ON THE SELECTION OF WRITE BLOCKERS FOR DISK ACQUISITION: A COMPARATIVE PRACTICAL STUDY

Mousa Al Falayleh
College of Computer Info. Tech.
American University in the Emirates
Dubai, United Arab Emirates
mousa.falayleh@aue.ae

Jamal N. Al-Karaki
Information Security Eng. Tech. Dept.
AbuDhabi Polytechnic
Abu Dhabi 111499, United Arab Emirates
jamal.alkaraki@adpoly.ac.ae

ABSTRACT

Digital Forensics (DF) is an evolutionary field with evolving techniques. One major step in DF Framework is the acquisition phase, where a copy or an image of a suspect disk is preserved with no alteration or modification. This is an important technique for the evidence to be accepted by a court of law. To accomplish that, investigators normally use hardware based or software based Write Blocker (WB). In this paper, we perform in-depth performance evaluation for a number of Hardware and Software write blockers from various vendors. The intent is to determine the best WB for a certain scenario in terms of shortest imaging time. The experimental results reported in this paper form an invaluable reference for field practioners.

KEYWORDS

Digital Forensics, Forensically Sound Imaging, Write Blockers, Data Acquisition.

1 INTRODUCTION

Digital forensics is a collection of specialized techniques, processes, and procedures used to preserve, extract, analyze, and present electronic evidence that is found in digital devices, often in relation to computer or cyber crime [1].

The National Institute of Standards and Technology, NIST, divide digital forensics investigation into four phases [2,3], which are briefly summarized below, see Figure 1:

1. **Collection**: Identify, label, record and acquire data from possible sources, while preserving the integrity of the data.
2. **Examination**: Use manual and automated methods to assess and extract data of particular interest, while preserving the integrity of the data.
3. **Analysis**: Use legally justifiable methods and techniques to derive useful information.
4. **Reporting**: Describe actions used, explain how tools and procedures were selected, determine what other actions need to be performed, including forensic examination of additional data sources, securing identified vulnerabilities and improving existing security controls. Recommend improvements to policies, guidelines, procedures, tools and other aspects of the forensic process.

The second phase in Digital Forensics workflow is the acquisition phase. During the acquisition process an investigator needs to copy or image a suspect drive in a forensically manner.

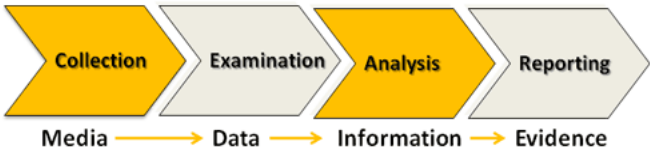

Figure 1. Digital Forensics Lifecycle.

Imaging a hard drive in a forensically manner guarantee that no alteration or modification should be done to the suspect drive. This is very important in order for the evidence to be used in a court of law. This is accomplished by using the so called Write Blocker.

Write blockers are devices that allow a forensically sound image of virtually any hard drive or storage device you may encounter without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but by blocking write commands, hence their name.

There are both hardware and software write blockers. Some software write blockers are designed for a specific operating system. One designed for Windows will not work on Linux. It is advised to use hardware write blockers as they are recognized as a court-validated standard. Hardware write blockers are more reliable than software ones. Moreover, hardware write blockers are software independent.

In this paper, we perform extensive set of experiments to measure various write blockers' performance based on the time that a write blocker consumes in imaging a storage unit. We have used Hardware and Software write blockers and from various venders. Our study outcomes represent very helpful guide for people working in the field of digital forensics. It helps investigators in deciding which write blocker better suits their needs based on the type of storage unit that they are investigating.

This paper is organized as follows. Section 2 introduces write blockers. Section 3 explains the experimental setup of this study while Section 4 focuses on presenting and analyzing the results. Section 5 suggests further future work. Finally, Section 6 gives some concluding remarks.

2 WRITE BLOCKER STATE OF THE ART REVIEWS

Write blockers are devices that allow a forensically sound image of virtually any hard drive or storage device you may encounter without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but by blocking write commands, hence their name.

There are both hardware and software write blockers [4,5]. Some software write blockers are designed for a specific operating system. One designed for Windows will not work on Linux. It is advised to use hardware write blockers as they are recognized as a court-validated standard. Hardware write blockers are more reliable than software ones. Moreover, hardware write blockers are software independent.

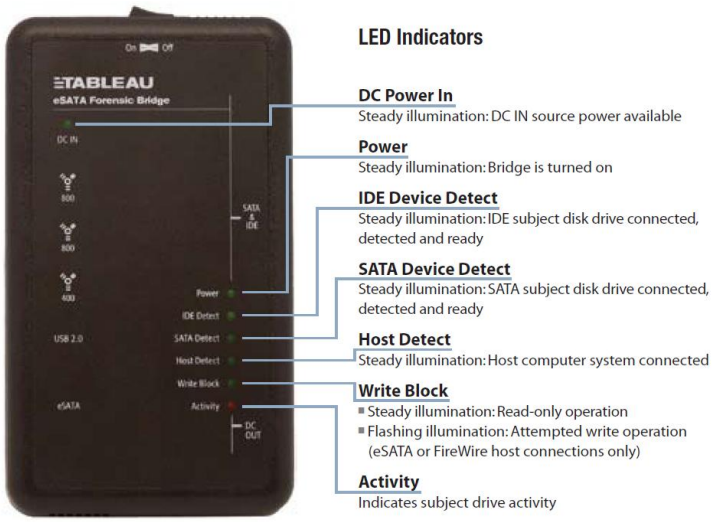

Figure 2. Tableau T35es Hardware Write Blocker
"Photo copyright (Retrieved from Tableau's website)."

We run our experiments on write blockers from three different venders. One of the write blockers was Software one and the rest were Hardware ones. In what follow, we explore these write blockers:

2.1 Tableau T35es

The Read Only UltraBlock eSATA IDE-SATA (Tableau T35es) [6] is used to acquire data from an IDE or SATA hard drive in a forensically sound write-protected environment. The eSATA Forensic Bridge supports four different host connection options for SATA and IDE device acquisitions: One eSATA Port, Two FireWire800 Ports, One FireWire400 Port, and One USB 2.0/1.1 Port, See Figure 2.

2.2 WiebeTech UltraDock V4

The Read Only Forensic UltraDock (WiebeTech UltraDock V4) [7] is WiebeTech's premium Forensic Dock. It is used to acquire data from an IDE or SATA hard drive in a forensically sound

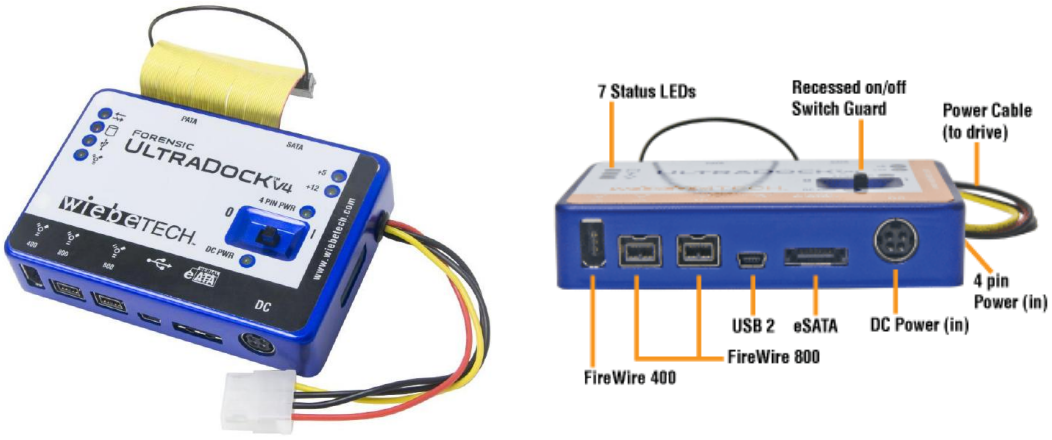

Figure 3. WiebeTech UltraDock V4 Hardware Write Blocker
"Photo copyright (Retrieved from WiebeTech's website)."

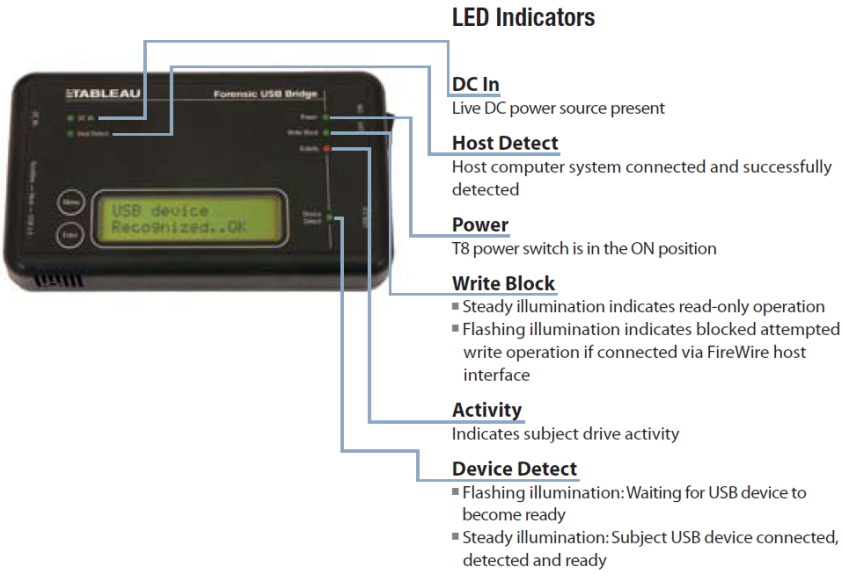

Figure 4. Tableau T8 Forensic USB Write Blocker
"Photo copyright (Retrieved from Tableau's website)."

write-protected environment. The Forensic UltraDock supports four different host connection options for SATA and IDE device acquisitions: One eSATA Port, Two FireWire800 Ports, One FireWire400 Port, and One USB 2.0 Port, See Figure 3.

2.3 Tableau T8 Forensic USB

The UltraBlock Forensic USB Bridge (Tableau T8 Forensic USB) [6] brings secure, hardware-based write blocking to the world of USB mass storage devices. The UltraBlock USB Write Blocker supports USB2.0 High-Speed, USB 1.1 Full-Speed and Low-Speed devices. The UltraBlock USB Write Blocker works with USB thumb drives, external USB disk drives, even USB-based cameras with card-reader capability. The USB Write Blocker supports both USB 2.0 and FireWire400 connections to a host computer, See Figure 4.

2.4 WiebeTech USB

The Read Only WiebeTech USB [7] is a USB Write Blocker. It is a forensic solution to access USB flash drives or devices that cannot be removed from a USB enclosure. USB Write Blocker works with devices that register as "USB

Figure 5. WiebeTech USB Write Blocker
"Photo copyright (Retrieved from WiebeTech's website)."

Mass Storage" devices, very common for thumb drives and storage enclosures. USB Write Blocker is also compatible with other devices that register in the same way, such as some Cellular Phones and Digital Cameras. The USB Write Blocker supports only USB connection to a host computer and does not support FireWire400 connection to a host computer, See Figure 5.

2.5 SAFE Block Win 7 64 bit

SAFE Block [8] is a software write-blocking product from ForensicSoft Company. By installing SAFE Block on your field and lab computers, you have a proven forensically-sound write-blocking solution with complete control over all connected disks, See Figure 6.

3 EXPERIMENTAL SETUP

In this section, we perform a set of extensive experiments to compare among the performance of different write blockers. The setup of the experiments is established by selecting the test imaging host computer that is defined in subsection 3.1. The second step was to select a set of hard disk drives to do the experiments on and that is defined in subsection 3.2. We have used different imaging tools to manage the acquisition process and that is introduced in subsection 3.3.

We conducted various experiments with all possible host connections that are available in various Hardware write blockers. Each imaging process has its own options and that was adjusted through the interface of imaging tools. In our experiments, we made the following options to be equal to the following values, see Figure 7:

1. Image File format: Encase E01
2. Compression: None
3. Error Recovery: Minimum
4. Hash Option: MD5 + SHA1
5. File Size: 2 GB

The acquisition process was allowed to be executed to the completion and the time consumed in acquisition was noted. The consumed time in imaging represents the performance metric in our experiments and we call it Disk Copy Time (DCT).

Figure 6. Software Write Blocker: SAFE Block Win 7 64 bit

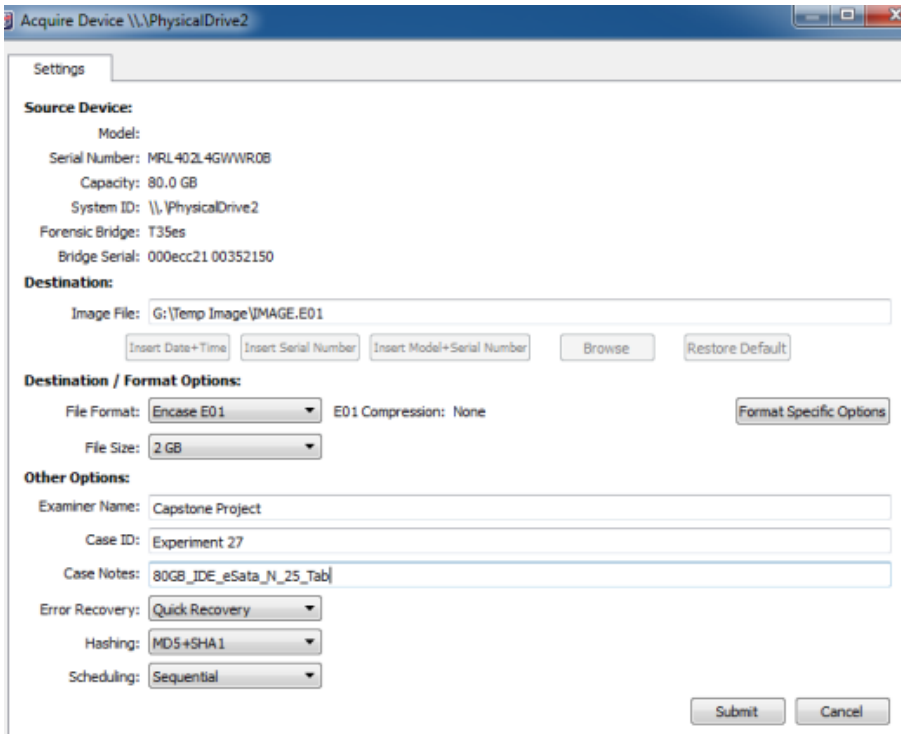

Figure 7. Imaging Options

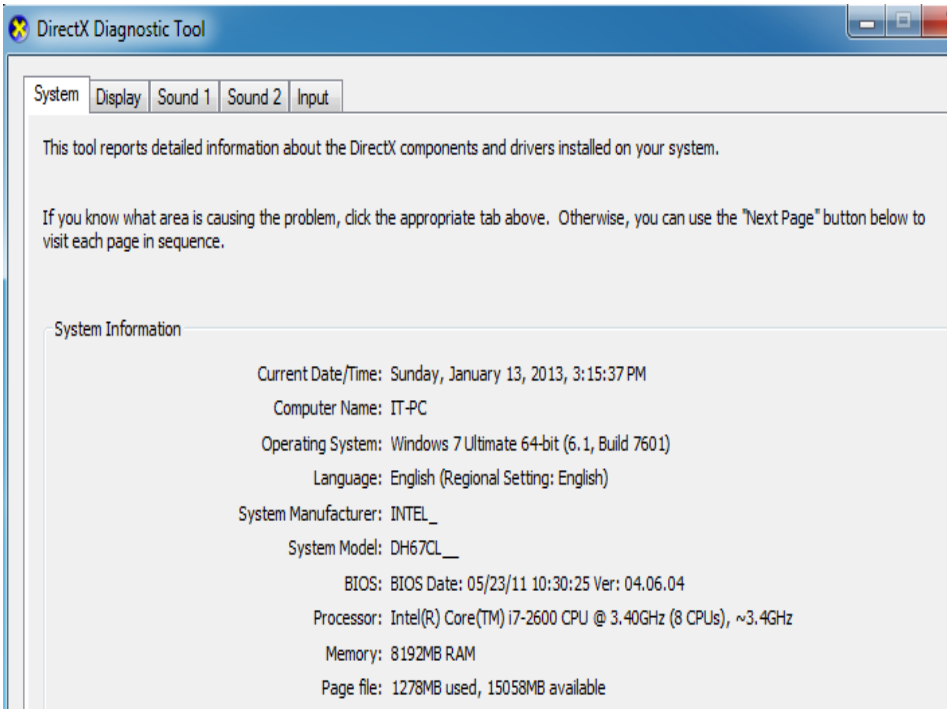

Figure 8. Host Specifications.

3.1 Image Host

The test imaging host was setup in the university digital forensics lab workstation. It has been used as a host for the copied images and has the specifications in Table 1 and Figure 8.

3.2 Test Disks

Table 2 explores a list of hard disk drives that has been used in our experiments. The first column in Table 2 is a serial number whereas the second column indicates the size of disk under experiment. The fourth column shows which connection the source disk has. The last column indicates if it is a disk for laptop or desktop computer. The last three storage units in the table, rows 6-8, are USB flash disk.

3.3 Imaging Tools

We have used different imaging tools in our experiments. An imaging tool is basically a software application that is designed to manage the imaging process from the source disk to the host computer with the usage of write blockers. Imaging tools help you identify various options to be used while you copying the data between the source and the host.

Tableau Imager [6] has been used as an imaging tool for Tableau write blocker both Tableau T35es and Tableau T8 Forensic USB, see Figure 9.

AcessData FTK Imager [9] has been used as an imaging tool for WiebeTech write blockers both WiebeTech UltraDock V4 and USB, see Figure 10.

Table 1. Host Specifications

Intel CORE i7 3.4GHZ CPU
8GB RAM DDR3
One 500 GB 72,000 RPM SATA hard disk drive (boot/OS drive)
One 500 GB 72,000 RPM SATA hard disk drive (Oracle storage)
Ports for eSata, FireWire 400, and USB.
Geforce GT210 1gb vga Card DDR3
10/100/1000 Integrated LAN
DVD RW
22.5” LCD Monitor

Table 2. Test Disks

Serial	Disk Size	Connection	Desktop/Laptop
1	40G	Sata	L
2	80G	IDE	L
3	250G	Sata	L
4	250G	IDE	D
5	320G	Sata	L
6	1G	USB	-
7	8G	USB	-
8	16G	USB	-

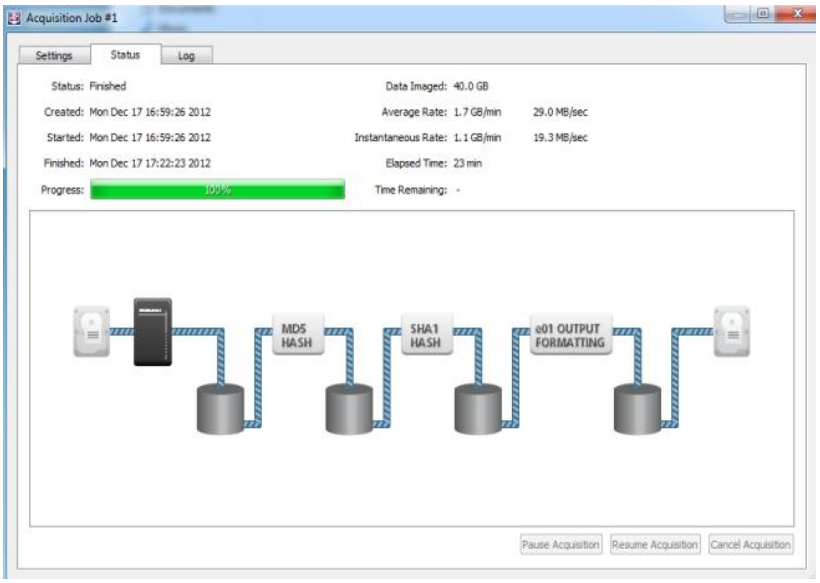

Figure 9. The Imaging Tool: Tableau Imager

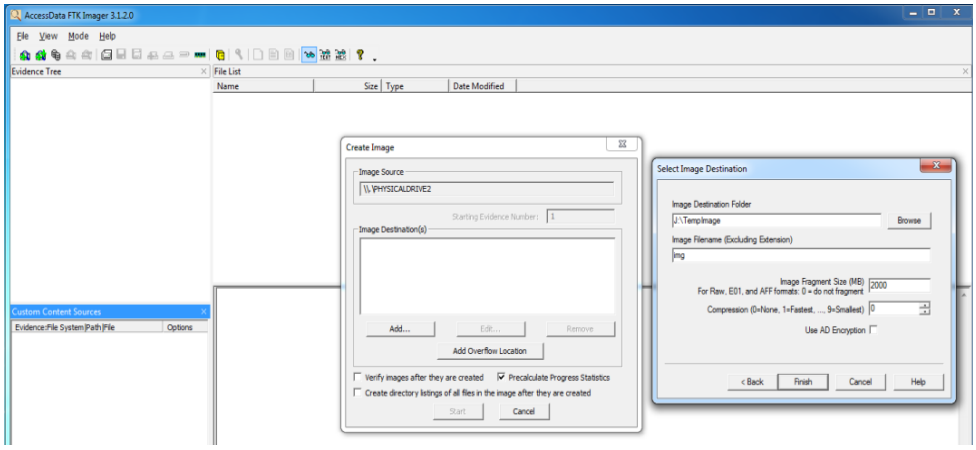

Figure 10. The Imaging Tool: AcessData FTK Imager

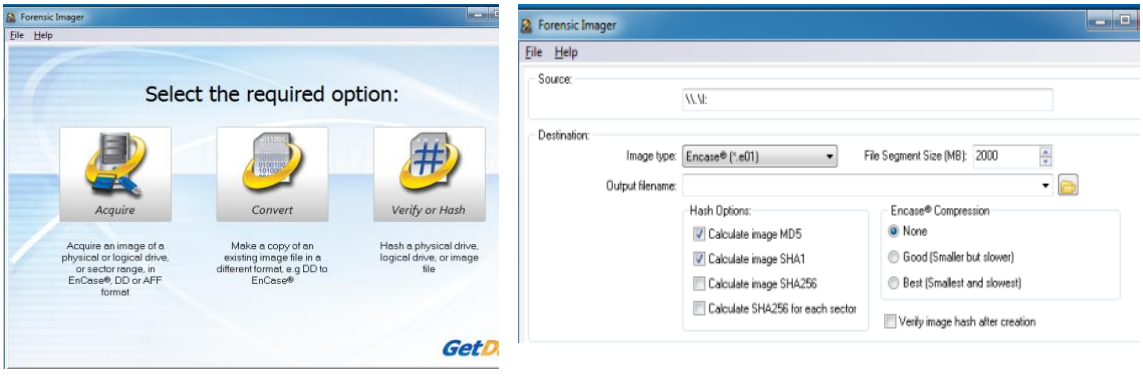

Figure 11. The Imaging Tool: Forensic Imager

Forensic Imager from GetData [10] has been used as an imaging tool for SAFE Block, the software write blocker, see Figure 11.

4 TEST RESULTS

Tables 3 to 5 show test results for most of the testing scenarios. The second column in the table indicates write blocker name. The third column in the table shows the size of the imaged disk in Gigabyte. Columns four and five indicate the type of connecting cable between the imaged disk (Source) and the used write blocker from one side and between the write blocker and the host computer from the other side. Column six indicates weather the understudy disk is for desktop computers (D) or for laptops (L). The seventh column is the most important column as it shows the time consumed in acquisition process for the corresponding disk and connection cables, Disk Copy Time (DCT). The last column is present for any comments.

Table 3 presents test results to compare the performance of Tableau T35es vs. WiebeTech UltraDock V4. Row 2 and row 3 in the table show that for a disk size of 250 GB and with an eSata cable connected to the host computer, Tableau T35es performs much faster than WiebeTech UltraDock V4 with imaging time "0:51:27" vs. "1:10:53". Row 6 and row 7 in the table show that the difference in imaging time is getting smaller as we image smaller disk with size 40 GB ("0:22:57" vs. "0:24:01"). In rows 2, 4, and 5 and by using the same write blocker (Tableau T35es) and the same imaged disk (250 GB), the best and faster acquisition process was by using

Table 3. Test Results: Tableau T35es vs. WiebeTech UltraDock V4

Serial	Write Blocker	Size	Source	Host	D/L	DCT Time	Comments
1.	**Tableau T35es**	250G	IDE	eSata	D	1:10:56	
2.	**Tableau T35es**	250G	Sata	eSata	L	0:51:27	
3.	**WiebeTech UltraDock V4**	250G	Sata	eSata	L	1:10:53	
4.	**Tableau T35es**	250G	Sata	FireWire400	L	1:36:16	
5.	**Tableau T35es**	250G	Sata	USB	L	1:59:59	
6.	**Tableau T35es**	40G	Sata	eSata	L	0:22:57	
7.	**WiebeTech UltraDock V4**	40G	Sata	eSata	L	0:24:01	
8.	**Tableau T35es**	40G	Sata	FireWire400	L	0:22:56	
9.	**Tableau T35es**	40G	Sata	USB	L	0:23:04	
10.	**Tableau T35es**	40G	Sata	USB	L	0:23:04	RAW
11.	**Tableau T35es**	80G	IDE	eSata	L	0:56:22	25''
12.	**WiebeTech UltraDock V4**	80G	IDE	eSata	L	0:37:16	
13.	**Tableau T35es**	80G	IDE	FireWire400	L	0:48:52	25''
14.	**WiebeTech UltraDock V4**	80G	IDE	FireWire400	L	0:52:36	25''
15.	**Tableau T35es**	80G	IDE	USB	L	0:42:48	
16.	**Tableau T35es**	80G	IDE	USB	L	0:49:02	25''
17.	**WiebeTech UltraDock V4**	80G	IDE	USB	L	0:51:23	25''

eSata cable as a connecting cable to the host. eSata achieved "0:51:27" as imaging time while FireWire400 achieved "1:36:16" and USB was the slowest by consuming "1:59:59".

Another observation worth noticing is the difference in imaging time, between Tableau T35es and WiebeTech UltraDock V4. DCT time is getting smaller as the size of the imaged disk is getting smaller. This is eviedanced by results in rows 6 and 7. Rows 15 and 16 show that when there is an adapter connected to the source disk such as 25 inch adapter in row 16, it slows the imaging process "0:49:02" rather than "0:42:48' in row 15 with two disks with the same size and same write blocker and connecting cables.

For the same write blocker and same disk size but with different source disk connections. Source disk with ID connection performs slower than source disk with Sata, see rows 1 and 2.

Table 4 indicates that there is a huge difference in imaging time when we use a hardware write blocker (Tableau T35es) and a software write blocker (SAFE Block). For the same source disk Tableau T35es takes "0:23:04" rather than "1:18:38" for SAFE Block.

Table 5 explores test results for imaging USB flash disks with various hardware and software write blockers. Tableau T8 Forensic USB write blocker proves to be the fastest to be used for imaging USB flash disk. It is even much faster when FireWire400 is used as a connection cable to the host. Tableau T8 Forensic USB is the only USB write blocker that provides two alternative connection cable to the host, FireWire400 and USB cables. The remarkable difference in imaging time can be easily inferred when imaging large size USB disk as with 16 GB in row 1.

Table 4. Test Results: Tableau T35es vs. SAFE Block

Serial	Write Blocker	Size	Source	Host	D/L	DCT Time	Comments
1.	**Tableau T35es**	40G	Sata	USB	L	0:23:04	
2.	**SAFE Block Win 7 64 bit**	40G	Sata	USB	L	1:18:38	

Table 5. Test Results: Tableau T8 Forensic USB vs. WiebeTech USB vs. SAFE Block

Serial	Write Blocker	Size	Source	Host	DCT Time	Comments
1.	**Tableau T8 Forensic USB**	16G	USB	FireWire400	0:09:26	
2.	**Tableau T8 Forensic USB**	16G	USB	USB	0:11:34	
3.	**WiebeTech USB**	16G	USB	USB	0:38:33	
4.	**Tableau T8 Forensic USB**	1G	USB	FireWire400	0:01:13	
5.	**Tableau T8 Forensic USB**	1G	USB	USB	0:01:26	
6.	**Tableau T8 Forensic USB**	8G	USB	FireWire400	0:06:59	
7.	**Tableau T8 Forensic USB**	8G	USB	USB	0:08:31	
8.	**WiebeTech USB**	8G	USB	USB	0:24:47	
9.	**SAFE Block Win 7 64 bit**	8G	USB	USB	0:24:47	

5 FUTURE WORKS

In our work, we did examine the impact of different factors on the acquisition process. We used different kinds of cable connectors including eSata, IDE, USB, and FireWire. Moreover, we have used different imaging applications such as Tableau imager, AccessData FTK Imager, and Forensic Imager. We left the door open for future enhancements and more experiments to be examined. We recommend redoing our experiments under different operating system environments such as different versions of Windows and additionally with Linux. Another factor to test will be the host specifications. I believe that redoing our experiments for different host workstation with different specifications such as the memory size, the processor speed, and different disk frequency of rotation (RPM) will reveal some interesting results.

6 CONCLUSIONS

Imaging a hard drive in a forensically manner guarantee that no alteration or modification should be done to the suspect drive. This is very important in order for an evidence to be used in a court of law. Our work shows that software write blockers are unreliable and an investigator cannot count on them as they are very slow and inefficient. On the other hand, Hardware write blockers are efficient. Write blocker products from Tableau perform better than those ones from WiebeTech. The difference was small when we imaged small size hard drives, but the difference starts to get bigger with imaging large size hard drives. When it comes to which imaging cables shall be used when connecting a write blocker to the host machine, we recommend using eSata cables as the first option followed by FireWire cables as the second option and finally USB cables. Further future work is suggested in this paper.

7 REFERENCES

1. Aminnezhad, A., Dehghantanha, A., & Abdullah, M. T.: A Survey on Privacy Issues in Digital Forensics. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1, pp. 311-323 (2012).
2. Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang: Guide to Integrating Forensic Techniques into Incident Responses: NIST Special Publication 800-86 (2006).
3. Shrivastava, G., Sharma, K., & Dwivedi, A.: Forensic Computing Models: Technical Overview. CCSEA, SEA, CLOUD, DKMP, CS & IT, 5, pp. 207-216 (2012).
4. Lyle, J. R.: A strategy for testing hardware write block devices. Digital Investigation, 3, pp. 3-9 (2006).
5. Lyle, J. R. and Wozar, M.: Issues with imaging drives containing faulty sectors. Digital Investigation, 4, pp. 13-15 (2007).
6. Tableau: http://www.tableau.com/index.php?pageid=home
7. WiebeTech: http://www.wiebetech.com/
8. ForensicSoft: http://forensicsoft.com/
9. AcessData: http://www.accessdata.com/
10. GetData: http://www.getdata.com/