Tool	**Results**	
Used	***MD5 Match***	***SHA1 Match***
FTK Imager Lite	Yes	Yes
Belkasoft Capturer	Yes	Yes
Roadkil's DiskImage	Fail to Capture	Fail to Capture

Differences in mounting policy among Linux suites should be considered when testing tools. CAINE 11 mounted all volumes as read only; Kali Linux 2020 and Parrot 4.7 did not mount any volumes (even in live non-forensics mode); BackBox 6 did not mount the internal volumes, but mounted the external volumes as read / write; OSFClone asked before mounting volumes for writing (and unmounted as soon as writing was completed); DEFT 8.2 did not mount any volumes; Paladin Edge and Paladin 7 did not mount any

Table 20. Windows To Go Imaging - Suspect

Tool Used	**Results**	
	MD5 Match	***SHA1 Match***
FTK Imager 4.2.1.4	Yes	Yes
MAGNET Acquire	Yes	Yes
Tableau Imager	Fail to Capture*	Fail to Capture*

Table 21. Windows To Go Imaging - Clone SATA

Tool Used	**Results**	
	MD5 Match	***SHA1 Match***
FTK Imager 4.2.1.4	Yes	Yes
MAGNET Acquire	Yes	Yes
Tableau Imager	Fail to Capture*	Fail to Capture*

Table 22. Windows To Go Imaging - Clone IDE

Tool Used	**Results**	
	MD5 Match	***SHA1 Match***
FTK Imager 4.2.1.4	Yes	Yes
MAGNET Acquire	Yes	Yes
Tableau Imager	Fail to Capture*	Fail to Capture*

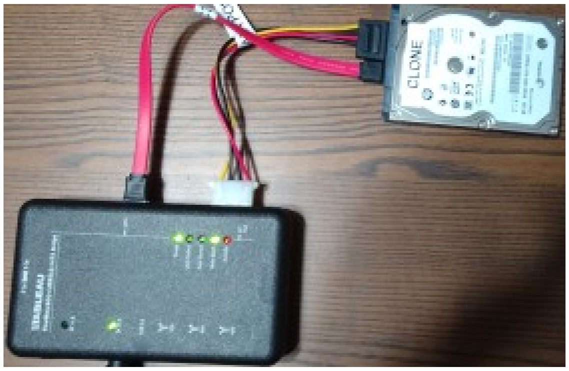


Figure 19. Tableau T3U Not Recognizing Drive

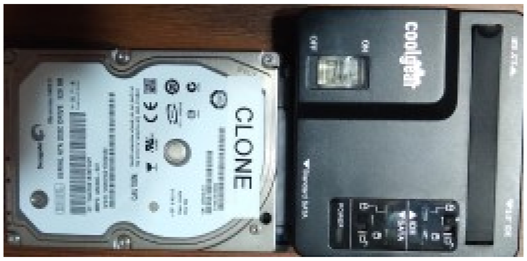
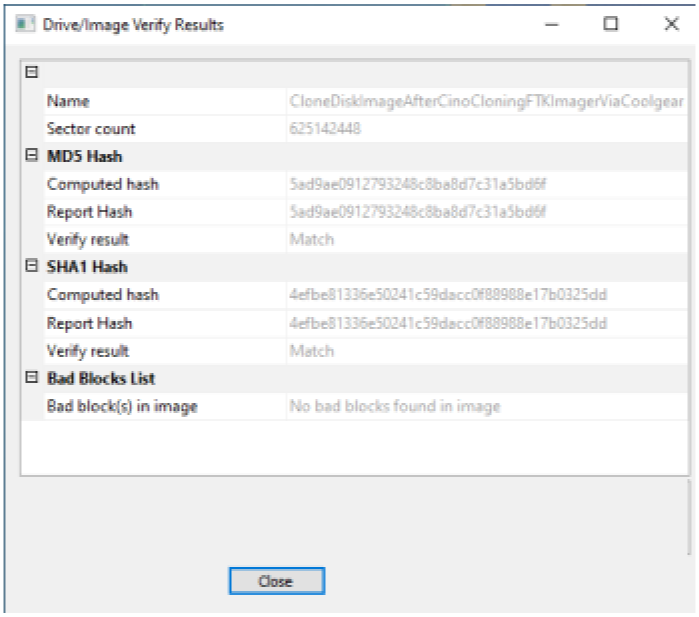


Figure 20. CoolGear Configuration

volumes, did not allow mounting the disks as read/write, and does not allow imaging when volumes are mounted.

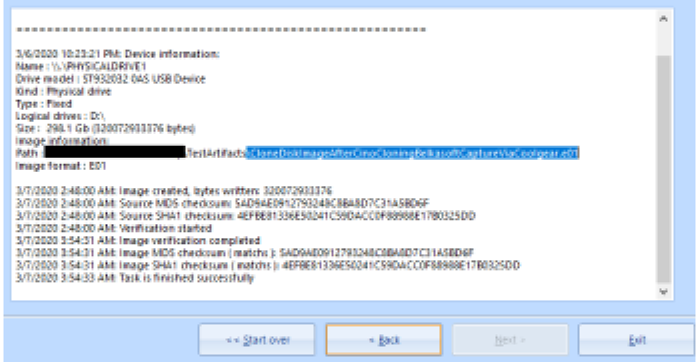
The following devices (Nvidia Flash Drive, Netac SD Card, and WD Blue) had to be cleaned by diskpart before they could be 'wiped' by Roadkil's Diskwipe (Figure 34).



Drive/Image Verify Results

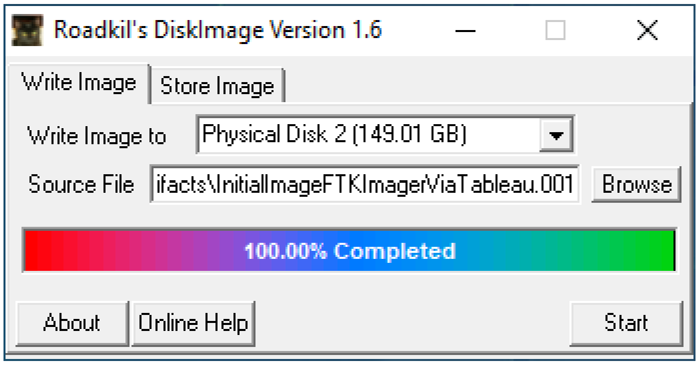
Name	CloneDiskImageAfterCinoCloningFTKImagerViaCoolgear
Sector count	625142448
MD5 Hash	
Computed hash	5ad9ae0912793248c8ba8d7c31a5bd6f
Report Hash	5ad9ae0912793248c8ba8d7c31a5bd6f
Verify result	Match
SHA1 Hash	
Computed hash	4efbe81336e50241c59dacc0f88988e17b0325dd
Report Hash	4efbe81336e50241c59dacc0f88988e17b0325dd
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 21. Clone FTK Image Verification



```
================================================================

3/6/2020 10:23:21 PM: Device information:
Name : \\.\PHYSICALDRIVE1
Drive model : ST932032 0AS USB Device
Kind : Physical drive
Type : Fixed
Logical drives : D:\
Size :  298.1 Gb (320072933376 bytes)
Image information:
Path : [redacted]\TestArtifacts\CloneDiskImageAfterCinoCloningBelkasoftCaptureViaCoolgear.e01
Image format : E01

3/7/2020 2:48:00 AM: Image created, bytes written: 320072933376
3/7/2020 2:48:00 AM: Source MD5 checksum: 5AD9AE0912793248C8BA8D7C31A5BD6F
3/7/2020 2:48:00 AM: Source SHA1 checksum: 4EFBE81336E50241C59DACC0F88988E17B0325DD
3/7/2020 2:48:00 AM: Verification started
3/7/2020 3:54:31 AM: Image verification completed
3/7/2020 3:54:31 AM: Image MD5 checksum ( matchs ): 5AD9AE0912793248C8BA8D7C31A5BD6F
3/7/2020 3:54:31 AM: Image SHA1 checksum ( matchs ): 4EFBE81336E50241C59DACC0F88988E17B0325DD
3/7/2020 3:54:33 AM: Task is finished successfully
```

Figure 22. Clone Belkasoft Capture Image Verification



Roadkil's DiskImage Version 1.6

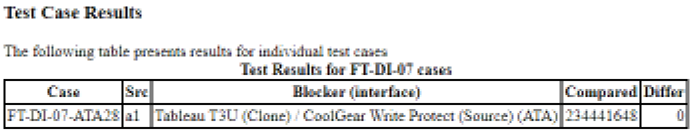
Write Image to: Physical Disk 2 (149.01 GB)

Source File: ifacts\InitialImageFTKImagerViaTableau.001

100.00% Completed

Figure 23. Clone IDE HDD Written

After completing the testing for imaging, testing was performed for Forensic Wiping using Roadkil's Diskwipe and NIST's CFTT Federated Testing Thelma.allen@nist.gov



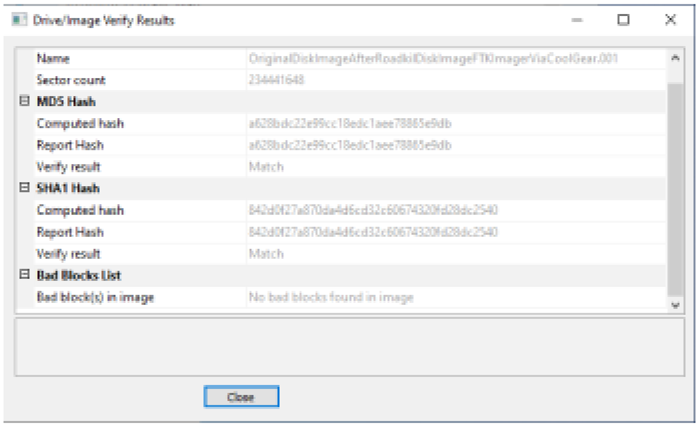
Test Case Results

The following table presents results for individual test cases

Test Results for FT-DI-07 cases

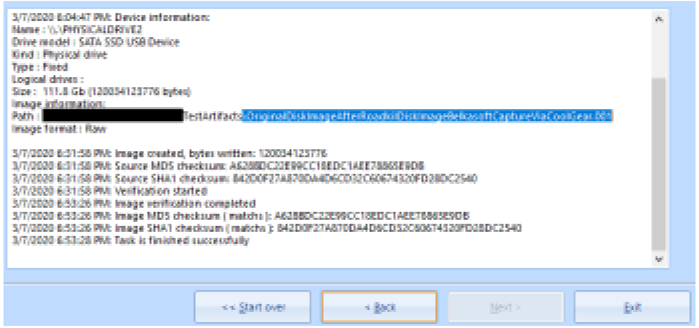
Case	Src	Blocker (interface)	Compared	Differ
FT-DI-07-ATA28	a1	Tableau T3U (Clone) / CoolGear Write Protect (Source) (ATA)	234441648	0

Figure 24. NIST Roadkil's DiskImage Cloning Results



Name	OriginalDiskImageAfterRoadkilDiskImageFTKImagerViaCoolGear.001
Sector count	234441648
⊟ **MD5 Hash**	
Computed hash	a628bdc22e99cc18edc1aee78865e9db
Report Hash	a628bdc22e99cc18edc1aee78865e9db
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	842d0f27a870da4d6cd32c60674320fd28dc2540
Report Hash	842d0f27a870da4d6cd32c60674320fd28dc2540
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

Figure 25. After Validating IDE Suspect FTK Imager Image Verification



```
3/7/2020 6:04:47 PM: Device information:
Name : \\.\PHYSICALDRIVE2
Drive model : SATA SSD USB Device
Kind : Physical drive
Type : Fixed
Logical drives :
Size :  111.8 Gb (120034123776 bytes)
Image information:
Path : [redacted]TestArtifacts\OriginalDiskImageAfterRoadkilDiskImageBelkasoftCaptureViaCoolGear.001
Image format : Raw

3/7/2020 6:31:58 PM: Image created, bytes written: 120034123776
3/7/2020 6:31:58 PM: Source MD5 checksum: A628BDC22E99CC18EDC1AEE78865E9DB
3/7/2020 6:31:58 PM: Source SHA1 checksum: 842D0F27A870DA4D6CD32C60674320FD28DC2540
3/7/2020 6:31:58 PM: Verification started
3/7/2020 6:53:26 PM: Image verification completed
3/7/2020 6:53:26 PM: Image MD5 checksum ( matchs ): A628BDC22E99CC18EDC1AEE78865E9DB
3/7/2020 6:53:26 PM: Image SHA1 checksum ( matchs ): 842D0F27A870DA4D6CD32C60674320FD28DC2540
3/7/2020 6:53:28 PM: Task is finished successfully
```

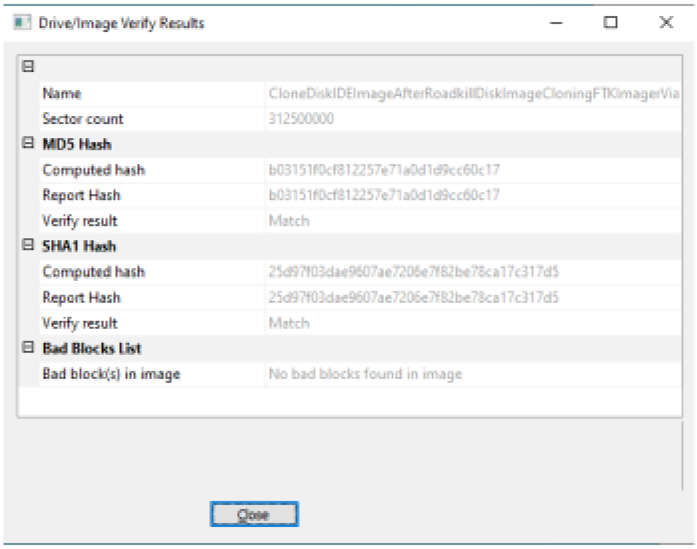
Figure 26. After Validating IDE Suspect Belkasoft Capture Image Verification

(2020) suite. Results were passed to NIST for future publications (Figure 35, Figure 36, and Table 26).

4. CONCLUSION

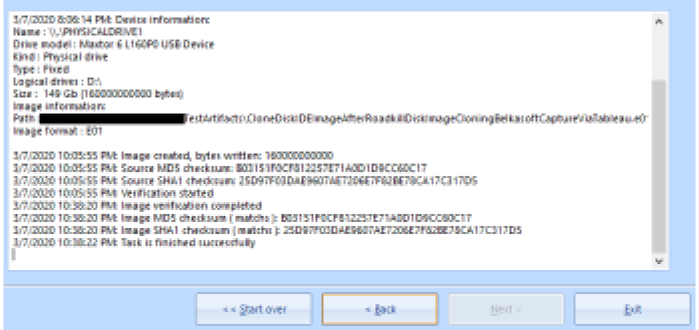
The consumer grade software tested (Roadkil's DiskWipe and Roadkil's DiskImage) were able to pass some of the NIST suite of tests in a variety of scenarios. Roadkil's DiskWipe was not able to fully wipe any of the target disksof Homeland Security (DHS) Science & (ST) (2020c) while Roadkil's DiskImage was able to write an image back to a disk successfully although it had some issues acquiring images from disksof Homeland Security (DHS) Science & (ST) (2020b).

The consumer grade hardware tested (Cinolink Dual HDD Dock and CoolGear Write Protect) were able to pass some of the NIST suite of tests. Cinolink Dual HDD Dock was able to perform a forensic clone of multiple SATA disks without contaminating the original deviceof Homeland Security (DHS) Science & (ST) (2020a) while the CoolGear Write Protect had issues maintaining



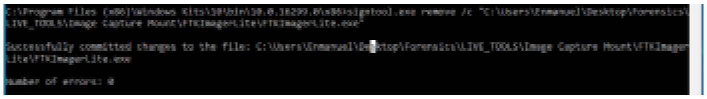
Name	CloneDiskIDEImageAfterRoadkillDiskImageCloningFTKImagerVia
Sector count	312500000
MD5 Hash	
Computed hash	b03151f0cf812257e71a0d1d9cc60c17
Report Hash	b03151f0cf812257e71a0d1d9cc60c17
Verify result	Match
SHA1 Hash	
Computed hash	25d97f03dae9607ae7206e7f82be78ca17c317d5
Report Hash	25d97f03dae9607ae7206e7f82be78ca17c317d5
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 27. Clone IDE FTK Image Verification



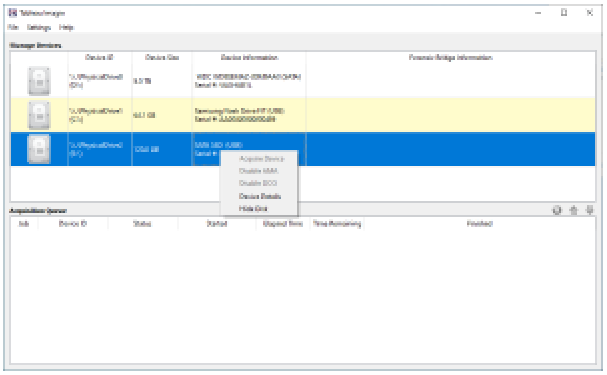
```
3/7/2020 8:06:14 PM: Device information:
Name : \\.\PHYSICALDRIVE1
Drive model : Maxtor 6 L160P0 USB Device
Kind : Physical drive
Type : Fixed
Logical drives : D:\
Size :  149 Gb (160000000000 bytes)
Image information:
Path : [redacted]TestArtifacts\CloneDiskIDEImageAfterRoadkillDiskImageCloningBelkasoftCaptureViaTableau.e0
Image format : E01

3/7/2020 10:05:55 PM: Image created, bytes written: 160000000000
3/7/2020 10:05:55 PM: Source MD5 checksum: B03151F0CF812257E71A0D1D9CC60C17
3/7/2020 10:05:55 PM: Source SHA1 checksum: 25D97F03DAE9607AE7206E7F82BE78CA17C317D5
3/7/2020 10:05:55 PM: Verification started
3/7/2020 10:38:20 PM: Image verification completed
3/7/2020 10:38:20 PM: Image MD5 checksum ( matchs ): B03151F0CF812257E71A0D1D9CC60C17
3/7/2020 10:38:20 PM: Image SHA1 checksum ( matchs ): 25D97F03DAE9607AE7206E7F82BE78CA17C317D5
3/7/2020 10:38:22 PM: Task is finished successfully
```

Figure 28. Clone IDE Belkasoft Capture Image Verification



```
C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x86\signtool.exe remove /c "C:\Users\Emmanuel\Desktop\Forensics\
LIVE_TOOLS\Image Capture Mount\FTKImagerLite\FTKImagerLite.exe"

Successfully committed changes to the file: C:\Users\Emmanuel\Desktop\Forensics\LIVE_TOOLS\Image Capture Mount\FTKImager
Lite\FTKImagerLite.exe

Number of errors: 0
```

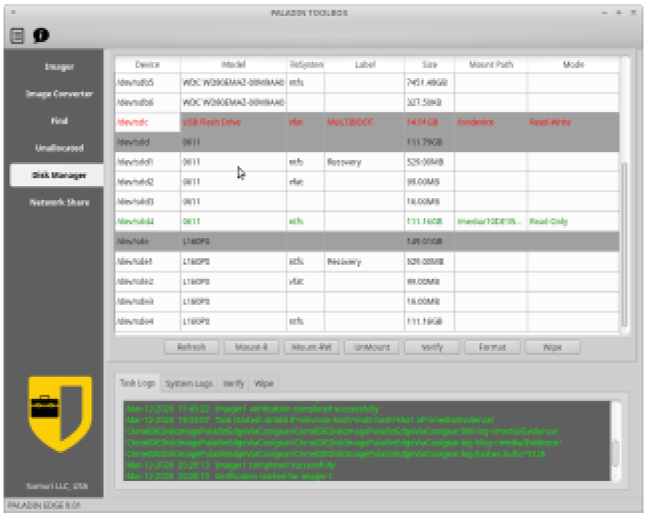
Figure 29. Signtool.exe



Device ID	Device Size	Device Information	Forensic Bridge Information
\\.\PhysicalDrive0 (C:\)	[illegible]	WDC [illegible] Serial # [illegible]	
\\.\PhysicalDrive1 (E:\)	[illegible] GB	Samsung Flash Drive FIT (USB) Serial # [illegible]	
\\.\PhysicalDrive2 (D:\)	[illegible] GB	[illegible] SSD (USB) Serial #	

Job	Device ID	Status	Started	Elapsed Time	Time Remaining	Finished

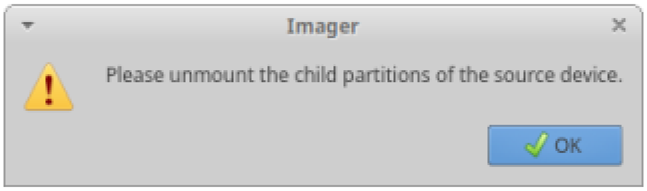
Figure 30. Tableau Imager Fail to Image



Device	Model	FileSystem	Label	Size	Mount Path	Mode
/dev/sdb5	WDC WD80EMAZ-00WJTA0	ntfs		7451.48GB		
/dev/sdb6	WDC WD80EMAZ-00WJTA0			327.58KB		
/dev/sdc	USB Flash Drive	vfat	MULTIBOOT	14.91GB	/nodevice	Read-Write
/dev/sdd	0X11			111.79GB		
/dev/sdd1	0X11	ntfs	Recovery	529.00MB		
/dev/sdd2	0X11	vfat		99.00MB		
/dev/sdd3	0X11			16.00MB		
/dev/sdd4	0X11	ntfs		111.16GB	/media/10DE1B...	Read-Only
/dev/sde	LT60P0			149.05GB		
/dev/sde1	LT60P0	ntfs	Recovery	529.00MB		
/dev/sde2	LT60P0	vfat		99.00MB		
/dev/sde3	LT60P0			16.00MB		
/dev/sde4	LT60P0	ntfs		111.19GB		

```
Mar-12-2020 11:43:22 Imager1 verification completed successfully
Mar-12-2020 19:33:07 Task started: dd [illegible] /dev/sde [illegible] /media/Evidence/
CloneOfDiskImagePaladinEdgeViaCaiguard/CloneOfDiskImagePaladinEdgeViaCaiguard [illegible] /media/Evidence/
CloneOfDiskImagePaladinEdgeViaCaiguard/CloneOfDiskImagePaladinEdgeViaCaiguard.log [illegible] /media/Evidence/
CloneOfDiskImagePaladinEdgeViaCaiguard/CloneOfDiskImagePaladinEdgeViaCaiguard.log [illegible]
Mar-12-2020 20:28:13 Imager1 completed successfully
Mar-12-2020 20:28:15 Verification started for imager1
```

Figure 31. Paladin Edge Read Only



Please unmount the child partitions of the source device.

Figure 32. Paladin Edge No Mounting While Imaging

Table 23. Linux-based Imaging - Suspect

OS Used	**Tool Used**	**Results**	
		MD5 Match	***SHA1 Match***
CAINE 11	Guymager	Yes	Yes
Kali Linux 2020 (forensics)	Guymager	Yes	Yes
Kali Linux 2020 (live)	Guymager	Yes	Yes
Parrot 4.7 (forensics)	Guymager	Yes	Yes
Parrot 4.7 (live)	Guymager	Yes	Yes
BackBox 6	Guymager	Yes	Yes
OSFClone 1.2.1000	Image	Yes*	Yes*
DEFT 8.2	Guymager	Yes	Yes
Paladin Edge (read)	Imager	Yes	Yes
Paladin Edge (read/write)	Imager	Not Allowed	Not Allowed
Paladin 7 (read)	Imager	Yes	Yes
Paladin 7 (read/write)	Imager	Not Allowed	Not Allowed

*Hash Manually Computed

Table 24. Linux-based Imaging - Clone SATA

OS Used	**Tool Used**	**Results**	
		MD5 Match	***SHA1 Match***
CAINE 11	Guymager	Yes	Yes
Kali Linux 2020 (forensics)	Guymager	Yes	Yes
Kali Linux 2020 (live)	Guymager	Yes	Yes
Parrot 4.7 (forensics)	Guymager	Yes	Yes
Parrot 4.7 (live)	Guymager	Yes	Yes
BackBox 6	Guymager	Yes	Yes
OSFClone 1.2.1000	Image	Yes*	Yes*
DEFT 8.2	Guymager	Yes	Yes
Paladin Edge (read)	Imager	Yes	Yes
Paladin Edge (read/write)	Imager	Not Allowed	Not Allowed
Paladin 7 (read)	Imager	Yes	Yes
Paladin 7 (read/write)	Imager	Not Allowed	Not Allowed

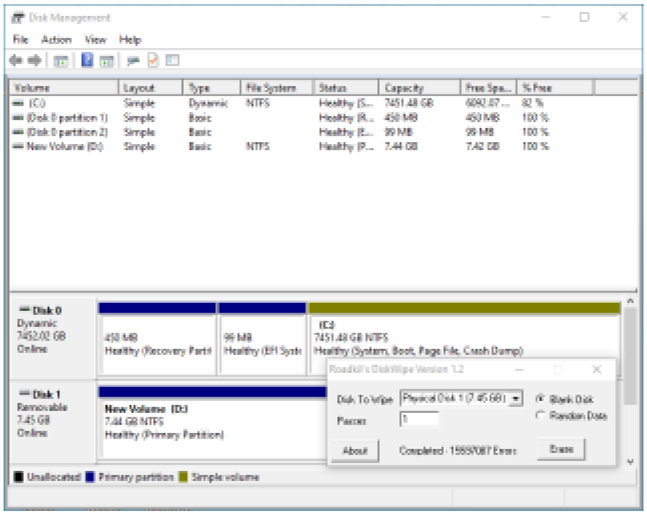
*Hash Manually Computed

Table 25. Linux-based Imaging - Clone IDE

OS Used	**Tool Used**	**Results**	
		MD5 Match	***SHA1 Match***
CAINE 11	Guymager	Yes	Yes
Kali Linux 2020 (forensics)	Guymager	Yes	Yes
Kali Linux 2020 (live)	Guymager	Yes	Yes
Parrot 4.7 (forensics)	Guymager	Yes	Yes
Parrot 4.7 (live)	Guymager	Yes	Yes
BackBox 6	Guymager	Yes	Yes
OSFClone 1.2.1000	Image	Yes*	Yes*
DEFT 8.2	Guymager	Yes	Yes
Paladin Edge (read)	Imager	Yes	Yes
Paladin Edge (read/write)	Imager	Not Allowed	Not Allowed
Paladin 7 (read)	Imager	Yes	Yes
Paladin 7 (read/write)	Imager	Not Allowed	Not Allowed

write protection under Windows and Linux environments. Additional testing of the CoolGear Write Protect shows that most common imaging software under Windows and Linux suites can be used successfully without contaminating devices being write blocked.

Consumer grade software and hardware offers great value for budget conscious organizations wanting to improve the overall



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Dynamic	NTFS	Healthy (S...	7451.48 GB	6092.07 ...	82 %
(Disk 0 partition 1)	Simple	Basic		Healthy (R...	450 MB	450 MB	100 %
(Disk 0 partition 2)	Simple	Basic		Healthy (E...	99 MB	99 MB	100 %
New Volume (D:)	Simple	Basic	NTFS	Healthy (P...	7.44 GB	7.42 GB	100 %

Disk 0
Dynamic
7452.02 GB
Online

450 MB
Healthy (Recovery Parti

99 MB
Healthy (EFI Syste

(C:)
7451.48 GB NTFS
Healthy (System, Boot, Page File, Crash Dump)

Disk 1
Removable
7.45 GB
Online

New Volume (D:)
7.44 GB NTFS
Healthy (Primary Partition)

Disk To Wipe: Physical Disk 1 (7.45 GB)
Passes: 1
● Blank Disk
○ Random Data
Completed - 15597087 Errors

Figure 33. Failed To Wipe

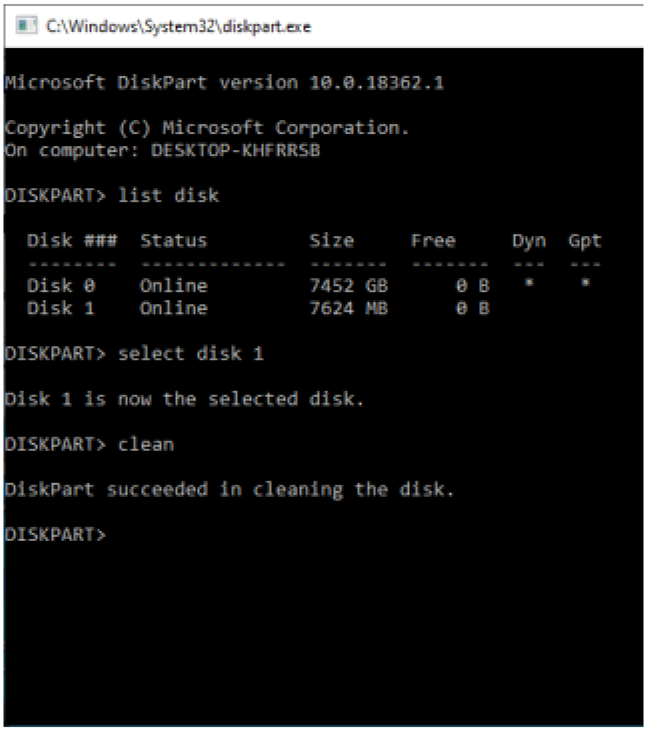
Table 26. Forensic Wipe Testing

Device Used	**Device Capacity**	**Results**	
		Device Type	***Outcome***
Nvidia Flash Drive	64Gb	Flash Drive	Fail
Netac SD Card	8Gb	SD Card	Fail
Inland Professional	120Gb	2.5" SSD	Fail
WD Green	120Gb	2.5" SSD	Fail
Maxtor Diamond 10	160Gb	3.5" HDD	Fail
Corsair Force	200gb	2.5" SSD	Fail
Seagate Momentus	300Gb	3.5" HDD	Fail
Toshiba MQ01ABD100	1Tb	2.5" HDD	Fail
WD Blue	1Tb	3.5" HDD	Fail

technical proficiency of students. This testing shows that the customer grade hardware has forensics value on a budget but is not guaranteed to be usable in a legal setting. Organizations wanting to teach fundamentals can utilize consumer grade hardware for teaching fundamentals and are always advised to validate their hardware using scientific methods and tools as outlined. Utilizing a mixture of open source software and hardware allows for the hardware to produce reproducible results that can be relied upon and shows that there are potential uses of some of this consumer grade hardware and software as long as the limitations that exist within the hardware and software are understood and accounted for.

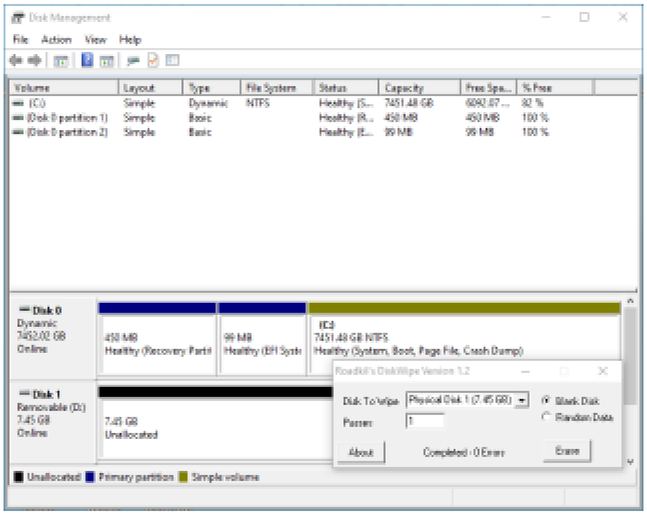
5. FUTURE WORK

Future work can focus on validating the forensic validity of free / open source USB write blockers such as Ratool Sordum.org (2015), Thumbscrew IronGeek (2013), and USB WriteProtector Gaigin.net (2011) against other software based USB write blockers



```
Microsoft DiskPart version 10.0.18362.1

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-KHFRRSB

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online         7452 GB      0 B   *    *
  Disk 1    Online         7624 MB      0 B

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART>
```

Figure 34. Cleaning with diskpart



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Dynamic	NTFS	Healthy (S...	7451.48 GB	6092.07 ...	82 %
(Disk 0 partition 1)	Simple	Basic		Healthy (R...	450 MB	450 MB	100 %
(Disk 0 partition 2)	Simple	Basic		Healthy (E...	99 MB	99 MB	100 %

Disk 0
Dynamic
7452.02 GB
Online

450 MB
Healthy (Recovery Partit

99 MB
Healthy (EFI Syste

(C:)
7451.48 GB NTFS
Healthy (System, Boot, Page File, Crash Dump)

Disk 1
Removable (D:)
7.45 GB
Online

7.45 GB
Unallocated

■ Unallocated ■ Primary partition ■ Simple volume

Roadkil's DiskWipe Version 1.2

Disk To Wipe: Physical Disk 1 (7.45 GB)
Passes: 1
● Blank Disk
○ Random Data

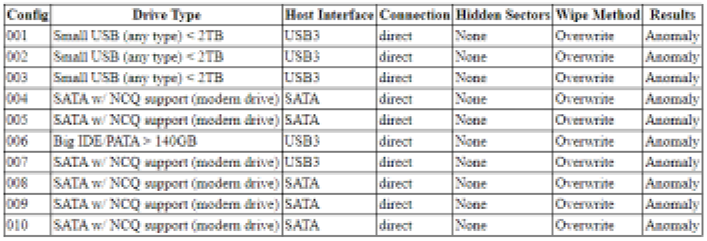
Completed - 0 Errors

Figure 35. Successful Wipe

such as SAFE Block ForensicSoft (2008) and ACES WriteBlocker for Law Enforcement (2008) as well as other hardware-based USB write blockers from CRU CRU (2020) or Tableau Tableau (2020).

ACKNOWLEDGMENT

This paper and the research behind it would not have been possible without the exceptional support of the Miami-Dade Police Department Digital Forensic Unit for providing the loaner forensics hardware, the knowledge



Config	Drive Type	Host Interface	Connection	Hidden Sectors	Wipe Method	Results
001	Small USB (any type) < 2TB	USB3	direct	None	Overwrite	Anomaly
002	Small USB (any type) < 2TB	USB3	direct	None	Overwrite	Anomaly
003	Small USB (any type) < 2TB	USB3	direct	None	Overwrite	Anomaly
004	SATA w/ NCQ support (modern drive)	SATA	direct	None	Overwrite	Anomaly
005	SATA w/ NCQ support (modern drive)	SATA	direct	None	Overwrite	Anomaly
006	Big IDE/PATA > 140GB	USB3	direct	None	Overwrite	Anomaly
007	SATA w/ NCQ support (modern drive)	USB3	direct	None	Overwrite	Anomaly
008	SATA w/ NCQ support (modern drive)	SATA	direct	None	Overwrite	Anomaly
009	SATA w/ NCQ support (modern drive)	SATA	direct	None	Overwrite	Anomaly
010	SATA w/ NCQ support (modern drive)	SATA	direct	None	Overwrite	Anomaly

Figure 36. Forensic Wipe Results

on how to best utilize the hardware and being reachable for all questions.

Additionally, Benjamin Livelsberger of the NIST's Computer Forensics Tool Testing Program (CFTT) was of key importance to ensure consistent testing of all of the consumer grade tools, providing updates on CFTT's Version 5 with Forensic Wipe testing and troubleshooting issues with our setup.

Last, but not least, Dr James Kiper for continuously encouraging and supporting me to take on research into fringe and underserved topics within the field of computer forensics. His mentorship of his students to continously apply scientific methodologies derived from the forensics field to bring scientific ideals to the computer forensics field is an example to be followed.

REFERENCES

Bureau of Labor Statistics, U. D. o. L. (2019). *Usual weekly earnings of wage and salary workers fourth quarter 2019.* Retrieved from https://www.bls.gov/news.release/pdf/wkyeng.pdf

CRU. (2020). *Usb 3.1 write blocker.* Retrieved from https://www.cru-inc.com/products/wiebetech/usb-3-1-writeblocker/

FinancialRed. (2018). *Salario mínimo en latinoamérica.* Retrieved from https://salariominimo.com.mx/comparativa-salario-minimo-latinoamerica/

ForensicSoft, I. (2008). *Safeblock to go.* Retrieved from https://www.forensicsoft.com/sb2go.php

for Law Enforcement, A. C. E. S. (2008). *Aces writeblocker.* Retrieved from http://www.acesle.org/

Gaigin.net. (2011). *Usbwriteprotector.* Retrieved from https://gaijin.at/en/software/usbwriteprotector

IronGeek. (2013). *Thumbscrew.* Retrieved from http://www.irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker/

Lawrence, T., Karabiyik, U., & Shashidhar, N. (2018, 03). Equipping a digital forensic lab on a budget. In (p. 1-7). doi: 10.1109/ISDFS.2018.8355345

of Homeland Security (DHS) Science, D., & (ST), T. D. (2020a). *Test results for forensic media preparation tool: Cinolink dual hdd dock.* Retrieved from https://www.dhs.gov/sites/default/files/publications/test_results_for_cinolink_dual_hdd_dock_with_edits_gd1_2581_508c.pdf

of Homeland Security (DHS) Science, D., & (ST), T. D. (2020b). *Test results for forensic media preparation tool: Roadkil's disk image version 1.6.* Retrieved from https://www.dhs.gov/sites/default/files/publications/

0211-01_test_results_for_roadkils_disk_image_version_508c_0.pdf

of Homeland Security (DHS) Science, D., & (ST), T. D. (2020c). *Test results for forensic media preparation tool: Roadkil's disk wipe version 1.2.* Retrieved from https://www.dhs.gov/sites/default/files/publications/test_results_for_roadkils_diskwipe_ver_1.2_final1.pdf

Pendrivelinux.com. (2020). *Yumi – multiboot usb creator.* Retrieved from https://www.pendrivelinux.com/yumi-multiboot-usb-creator/

Press, B. (2019). *Human development report 2019.* Retrieved from http://hdr.undp.org/sites/default/files/hdr2019.pdf

Sordum.org. (2015). *Ratool (removable access tool) 1.3.* Retrieved from https://www.sordum.org/8104/ratool-v1-3-removable-access-tool/

Tableau. (2020). *Tableau forensic usb 3.0 bridge.* Retrieved from https://www.guidancesoftware.com/tableau/hardware/t8u/

Thelma.allen@nist.gov. (2020). *Federated testing project.* Retrieved from https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/federated-testing

Tilbury, C. (2010). *Tableau imager: First look.* Retrieved from https://www.sans.org/blog/tableau-imager-first-look/

APPENDIX A - SUSPECT'S COMPUTER IMAGES

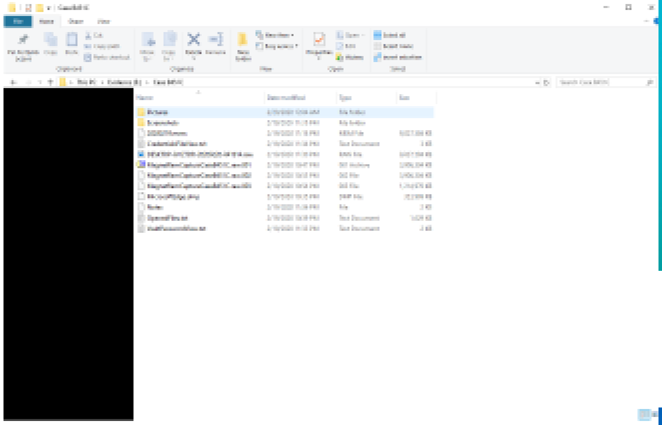

[redacted]

Figure 37. Case B451C Contents

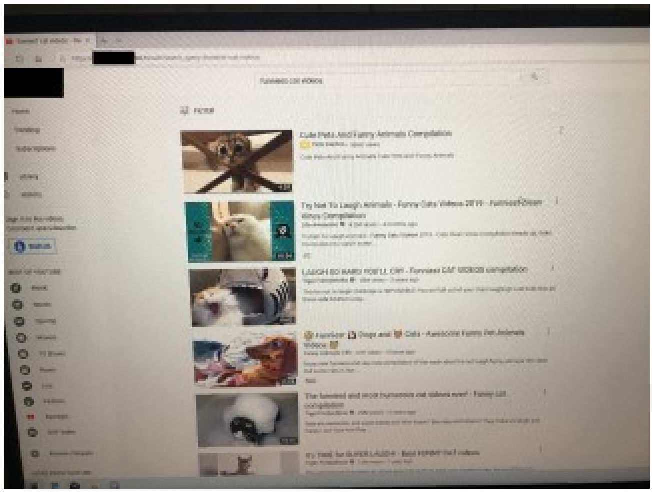

[redacted]
[redacted]

Figure 38. Contents of Suspect's Screen

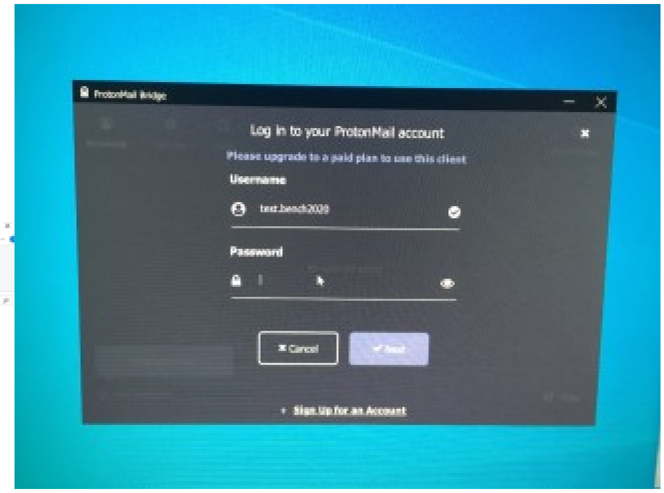

ProtonMail Bridge
Log in to your ProtonMail account
Please upgrade to a paid plan to use this client
Username
test.bench2020
Password
Cancel
Next
Sign Up for an Account

Figure 39. Open Application on Suspect's Computer - Proton Mail Bridge

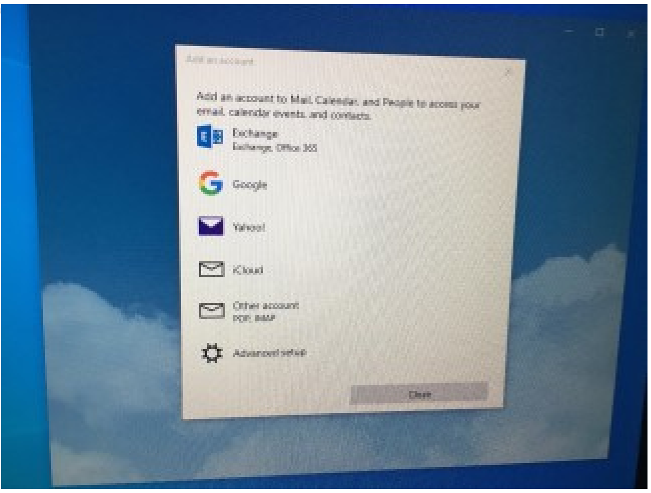


Figure 40. Open Application on Suspect's Computer - Mail App

Figure 41. Flash Drive with tools connected to Suspect's Computer

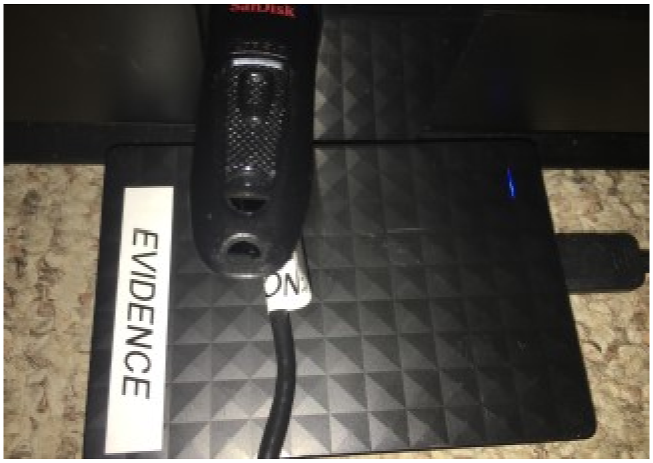


Figure 42. Evidence Drive connected to Suspect's Computer

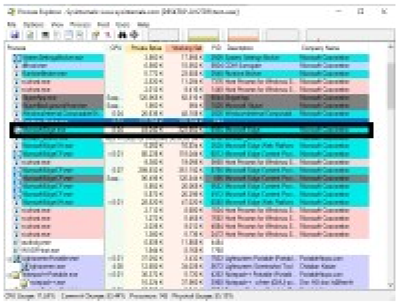


Figure 43. Process Explorer Dump

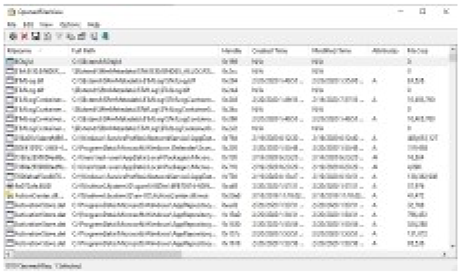


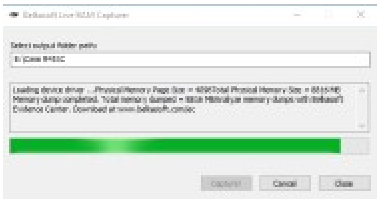
Figure 44. OpenedFileView

RAM Capture v1.2.0

Segment size:

Save RAM capture to...

Figure 45. MAGNET RAM Capture

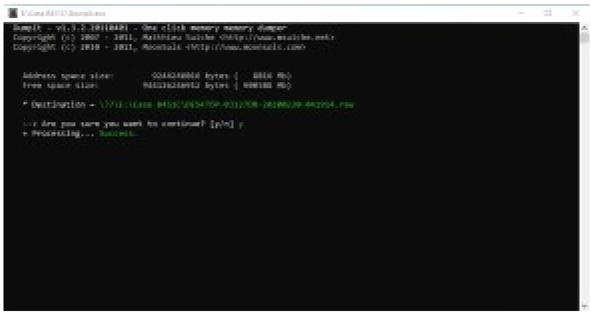


Select output folder path:

E:\Case B453C

Loading device driver ...PhysicalMemory Page Size = 4096Total Physical Memory Size = 8816 MB
Memory dump completed. Total memory dumped = 8816 MBAnalyze memory dumps with Belkasoft Evidence Center. Download at www.belkasoft.com/ec

Figure 46. Belkasoft RAM Capturer



```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

  Address space size:       [illegible] bytes (   8816 Mb)
  Free space size:          [illegible] bytes ( [illegible] Mb)

  * Destination = \??\E:\Case B453C\[illegible].raw

  --> Are you sure you want to continue? [y/n] y
  + Processing... Success.
```

Figure 47. DumpIt

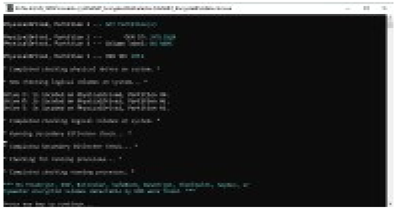
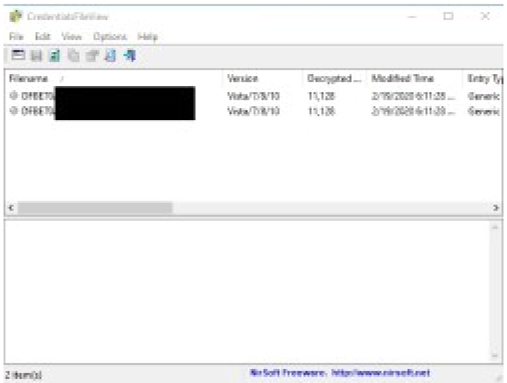


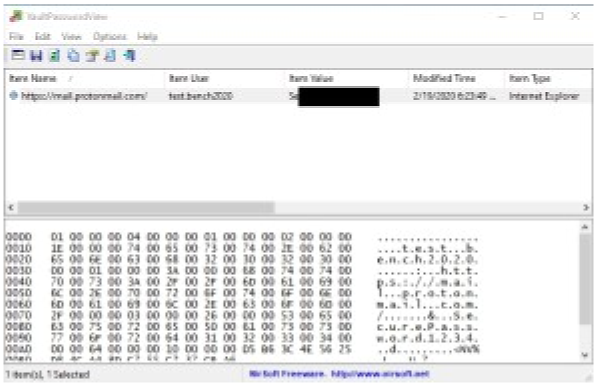
Figure 48. MAGNET's Encrypted Disk Detector



Filename	Version	Decrypted ...	Modified Time	Entry Ty
DFBE7[redacted]	Vista/7/8/10	11,128	2/19/2020 6:11:28 ...	Generic
DFBE7	Vista/7/8/10	11,128	2/19/2020 6:11:28 ...	Generic

2 item(s) NirSoft Freeware. http://www.nirsoft.net

Figure 49. CredentialsFileView

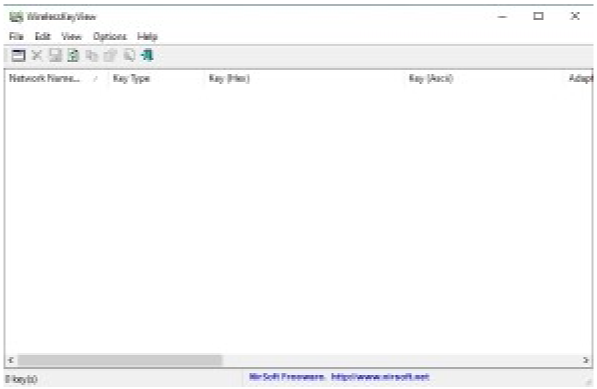


Item Name /	Item User	Item Value	Modified Time	Item Type
https://mail.protonmail.com/	test.bench2020	Se[redacted]	2/19/2020 6:23:49 ...	Internet Explorer

```
0000   01 00 00 00 04 00 00 00 01 00 00 00 02 00 00 00   ................
0010   1E 00 00 00 74 00 65 00 73 00 74 00 2E 00 62 00   ....t.e.s.t...b.
0020   65 00 6E 00 63 00 68 00 32 00 30 00 32 00 30 00   e.n.c.h.2.0.2.0.
0030   00 00 01 00 00 00 3A 00 00 00 68 00 74 00 74 00   ......:...h.t.t.
0040   70 00 73 00 3A 00 2F 00 2F 00 6D 00 61 00 69 00   p.s.:././.m.a.i.
0050   6C 00 2E 00 70 00 72 00 6F 00 74 00 6F 00 6E 00   l...p.r.o.t.o.n.
0060   6D 00 61 00 69 00 6C 00 2E 00 63 00 6F 00 6D 00   m.a.i.l...c.o.m.
0070   2F 00 00 00 03 00 00 00 26 00 00 00 53 00 65 00   /.......&...S.e.
0080   63 00 75 00 72 00 65 00 50 00 61 00 73 00 73 00   c.u.r.e.P.a.s.s.
0090   77 00 6F 00 72 00 64 00 31 00 32 00 33 00 34 00   w.o.r.d.1.2.3.4.
00A0   00 00 64 00 00 00 10 00 00 00 D5 B6 3C 4E 56 25   ..d.........<NV%
```

1 item(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

Figure 50. VaultPasswordView



Network Name... /	Key Type	Key (Hex)	Key (Ascii)	Adapt

0 key(s) NirSoft Freeware. http://www.nirsoft.net

Figure 51. WirelessKeyView

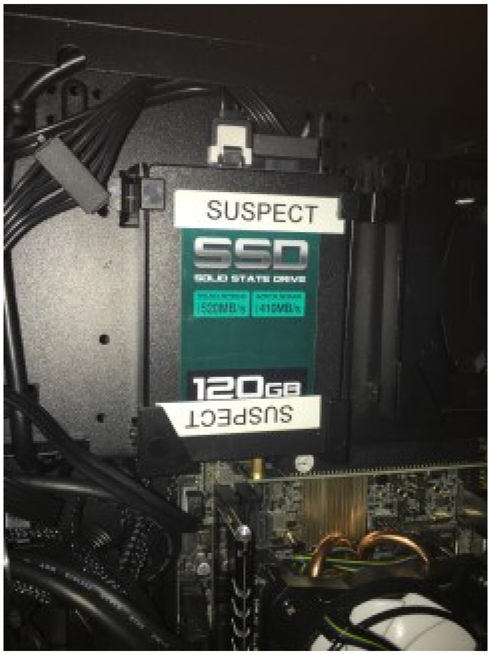
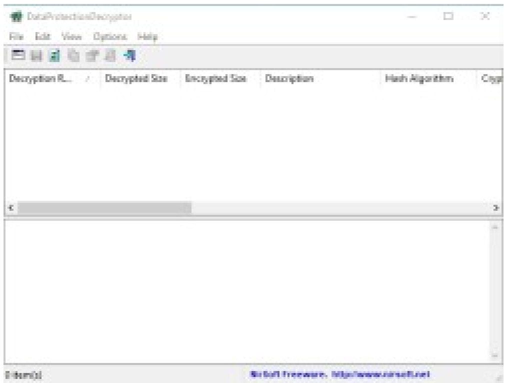


Figure 53. Suspect's Drive inside Suspect's Computer



Decryption R... /	Decrypted Size	Encrypted Size	Description	Hash Algorithm	Cryp

0 item(s) NirSoft Freeware. http://www.nirsoft.net

Figure 52. DataProtectionDecryptor