Bachelor's thesis

IT Forensics and information security, 180hp

Need for speed

A study of the speed of forensic disk imaging tools

Halmstad 2022-06-04
Authors: Dawid Stewart and Alex Arvidsson

HÖGSKOLAN
I HALMSTAD

Need for speed

A study of the speed of forensic disk imaging tools

Authors: Dawid Stewart and Alex Arvidsson
Examiner: Eric Järpe
Supervisor: Mohamed Eldefrawy
The academy of information technology
University: Halmstad University
City: Halmstad
Date: 2022-06-04

Abstract

As our society becomes increasingly digitalized, there is an ever-increasing need for forensic tools to become faster and faster. This paper was made to help the Police and other digital forensic investigators choose the fastest disk imaging tool while still maintaining the integrity of the imaged disk. To answer this, an experiment including 162 disk imaging tests was done, with an active imaging and verification time of over 160 hours. The results were analyzed with the help of a scoring system and statistical significance tests. The paper also aimed to show if there is any difference when making images of disks that are filled to 100% compared to disks filled to 50%, and which of the disk imaging tools that handles it best.

The results of the experiment showed that Guymager was the fastest disk imaging tool among the tested alternatives. It also illustrated that the speed was affected by the disks being filled to 50% as opposed to 100%. Guymager showed the best performance improvement using the EWF_E01 format, and OSForensics showed the biggest improvement when imaging using the DD format.

Keywords: Disk imaging, digital forensics, disk imaging speed, data extraction

Foreword

We would like to thank our supervisor, Mohamed Eldefrawy, for all the suggestions, feedback and knowledge he has been providing.

We would also like to thank our friends and family for being supportive and patient.

Glossary

Malware: Malware consists of malicious code that an attacker places on a system to execute tasks without the victim's permission.

Disk imaging: A disk image is a file copy of a storage device containing the content and the storage structure. It can be different types of disks or other forms of storage devices.

Hash value: A hash value is a specified length value that can be created using a hash algorithm. The value length depends on which type of hash algorithm is used, and the resulting value is unique to the data for which it was calculated. Hashing is often used to verify the integrity of data.

AV-TEST: An independent research institute for IT-security.

McAfee: A global American computer security software company.

Forensically sound: If digital evidence is collected, analyzed, handled, and stored in a legal manner and there is reasonable evidence to prove it, it is said to be forensically sound.

Partition: A partition, or volume, is a logical section of a hard drive. Using partitions, which can also be thought of as parts of a hard drive, enables the use of several filesystems on the same hard drive.

Partition slack: Partition slack, also known as volume slack, is the space on a disk which is not occupied by any filesystem. The slack is the unallocated space of the disk.

Byte: A unit of information in computer storage and processing.

TB, KB, PB, MiB, TiB: Terabyte (TB), Kilobyte (KB), Petabyte (PB), Mebibyte (MiB) and Tebibyte (TiB) are multiple-byte units. One TB is 10^{12} bytes, one KB is 10^{3} bytes, one PB is 10^{15} bytes, one MiB is 2^{20} bytes and one TiB is 2^{40} bytes.

Table of contents

1 Introduction

As the world becomes increasingly digital, the need for trained digital forensic investigators and well-developed digital forensic tools also grows. With smartphones, smart homes, and smart cars, the number of devices from which information can be extracted increases every year.

The types of malware identified have increased dramatically in recent years. According to AV-TEST, 182.90 million types of malware existed in 2013; in 2021, this figure was significantly higher: 1312.63 million [1]. The marked increase in cybercrime has resulted in increased costs. According to a report by McAfee, cybercrime cost $600 billion internationally in 2017 [2]. But even traditional crimes now have digital evidence. Examples of this can be chat logs, prohibited material such as child pornography, or location information from mobile devices.

Data extraction for criminal investigations takes time, and more digital forensic investigators are needed to streamline work. But it also requires that the available digital forensic tools are continuously tested and optimized for the tasks.

The first step for IT forensic investigations is collecting and extracting information and data. To obtain evidence from a unit, it is necessary to make an image of it. This is so that evidence can be obtained without affecting the unit itself and thus not affecting the integrity of the seized unit. If the integrity is affected, the evidence may become invalid and may not be used at trial [3].

In an email interview with Peter Bergström from the National Forensic Center (NFC), a subdivision of the Swedish police, he explained that it is essential that the disk imaging process is trustworthy and that it also needs to be fast to prevent bottlenecking. If two tools are equal in accuracy, then the speed of the tools is essential to be as effective as possible [4].

Previous research in the field of disk imaging has extended over the validation of imaging integrity for individual tools [5][6], speed based on the type of interface [7][8], and comparisons of speed between selected tools. In the previous research, the speed comparisons between disk imaging software have been woven into tests where the previously mentioned aspects have also been compared.

Few studies have prioritized the speed of software as a primary topic. However, Jack Riley, David Dampier, and Rayford Vaughn measured the speed of two imaging tools with different types of interfaces where speed was prioritized. However, they turned off the hash function in their measurements to focus on just the speed [8]. In a study by Erhan Akbal and Sengul Dogan, speed was also a priority. Still, there the software was compared when they were connected to two write blockers and disk imaging hardware was also compared.

Based on previous studies and research, this study will focus on the speed of disk imaging software without comparing different write blockers or types of interfaces. On the other hand, integrity will be tested by validating hash values, unlike the study conducted without a hash function [8], due to integrity being a requirement in a criminal investigation.

1.1 Scope, delimitations, and motivation

There is a wide array of disk imaging tools available on the market. Testing all known tools is unrealistic because of the time restraints on the project, and as such, the selection must be limited in some way. Six tools have been chosen to be included in this paper. The reasons why these six tools have been selected are as follows:

- (1) OSForensics and (2) FEX Imager have been chosen because they are tools that, as far as we are aware, are not included in the previous research for the area.
- (3) FTK Imager and (4) Encase Forensic Imager have been selected since they are the most widely used disk imaging tools according to the book "Cybercrime and Digital Forensics: An introduction" [9].
- (5) Guymager has been selected because this tool is built into Kali Linux, Parrot OS, and other Linux distributions specialized in digital forensics and penetration testing.
- (6) Magnet Acquire was chosen because it, to our knowledge, has not been included in any speed comparisons

There are also many formats for disk images, for example, Expert Witness Format (EWF_E01), Raw/DD, Advanced Forensic Format (AFF), dmg (Apple disk image), and asb (Ilook File Format). This means that this study needs to exclude formats that can be used due to time constraints and the fact that they are not supported by most tools in this paper. However, the formats used in the study are the most common formats for disk imaging. Images will be created in the Expert Witness Format (EWF_E01) and Raw/DD format. The Expert Witness Format is the most common format in the forensic field, while Raw/DD is another common format [10]. The study was initially designed to include another forensic image format, Advanced Forensic Format (AFF). However, it was discovered that FTK Imager struggled with the AFF format during the process. Guymager had the AFF format disabled by default as the format is no longer recommended by the original creator, Simson Garfinkel [11][12]. It was decided that the format would not be used in the study.

2 Theoretical Background

This section of the paper will present the theory behind the basic technologies used in the study.

2.1 Disk imaging

Imaging is often the first step when it comes to securing evidence. This process can be done with or without a write blocker, although for the image to be forensically sound, it should be done with a write blocker. This is to prevent any data from being modified, which can be verified by calculating a hash value.

There are many different file formats for disk images, which use different methods to create an image. In this bachelor thesis, two different image formats are used. The first one is RAW/DD, and images done with this format are made by a sector-for-sector copy of the original. The DD command was initially released in 1974 and is included by default in Unix systems. An advantage of RAW/DD images is that it copies everything sector-for-sector with no modification, and because of this, the format can be analyzed and used by any tool or system. A disadvantage of this image format is that RAW/DD does not include metadata by default, although many tools that use RAW/DD include the metadata as a text file created along with the image. Also, RAW/DD does not support any compression, which can be a problem if the user does not have enough free storage space [13][14].

The second imaging format used is the Expert Witness Format (EWF_E01). EWF_E01 is a proprietary format made by Guidance Software (now branded EnCase), which digital forensic investigators widely use. The format can store metadata with the image, and EWF_E01 supports compression. The EWF_E01 images are searchable; this can be done because when the image is created, it stores metadata, header, footers, examiner's name, etc., in the different parts of the image. The main disadvantage of EWF_E01 is that it is proprietary and therefore not supported by as many tools as the others are, both when it comes to creating EWF_E01 images and analyzing them [15].

2.2 Write blockers

A write blocker is a software or hardware solution which prevents any accidental writing to a mounted volume. If the original drive were to be altered through a write command, it would no longer be considered forensically sound and would not be admissible in court as evidentiary material. Because of this, it is of the utmost importance that any write requests are blocked. This can be achieved through a couple of different methods: mounting an image in read-only mode, using a software write blocker, and using a hardware write blocker.

Mounting media using read-only mode is much riskier than using any write blocker. It is easy to accidentally mount the volume using different options, and the likelihood of errors is much larger. It may also prove challenging to convince a court that no changes have been made when a write blocker has not been used. If available, a better option would be to use a software or hardware write blocker [16].

A software write blocker functions by operating between the operating system and the device driver for the disk. The software prevents any write requests from reaching the actual device. While certain software write blockers do work without issues, some may still allow access to the disks, and it is generally preferred to use a hardware write blocker. This is because it is argued that they are less likely to fail [17].

While the software write blocker functions between the operating system and the device driver, a hardware write blocker works as a bridge where the disk is connected to the write blocker, and the write blocker is connected to the computer. A hardware write blocker is stationed between the disk and the computer, and any read or write requests must go through the hardware. If the computer sends a write request, it will be stopped once it reaches the write blocker [16][17].

2.3 The NTFS file system

The NTFS file system was first introduced in July 1993 with the Windows NT 3.1 operating system. It has become the default file system in Windows NT systems. The maximum file size using the NTFS file system varies depending on the operating system used. The different theoretical maximum file sizes are included in the table below [18][19]. An example is the maximum file size for Windows 10 version 1709 and Server 2019, which is 8 PB minus 2 MiB.

Windows 7, Server 2008 R2 or earlier	Windows 8, Server 2012 or later	Windows 10 version 1709, Server 2019, or later
16 TB – 64 KB	256 TB – 64 KB	8 PB – 2 MiB

Table 1 - Theoretical maximum file size

The NTFS file system supports different maximum volume sizes of a partition depending on which system is using it. They can be found below.

Windows 10, version 1703, Server 2016 or earlier	Windows 10 version 1709, Server 2019 or later
256 TiB – 64 KB	8 PB – 2 MB

Table 2 - Maximum volume size

In comparison to the current maximum size of the NTFS file system, which is 8PB – 2MiB and a maximum volume size of 8 PB – 2 MB, the FAT32 file system only supports 4GB with a max volume size of 2 TB or 16TB dependent on the sector size. The ext4 file system supports volumes up to 1 EB and files with sizes up to 16 TB. While NTFS is used with Windows operating systems, the ext4 file system has been the default file system for many Linux distributions. In contrast, FAT32 is generally used for USB drives, flash memory cards, and similar storage devices when the files are

smaller than 4 GB and compatibility between different file systems is required [20].

In terms of security, the NTFS file system uses Access Control Lists (ACLs) to regulate the permissions on a file or folder. The ACL can restrict or allow access and set access types. It also includes support for BitLocker Drive Encryption. The NTFS file system saves information about a file, also known as metadata. This information includes name, creation date, permissions, and more. The file system uses a Journaling File system that keeps track of any changes made in the system. This would allow a quicker reboot if the computer were to crash and helps prevent files from becoming corrupted [21].

2.4 Single factor ANOVA and Bonferroni post hoc

A one-way analysis of variance, ANOVA, is a statistical test which determines if there are significant differences between the means of three or more groups. The ANOVA works by testing the null hypothesis, H0, that there are no significant differences in the means between the groups, and the alternative hypothesis that there are significant differences. The test uses a significance level which determines if there are any significant differences. If the p-value of the ANOVA is greater than the significance level, α, then the null hypothesis is correct. However, if the p-value is lower than the significance level then the null hypothesis is rejected and the means between groups are statistically significant. The ANOVA test itself only determines if there are differences, but not where they are [22][23].

The null hypothesis is represented as follows:

H0: $\mu_1 = \mu_2 = \mu_3 = \cdots = \mu_k$

H0 is the null hypothesis which says that the means, represented by μ, between groups 1 through k, where k is the last group, are equal, meaning that there are no significant differences.

In order to determine between which groups the differences are located, a post hoc test must be performed. For each time you do a significance test the likelihood of generating a significant result increase. The Bonferroni correction addresses this by dividing the significance level, α, by the number of tests performed in order to retain the previously determined error rate. For example: The significance level in a test is 0.05 and there will be ten significance tests. In order to account for the rising amounts of significant results the significance level is divided by 10. The Bonferroni correction would then give $\alpha/n = 0.05/10 = 0.005$. In this case the null hypothesis would only be rejected if the calculated p-value is smaller than 0.005 [24].

3 Previous research

The following section will present related and previous work in disk imaging.

3.1 NIST – Test results for disk imaging

The Office of Law Enforcement Standards of the National Institute of Standards and Technology has written several reports regarding the accuracy of disk imaging tools. This was done as part of The Computer Forensic Tool Testing (CFTT) program to provide concrete assurance that the tools used in IT forensic hard drives recreate an accurate image in the form of testing hash values. Some of the tools used were Guymager, FTK Imager, Paladin, OSForensics, and EnCase Forensic Imager.

In the test using Guymager, they tested three different write blockers and four different disks. They used two different disk types, SATA, and ATA. Both types had two different sizes of disks, one smaller than 138 GB and one larger than 138 GB. They tested both disks and partitions, and the partitions all used the NTFS file system. They created several different scenarios. In one, the disk contained 20 faulty sectors. In all scenarios where the disk image was made on a hard drive working as intended, the hash value of both the original disk and the disk image was identical. However, in the case of the hard drive with faulty sectors, there was a deviation of these sectors in the clone compared to the original [5].

In the test using FTK imager, they used two different write blockers and two different SATA disks. Just as in the previous test, one disk was smaller than 138 GB, and one was larger than 138 GB. FTK Imager could produce an image without errors [6].

In contrast to the other tools, OSForensics was used to create an image of a generic 7 GB USB device rather than a hard drive like the others. Furthermore, unlike previous tests where hardware write blockers were used, this one used the built-in software write blocker in OSForensics. They noted no differences in the hash between the device and image [25].

Another article analyzed the disk imaging tool EnCase Forensic Imager. They used EnCase Forensic Imager version 7.12.01.18, two different write blockers, and two SATA disks. The EnCase Forensic Imager tool was able to go through the scenarios as expected. However, there was one significant result. They write that an NTFS file system partition did not get the correct hash value after the imaging was done. They note that the image file was rehashed after omitting the partition slack, and after this was done, the hash value was correct. They write that the tool was able to image the file system and its contents but not the partition slack [26].

3.2 Forensics image acquisition process of digital evidence

The authors of this article state that evidence must be copied correctly to be used as evidence in a judicial setting and correct equipment is required in terms of both hardware and software. They also state that the report will investigate both hardware and software to facilitate the choice of disk imaging tools for future forensic investigations.

The article used both hardware and software to create its disk images. The hardware used to make an image was CRU Ditto and Tableau TD3. The images created with the help of software were tested with three different write blockers. The software tools used in the experiment were FTK imager and Forensic imager.

The time it takes to perform a disk image, the type of connection, and the average speed transfer was compared. The study also used compressed and uncompressed disk images. The types of disk images used were DD and EWF_E01. The Tableau TD3 was faster than the Ditto CRU in hardware disk imaging. In the case of software disk imaging, FTK imager was faster than Forensic imager [27].

3.3 The dependence of the performance of imaging tasks on the forensic imager interface type

The authors of this article state that the evidence used in a forensic investigation must maintain maximum integrity. This means that disk images must be created while using write blockers to prevent any potential changes to the information and maintain the data integrity. Therefore, they chose to perform experiments that measure both speed and integrity.

The article compared the speed of creating a disk image with and without a write blocker via USB 3.0 and between SATA III and SATA II. They concluded that a direct connection with SATA III was faster than the other alternatives [7].

3.4 Advances in digital forensics IV, chapter 26: Time analysis of hard drive imaging tools

The authors of the research article [8] included in the book "Advances in Digital Forensics IV" write that hard drives are gaining more storage capacity at an increasing rate. They believe this causes problems for digital forensic investigators and other researchers, as hard disks with more storage capacity take longer to make disk images of. Because of this, their report aims to examine how quickly the two most used disk imaging tools can perform the task.

The article compared the speed of two disk imaging programs: ICS ImageMASSter Solo Forensics III and Logicube Talon. To measure speed, they chose to turn off features unrelated to creating an image, such as hash. A software timer was used instead of manually clocking, something that can introduce human error.

The experiment consisted of two parts: First, they used an IDE cable and then a SATA cable. The tests were performed on three disks of different sizes that they judged to be representative of the disks used in forensic investigations. However, it is worth noting that the study itself is from 2008, and storage

capacities have increased since then. The tests were performed ten times per disk, and the tools were used on the same disks.

Talon performed better overall, but it also turned out that Talon was faster with an IDE connection than ImageMASSter performed on a SATA connection, which is surprising as SATA should have a faster data transfer rate [8].

3.5 Forensic disk imaging report

The Fido project (The Forensic Investigation of Digital Objects) investigated the application of digital forensics to The Higher Education Archive (UK HE). They present the role of disk imaging in forensics and general applications. These imaging formats can be used and explain the procedure that an archivist should follow when making forensically accurate imaging of media.

According to the authors, the Expert Witness Format (EWF_E01, which uses E01 as a file extension) is the most common format used in the forensic field, but some also use the Advanced Forensic Format (AFF) or Raw / DD. There are also additional formats that are not as common [10].

4 Research questions

This study seeks to provide the answers to the questions:

- Which disk imaging tool can perform disk imaging the fastest while retaining the integrity of both the original disk and the disk image?
- Is the speed of the disk imaging affected by the disk being filled to 100% compared to when it is filled to 50%?
    - If the speed is affected, which tool handles it best and how significant is the difference in speed?

4.1 Problematization of research questions

One issue is that the research question is relatively specialized and is primarily aimed at investigators who require fast imaging and individuals who need to perform a large amount of imaging. One problem with the research questions is that if the image does not live up to the criteria of retaining the integrity of both the original disk and the disk image, then the central question about the speed of the tools is no longer relevant. This means that the imaging tool will produce no valuable data to answer the central question in the thesis.

5 Method

This study will perform disk imaging using six disk imaging programs; the results will be documented and analyzed. An alternative method would be to

conduct a literature study; however, since there is a lack of previous studies regarding the speed of disk imaging tools, it would likely not produce any valuable results. The disk images will be performed by one computer.

The test computer has the following specifications:

Processor	Intel ® Core ™ i7-8750H CPU @ 2.20 GHz, six cores, 12 logical processors
RAM	16 GB, Manufacturer: SK Hynix, Speed: 2667 Mhz.
OS	Microsoft Windows 10 Home

Table 3 - Test computer specifications

More details on the computer specifications are included in the appendix [Appendix 2].

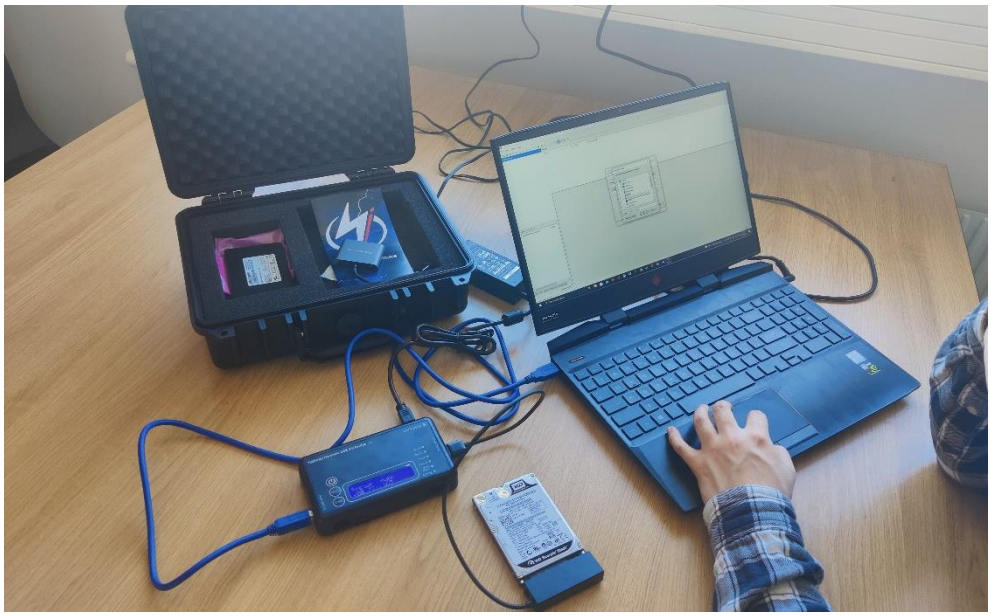

Figure 1 – Picture of the test computer, write blocker and disk 2

The write blocker used in the experiment is the Tableau Forensic USB 3.0 bridge. Three different disks will be used in this study: an SSD drive at 128GB capacity, an HDD drive at 250GB storage capacity, and an SD card with a storage capacity of 128GB. The SD card is meant to simulate the internal memory storage of a mobile device or camera. It was decided that the experiment would include both an SSD and an HDD drive to simulate the different types of disks, although there are also hybrid drives that combine both techniques. The sizes were chosen based on the time it would take to create an image. If the disks were larger, for example 1 TB, the amount of disk images or tools included in the study would have to be fewer. The specifications of the disks and the names used in this study (Disk 1, Disk 2 and the SD-card) are shown in the following table:

	Disk 1 - SSD	Disk 2 - HDD	SD-card

Vendor	Samsung	Western Digital	Samsung
Storage capacity	128GB	250GB	128GB
Model	MZ-7LN128D	WD2500BEKT-75A25T0	Samsung Evo MB-MP128GA/EU
Bus	SATA	SATA	SD-card
Read/Write speed	Up to 540/270 MB/s	No official data- User benchmarks: Max 98.8/91.7	Up to 100 MB/s

Table 4 - Test disk specifications

Figure 2 – Picture of the write blocker and disk 1

This study will create images in the Expert Witness Format (EWF_E01) and the Raw/DD format. The disk imaging tools support different disk image formats, and not all the tools support every disk image format; this is shown in the following table:

	FEX Imager	EnCase	OSForensics	FTK Imager	Guymager	Magnet Acquire
EWF_E01	✔	✔	✔	✔	✔	✔
RAW/DD	✔	N/A	✔	✔	✔	✔

Table 5 - Disk imaging tools and their supported disk image formats

In the previous research reviewed in this study, the hash value has been used to verify the integrity of the disk images made and the integrity of the original disk. Similarly, this study will also use hash values to verify integrity.

Before the disk images can be performed, the following preparations must be made:

1. Design of forms or tables for documenting experiments.
2. The hard disks in the experiments should be formatted to the proper file system.
3. Transfer predefined data to the hard drives.
4. Hash values (MD5 and SHA1) of the disks are documented.

The predefined data mentioned in step three is a sample of data copied from a hard drive in a computer that is used for everyday activities. The data consists of games, videos, images, text files, and other common files and file types.

The disk imaging process will be performed in the following order:

1. The test computer is started.
2. Test disk is connected to the test computer, with a write blocker.
3. EWF_E01 disk imaging is performed through the test tool. Hash values and elapsed time are documented.
4. DD disk imaging is performed through the test tool. Hash values and elapsed time are documented.

The process will be repeated three times for each disk imaging tool to ensure the correctness of the results.

A single factor ANOVA analysis will be performed in order to confirm if there are any significant differences in speed between the groups. The null hypothesis is that there are no significant differences. A significance threshold, α, of 0,05 has been chosen, meaning that if the P-value from the ANOVA analysis is smaller than 0,05, the null hypothesis will be rejected. That would mean that the means are different. If any ANOVA shows that there are significant differences between the groups, then a Bonferroni post hoc test will be performed to identify where the differences are.

5.1 Problematization of methods

In the previous research, some studies have included more iterations per test. For example, one paper used ten iterations per test as opposed to the three iterations used in this study [8]. Ten iterations would be preferable as it would reflect the consistency over multiple tests and as such would reflect the reality of the speed more accurately.

One issue with the study is that not all imaging tools can create images in all formats; EnCase Imager only supports the Expert Witness Format. This

means that the results of the tests will have to be divided into different categories depending on the format. It would be difficult to rank the tools in terms of overall performance. Furthermore, only the NTFS file system will be imaged in this study. Any possible differences in performance or integrity of the image depending on the file system will not be investigated.

When using the ANOVA and post hoc test, it would have been better to have more data than what is available in this paper. Since the data sample is on the small side, it is possible that the ANOVA and post hoc doesn't accurately reflect the reality of the data set. It is possible that it doesn't show statistically significant differences that would have been visible if there was more data. It is also possible that it shows statistically significant differences where there might not be any differences if more tests were conducted.

6 Results

The results chapter will illustrate all the results given by the experiment, the scoring system, the ANOVA and post hoc tests.

6.1 Disk 1, SSD 128GB

The test showed that FEX Imager was considerably slower than the other tools and was abandoned due to time constraints. Note that the time will be crossed out if a tool does not produce an image with the correct hash value. The "N/A" in the EnCase column for the DD format demonstrates that the tool cannot create those types of images. The times that are marked in green are the fastest.

The average acquisition time for each tool with the different image formats with the disk filled to 100% capacity is presented in the first table on the next page:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	18m 28s	16m 47s	17m 43s	19m 11s	15m 25s
DD avg.	16m 58s	17m 5s	18m 49s	17m 35s	N/A

Table 6 - Average acquisition time for disk 1 at 100%

The average speed in megabytes per second for the disk filled to 100% are presented in the following table:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	118.3 MB/s	129.6 MB/s	122.9 MB/s	111.6 MB/s	138.6 MB/s

DD avg.	127.5 MB/s	125.1 MB/s	115.8MB/s	123.2 MB/s	N/A

Table 7 – Average MB/s for disk 1 at 100%

The average acquisition time for each tool using different image formats with the disk filled to 50% capacity can be seen in the table below:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	15m 11s	11m 19s	16m 59s	17m 33s	14m 47s
DD avg.	15m 38s	17m 38s	15m 27s	17m 21s	N/A

Table 8 - Average acquisition time for disk 1 at 50%

The average speed in megabytes per second for the first disk filled to 50% are presented in the following table:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	140 MB/s	188.6 MB/s	126.1 MB/s	121.5 MB/s	144.3 MB/s
DD avg	136.6 MB/s	121.3 MB/s	138.1 MB/s	122.9 MB/s	N/A

Table 9 – Average MB/s for disk 1 at 50%

The tests for disk 1 show that EnCase was the fastest tool when making Expert witness format images when the disk was filled to 100%, while Guymager was the fastest tool when the disk was filled to 50%. The tests also show that FTK Imager was the fastest tool when making DD images when the disk was filled to 100%, while OSForensics was the fastest tool when the disk was filled to 50%.

The single factor ANOVA for the EWF_E01 and DD results for disk 1 filled to 100% showed that there were no significant statistical differences. The single factor ANOVA for the DD results of disk 1 filled to 50% showed that there were significant statistical differences in speed between the tools. The post-hoc test showed that the significant statistical differences were between OSForensics and Magnet Acquire, since this had the p-value 0.002128177. This value is below the statistical significance threshold which is at 0.0125 [Appendix 4].

The single factor ANOVA for the EWF_E01 results of disk 1 filled to 50% showed that there were significant statistical differences here as well. The post-hoc test showed that the significant statistical differences in speed between the tools were between the tools shown in the following table. Note that the statistical significance threshold for EWF_E01 is at 0.01:

Groups	P-value
FTK Imager – Guymager	0.006348
FTK Imager – Magnet Acquire	3.8E-05
FTK Imager – EnCase	0.009538
Guymager – OSForensics	0.001392
Guymager – Magnet Acquire	0.003506
Guymager – EnCase	0.007614
Magnet Acquire - EnCase	2.16E-05

Table 10 - Significant statistical differences - EWF_E01 - disk 1 at 50%

6.2 Disk 2, HDD 250GB

The average acquisition time for all the tools and the image formats while measuring disk 2 filled to 100% storage capacity can be seen below:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	50m 29s	50m 41s	51m 4s	51m 50s	50m 51s
DD avg.	53m 43s	51m 10s	51m 31s	51m 36s	N/A

Table 11 - Average acquisition time for disk 2 at 100%

The average speed in megabytes per second for disk 2 filled to 100% are presented in the following table:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	82.6 MB/s	82.2 MB/s	81.6 MB/s	80.4 MB/s	81.9 MB/s
DD avg.	77.6 MB/s	81.5 MB/s	80.7 MB/s	80.8 MB/s	N/A

Table 12 - Average MB/s for disk 2 at 100%

The average acquisition time for each tool in both image formats imaging disk 2 filled to 50% is presented in the table below:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	50m 45s	50m 56s	50m 56s	51m 14s	50m 46s

DD avg.	51m 45s	50m 44s	50m 56s	51m 28s	N/A

Table 13 - Average acquisition time for disk 2 at 50%

The average speed in megabytes per second for disk 2 filled to 50% are presented in the following table:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	82.1 MB/s	81.8 MB/s	81.8 MB/s	81.3 MB/s	82 MB/s
DD avg.	80.5 MB/s	82.2 MB/s	81.8 MB/s	81 MB/s	N/A

Table 14 - Average MB/s for disk 2 at 50%

The tests for disk 2 show that FTK Imager was the fastest tool when making EWF_E01 images both when the disk was filled to 100% and when the disk was filled to 50%. The tests also show that Guymager was the fastest tool when making DD images both when the disk was filled to 100% and when the disk was filled to 50%.

The single factor ANOVA for the EWF_E01 and DD results for disk 2 filled to 100% showed that there were no significant statistical differences [Appendix 4].

The single factor ANOVA for the EWF_E01 results for disk 2 filled to 50% showed that there were no major statistical differences here either [Appendix 4].

The single factor ANOVA for the DD results for disk 2 filled to 50% showed that there were significant statistical differences in speed. The post-hoc test showed that there were significant statistical differences between the following tools:

Groups	P-value
FTK Imager – Guymager	0.00138
FTK Imager – OSForensics	0.000157
Guymager – Magnet Acquire	0.004088
OSForensics – Magnet Acquire	0.001828

Table 15 - Significant statistical differences - DD - disk 2 at 50%

6.3 SD-card, 128GB

The average speed of the imaging using the SD-card filled to 100% is presented in the table below:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase

EWF_E01 avg.	22m 38s	22m 43s	23m 41s	32m 40s	22m 45s
DD avg.	23m 28s	22m 36s	23m 34s	32m 53s	N/A

Table 16 - Average acquisition time for the SD-card at 100%

The average speed in megabytes per second for the SD-card filled to 100% are presented in the following table:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	94.3 MB/s	93.9 MB/s	89.7 MB/s	65.3 MB/s	93.1 MB/s
DD avg.	91 MB/s	94.4 MB/s	90.5 MB/s	64.9 MB/s	N/A

Table 17 - Average MB/s for the SD-card at 100%

The test with the SD-card filled to 50% of the storage capacity resulted in the following average speed for each tool:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	22m 41s	22m 37s	23m 44s	32m 42s	22m 55s
DD avg.	22m 58s	22m 51s	23m 40	32m 56s	N/A

Table 18 - Average acquisition time for the SD-card at 50%

The average speed in megabytes per second for the SD-card filled to 50% are presented in the following table:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 avg.	94.1 MB/s	94.3 MB/s	89.7 MB/s	65.3 MB/s	93.1 MB/s
DD avg.	93.3 MB/s	93.4 MB/s	90.2 MB/s	64.8 MB/s	N/A

Table 19 - Average MB/s for the SD-card at 50%

The tests for the SD-card show that Guymager was the fastest tool for both EWF_E01 and DD images. Guymager was also the fastest both when it comes to the SD-card being filled to 100% and to 50%.

When performing the ANOVA for the E01 format with the SD-card filled to 100%, it showed that there were significant statistical differences in speed. After performing the post hoc, the following groups were identified as having significant differences:

Groups	P-value

FTK Imager – OSForensics	0.002685008
FTK Imager – Magnet Acquire	6.3875E-07
Guymager – OSForensics	0.002635392
Guymager – Magnet Acquire	0.00018457
OSForensics – Magnet Acquire	8.16354E-05
OSForensics – EnCase	0.004269706
Magnet Acquire - EnCase	0.000219728

Table 20 - Significant statistical differences - EWF_E01 - SD-card at 100%

The DD images of the SD-card filled to 100% capacity also showed that there were considerable differences in speed between the tools in this case as well. The groups that showed differences are presented in the following table:

Groups	P-value
FTK Imager – Magnet Acquire	0,009213094
Guymager – OSForensics	0,000141198
Guymager – Magnet Acquire	1,05634E-06
OSForensics – Magnet Acquire	1,8923E-09

Table 21 - Significant statistical differences - DD - SD-card at 100%

There were also significant differences when the SD-card was filled to 50% in both image formats. The differences are shown in the tables below:

EWF_E01 format:

Groups	P-value
FTK Imager – Magnet Acquire	2,69E-06
Guymager – Magnet Acquire	2,84E-09
OSForensics – Magnet Acquire	0,0005
Magnet Acquire - EnCase	0,001439

Table 22 - Significant statistical differences - EWF_E01 - SD-card at 50%

DD format:

Groups	P-value
FTK Imager – Magnet Acquire	3,89E-06
Guymager – Magnet Acquire	0,000396
OSForensics – Magnet Acquire	1,51E-05

Table 23 - Significant statistical differences - DD - SD-card at 50%

6.4 Speed difference between 100% and 50%

The following table presents the speed difference in MB/s using the EWF_E01 format for disks at 100% and 50%:

EWF_E01	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
Avg. 100%	98.4 MB/s	101.9 MB/s	98.2 MB/s	85.8 MB/s	104.8 MB/s
Avg. 50%	105.4 MB/s	121.6 MB/s	99.2 MB/s	89.4 MB/s	106.5 MB/s
Difference	7 MB/s	19.7 MB/s	1 MB/s	3.6 MB/s	1.7 MB/s
Difference in %	7.1%	19.3%	1%	4.1%	1.6%

Table 24 - Speed difference EWF_E01

The acquisition was faster when imaging the disks filled to 50% as opposed to the disks filled to 100% regardless of the tool used. However, there is a significant variance between the different groups in terms of how much faster it was in comparison to the speed of the 100% capacity tests. Guymager was significantly faster when imaging the 50% disks, it was 19.7 MB/s faster. In comparison, OSForensics was only 1 MB/s faster when imaging the disks at 50% in comparison to imaging at full capacity. Guymager was the fastest tool overall when performing the images at 50% while EnCase was the fastest when performing an image of a disk at full capacity.

The following table illustrates the speed difference in MB/s using the DD format for disks at 100% and 50%:

DD	FTK Imager	Guymager	OSForensics	Magnet Acquire
Avg. 100%	98.7 MB/s	100.3 MB/s	95.7 MB/s	89.6 MB/s
Avg. 50%	103.5 MB/s	99 MB/s	103.4 MB/s	89.6 MB/s
Difference	4.8 MB/s	1.3 MB/s*	7,7 MB/s	0 MB/s
Difference in %	4.9%	-1,30%	8,05%	0%

Table 25 - Speed difference DD

**In contrast to the other disk imaging tools, Guymager was slower when imaging the disks filled to 50% than the disk filled to 100%.*

The results show that the tools were faster when creating disk images of a disk filled to 50% as opposed to 100% when using the expert witness format and were generally faster when using the DD format as well. However, Magnet Acquire showed no difference using the DD format, and Guymager was slower. When comparing all the individual tests using the DD format,

Guymager had a slower speed when imaging the 50% disk in three out of four tests. Magnet Acquire was slower when imaging at 50% in the DD format in two out of four tests.

6.5 The overall result

During the experiment there were no images where the integrity was compromised. Every disk image was verified without any issues.

All the tests are put together in the tables below, where the tools have been given a score for each test. The total amount of images created is 162 and the imaging time without verification amounts to about 83 hours and 45 minutes. The verification of images took around as long as the imaging itself, as such the experiment took about 160 hours in total. The score for EWF_E01 is based on the average speed in MB/s, where the fastest tool for each test was awarded 5 points and the slowest was awarded 1 point. This can be seen in the following table on the next page:

EWF_E01 table	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
Disk 1, 100%	2	4	3	1	5
Disk 1, 50%	3	5	2	1	4
Disk 2, 100%	5	4	2	1	3
Disk 2, 50%	5	3	3	1	4
SD-card, 100%	5	4	2	1	3
SD-card, 50%	4	5	2	1	3
Total score	24	25	14	6	22

Table 26 - EWF_E01 scoring table

The same was done for the score of the DD tests. However, since there are only four tools in the DD tests, the fastest tool for each test will instead be awarded 4 points. The slowest tool is still awarded 1 point. The DD score table is presented below:

DD table	FTK Imager	Guymager	OSForensics	Magnet Acquire
Disk 1, 100%	4	3	1	2
Disk 1, 50%	3	1	4	2
Disk 2, 100%	1	4	2	3
Disk 2, 50%	1	4	3	2

SD-card, 100%	3	4	2	1
SD-card, 50%	3	4	2	1
TOTAL	15	20	14	11

Table 27 - DD scoring table

The overall score shows that Guymager had the highest total score, in both the EWF_E01 and DD tests.

7 Discussion

One of the earliest discoveries when conducting the experiment was the fact that FEX Imager was considerably slower than the other tools. FEX Imager had an average speed of 47 MB/s when creating EWF_E01 images and an average speed of 48.2 MB/s when creating DD images. Compare this to the slowest of the other tools in that test, the slowest for EWF_E01 was Magnet Acquire with a speed of 111.6 MB/s and the slowest for DD was OSForensics at a speed of 115.8 MB/s. This means that FEX Imager had less than half of the speed that the slowest of the other tools had. Because of this, it was decided that the rest of the tests would be done without FEX Imager. The tests still took about 160 hours of active imaging to complete, and it would have taken far too much time to include FEX Imager in all other tests.

One thing that is not researched in this bachelor thesis is whether the size of the disk being imaged could affect the speed of the tools. For example, there might be a chance that the speed of the tools scales differently when making an image that is a copy of an SSD at 128 GB compared to an image made of an SSD at 1 TB.

One criterion when conducting the tests was that the integrity of the disk and disk image would be maintained. The reason for the inclusion of this criteria was that the disk imaging conducted in the experiment must be forensically sound. In order to test this, hash verification using SHA-1 and MD5 was used. In previous research conducted by NIST, Guymager and OSForensics produced faulty images when imaging disks with faulty sectors. In this study no faulty sectors were used, and it produced no incorrect images [5][26]. The experiment also used a hardware write blocker to prevent any accidental write commands from the computer. One facet of the tools that wasn't tested during the experiment was whether the tools themselves have write-blocking capabilities and how effective they would be. This is because the hardware write blocker was used. Furthermore, no comparison has been made in terms of speed differences when using a write blocker versus not using a write blocker. Since no such comparison was made, it's not possible to say if and how much faster imaging would be if the disk or SD-card was connected directly to the computer.

It should also be noted that verifying significantly increases the time it takes to create the disk images. When creating the disk images, the verification time was approximately as long as the imaging itself in most cases.

In order to assess whether a tool is more effective than another, this study used a single factor ANOVA test to detect any significant statistical differences. The ANOVA test was supplemented with a Bonferroni post hoc test to identify where the differences have occurred. When looking at all the individual ANOVA tests on the disks, disk 1 and disk 2 showed no statistically significant differences when performing imaging on the disks filled to 100% regardless of format. Although there were no differences that were significant from a statistical perspective, there were still differences in speed that could be identified when comparing the time it took and the average speed of the imaging. Even though it wasn't possible to say that the differences were significant from a statistical point of view, perhaps due to the limited number of tests performed, it still provides anecdotal evidence that there is some difference. However, this would not be considered solid enough to truly argue that there is a difference.

One exception to this is the SD-card, which showed statistically significant differences in all tests performed, both when using different formats and percentage of storage capacity used.

When conducting tests on the disks and the SD-card filled to 50%, all images in the DD format suggested significant differences in the acquisition speed. The EWF_E01 format also showed significant statistical differences when imaging disk 1 and the SD-card.

When looking at the fastest tool for each category and the results of the ANOVA, only seven out of twelve showed a statistically significant difference between tools. This can be seen in the two following tables:

EWF_E01 table	Fastest tool	Significant ANOVA?
Disk 1, 100%	EnCase	No
Disk 1, 50%	Guymager	Yes
Disk 2, 100%	FTK Imager	No
Disk 2, 50%	FTK Imager	No
SD-card, 100%	FTK Imager	Yes
SD-card, 50%	Guymager	Yes

Table 28 - Significant ANOVA for fastest tool - EWF_E01

DD table	Fastest tool	Significant ANOVA?

Disk 1, 100%	FTK Imager	No
Disk 1, 50%	OSForensics	Yes
Disk 2, 100%	Guymager	No
Disk 2, 50%	Guymager	Yes
SD-card, 100%	Guymager	Yes
SD-card, 50%	Guymager	Yes

Table 29 - Significant ANOVA for fastest tool - DD

The first test that showed a significant difference was the EWF_E01 test with disk 1 at 50%. In this case, the fastest tool was Guymager. When looking at the post hoc results it shows that Guymager was significantly faster than all other tools, meaning that not only is Guymager faster anecdotally, but it is also supported by the post hoc.

The next test which showed any significant differences was the EWF_E01 test of the SD card at 100%. This test also showed that Guymager is the fastest tool. However, in this test it only showed that it was significantly faster from a statistical point of view in comparison to the two slowest tools, Magnet Acquire and OSForensics. This suggests that the top three tools are similar enough in speed that a major difference is not supported by any statistical evidence. Despite this the tool is somewhat faster in the collected data.

The next test using the EWF_E01 image format that showed significant statistical differences was the SD card test at 50%. The winner in this test was Guymager. In this case, Guymager is only significantly faster than Magnet Acquire. In a similar manner, every tool in the test is significantly faster than Magnet Acquire. This means that the only differences supported by statistical evidence is that Magnet Acquire is slower than all other tools, and that the differences aren't significant from a statistical point of view between any other tools.

Moving on to the DD format, the image of disk 1 at 50%, OSForensics was the fastest tool. The only statistically significant differences between individual tools were between OSForensics and the slowest tool, Magnet Acquire.

The second test which showed statistically significant differences was disk 2 at 50%, where the fastest tool was Guymager. In this case, Guymager was only significantly faster than the two slowest tools, and the second fastest tool OSForensics was also significantly faster than those tools. This suggests that the top two tools are both faster than the others, but that there are no statistical differences between the two fastest tools. Looking from a purely statistical point of view, this means that it would not be significantly faster to choose

Guymager over OSForensics but based on the anecdotal evidence it may still end up being slightly faster.

The next test highlighted by the ANOVA is the SD card filled to 100% created in the DD format. The fastest tool was Guymager in this test as well. Guymager is faster than the two slowest tools, Magnet Acquire and OSForensics. The second fastest is not significantly slower than Guymager, but it is significantly faster than Magnet Acquire which is the slowest tool. Magnet Acquire is also statistically slower than OSForensics which is the second slowest tool. Similarly to other tests, this test also shows that the top two tools have no significant statistical differences.

In the same way as the previous test, Guymager was the fastest and Magnet Acquire was the slowest. All tools included in the test are significantly faster than Magnet Acquire, without any significant statistical differences between any of the other tools.

Overall, the fastest tool was generally faster than the slowest or the two slowest tools and the top two tools generally had minimal statistical differences. There are however a couple of exceptions, a notable example being the EWF_E01 image of disk 1 filled to 50% where Guymager was significantly faster than all other tools. While there is very little statistical evidence that the top tool is faster than all others in the majority of all the tests, it could still be worth it to consider all the data collected as a whole. There may not be any significant statistically supported differences at the top of the scale, but there is still a difference when simply looking at the results.

During the tests Guymager was used on a Manjaro Linux live system on a USB drive. It's possible that Guymager would have been capable of running even faster if it had been run directly from the PC in the same manner as the tools used through Windows.

When comparing the results in this paper with the results of previous research, there is to the best of our knowledge no other paper that includes the same disk imaging tools. Thus, a real result comparison would not be possible or fair.

8 Conclusion

This study included an experiment with 162 disk imaging tests, which had an active imaging and verification time of over 160 hours. The results have been analyzed both by interpreting the speed (MB/s), scoring system and by making ANOVA tests followed by a Bonferroni post hoc test.

The main research question for this bachelor thesis was: Which disk imaging tool can perform disk imaging the fastest while retaining the integrity of both the original disk and the disk image?

As shown in the result and discussion sections of this paper, there are several answers to the main research question. The detailed answer is presented in the summary table below. The tools were compared using a scoring system where 5 points are awarded to the fastest tool for each disk in the EWF_ E01 category, and 4 points are awarded to the fastest tool in the DD category. Second place receives 4 points or 3 points respectively. The points decrease per position down to 1 point for the slowest tool. The total amount of points determines which tool is the fastest in each category. The last two rows show the overall ranking for each disk image format. The column to the far-right notes whether the tests showed any statistically significant differences when performing an ANOVA analysis. The summary score table on the next page is based on the speed (MB/s) results and is also explained in the discussion part of the paper:

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase	Significant
EWF_E01 Disk1,100%	2	4	3	1	5	No
DD Disk1, 100%	4	3	1	2	N/A	No
EWF_E01 Disk1,50%	3	5	2	1	4	Yes
DD Disk1, 50%	3	1	4	2	N/A	Yes
EWF_E01 Disk2,100%	5	4	2	1	3	No
DD Disk2, 100%	1	4	2	3	N/A	No
EWF_E01 Disk2, 50%	5	3	3	1	4	No
DD Disk2, 50%	1	4	3	2	N/A	Yes
EWF_E01 SD, 100%	5	4	2	1	3	Yes
DD SD, 100%	3	4	2	1	N/A	Yes
EWF_E01 SD, 50%	4	5	2	1	3	Yes
DD SD, 50%	3	4	2	1	N/A	Yes
Total EWF_E01 score	24	25	14	6	22	
Total DD score	15	20	14	11	N/A	

Table 30 - Conclusion summary table

When it comes to just looking at the total score, the answer to the main research question, **"which disk imaging tool can perform disk imaging the fastest while retaining the integrity of both the original disk and the disk image?", becomes the following: Guymager is the fastest disk imaging tool**, **since it had the highest total score in both categories.** However, not all individual tests showed that it was significantly faster than all of the other tools, meaning that it is based on both statistical and anecdotal evidence. When imaging in EWF_ E01, Guymager was the fastest in 3 out of 6 tests and placed first overall. However, only one test showed that it was

significantly faster in comparison to all other tools. In combination with anecdotal evidence however, it is the fastest tool when creating a EWF_E01 disk image.

The secondary research question was the following: **Is the speed of the disk imaging affected by the disk being filled to 100% compared to when it is filled to 50%? The answer to this question is that the speed of the disk imaging is affected by the disk being filled to 100% compared to when it is filled to 50%**. Although, the speed difference is most noticeable for FTK Imager and Guymager when it comes to making EWF_E01 images. For DD images, the speed difference is most noticeable for OSForensics. It should be noted that Guymager was an exception to the rule as it was slower when imaging a disk filled to 50% in the DD format.

The sub question to the second research question was: **If the speed is affected, which tool handles it best and how significant is the difference in speed? The answer is that Guymager handles it best for EWF_E01 images and OSForensics handles it best for DD images.** Guymager was 19.3% faster when making EWF_E01 images of disks filled to 50% compared to when making EWF_E01 images of disks filled to 100%. OSForensics was 8.05% faster when making DD images of disks filled to 50% compared to when making DD images of disks filled to 100%.

9 Future work

One thing which this study did not cover but that could be of interest is the scaling of the tools when using disks of increasing sizes. This study was limited to a narrow span of disk sizes, from 128 to 250GB. It is possible that the tools that were slower may have scaled better than the others as the size increases. This could result in the gap between the speed of the tools diminishing.

Another suggestion for future research is that it would certainly give more statistically significant results if the tests were narrowed to fewer disk imaging tools and instead doing more tests with just these tools. That would be beneficial when it comes to making ANOVA and post hoc tests with the results.

This study only used the EWF_E01 and RAW/DD format and did not include others such as AFF4, EWF_Ex01, SMART or any other disk formats. Since the study demonstrated that certain tools handle one format better than the other it could be valuable to investigate what tools would be most effective on other formats.

Furthermore, this study used a write blocker. The effect of this write blocker on the imaging speed is unknown, as such it could be valuable to not only compare this write blocker to others, but also to do tests both with and without the write blocker.

The tests showed that the difference in speed between disks filled to 100% compared to 50% was smaller using disk number two, the HDD with a storage capacity of 250 GB, in comparison to the other two. Further research would be necessary to discover if the fact that it is an HDD is the reason for the slower speed when creating a disk image filled to 50%.

References

[1] "Malware Statistics & Trends Report | AV-TEST", Av-test.org, 2022. [Online]. Available: https://www.av-test.org/en/statistics/malware/. [Accessed: 21- Jan- 2022].

[2] "Economic Impact of Cybercrime Report | McAfee", Mcafee.com, 2017. [Online]. Available: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html. [Accessed: 21- Jan- 2022].

[3] K. Curran and A. Ijeh, Crime Science and Digital Forensics - A Holistic View, 1st ed. Boca Raton: CRC Press, 2021, p. 102.

[4] P. Bergström, "Frågor om diskavbildning (Questions about disk imaging)", 2022, Appendix 1.

[5] Homeland Security, "Test results for disk imaging tool: Guymager v0.8.1", Homeland Security, 2016.

[6] Homeland Security, "Test Result for Disk Imaging Tools: FTK Imager Version 4.3.0.18", Homeland Security, 2020.

[7] F. Tebueva, M. Ogur, M. Zubkov, and M. Moisov, "The dependence of the performance of imaging tasks on the forensic imager interface type", IOP Conference Series: Materials Science and Engineering, vol. 1069, no. 1, 2021. Available: https://iopscience.iop.org/article/10.1088/1757-899X/1069/1/012048/pdf. [Accessed 20 January 2022].

[8] I. Ray, S. Shenoi, J. Riley, D. Dampier, and R. Vaughn, “26,” in Advances in Digital Forensics IV, Boston, MA: International Federation for Information Processing, 2008, pp. 335–343.

[9] A. M. Bossler, T. J. Holt, and K. C. Seigfried-Spellar, Cybercrime and Digital Forensics: An introduction, New York, NY: Routledge, 2018. p. 536.

[10] G. Knight, Forensic Disk Imaging Report, King's College London, London, rep., 2011.

[11] S. Garfinkle [@xchatty], “This is an official publication of Simson Garfinkel: I no longer support AFF”, Twitter, 30-March-2022. Available: https://twitter.com/xchatty/status/1509204638888861704?s=20&t=XU9VferXlwItPL_oN3gDdQ [Accessed: 02-April-2022]

[12] S. Garfinkle [@xchatty], “Meaning that I no longer provide software support for the AFF file format. This is not a comment on AFF4. Sorry for any confusion”, Twitter, 31-March-2022. Available: https://twitter.com/xchatty/status/1509204638888861704?s=20&t=XU9VferXlwItPL_oN3gDdQ [Accessed: 02-April-2022]

[13] "dd (Unix) - Wikipedia", En.wikipedia.org, 2022. [Online]. Available: https://en.wikipedia.org/wiki/Dd_(Unix). [Accessed: 01- Apr- 2022].

[14] "Forensics 101: What is a forensic image? - Raedts.BIZ | IT SECURITY & FORENSICS", Raedts.BIZ | IT SECURITY & FORENSICS, 2022. [Online]. Available: https://www.raedts.biz/forensics/forensics-101-forensic-image/. [Accessed: 01- Apr- 2022].

[15] Garfinkel, Simson L., David J. Malan, Karl-Alexander Dubec, Christopher C. Stevens, and Cecile Pham. 2006. Advanced forensic format: An open, extensible format for disk imaging. In Advances in Digital Forensics II: FIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, January 29-February 1, 2006, ed. Martin Olivier and Sujeet Shenoi, 17-31. New York: Springer.

[16] M. Solomon, K. Rudolph, and E. Tittel, Computer Forensics JumpStart, 2nd ed. John Wiley & Sons, 2011, pp. 74 - 75.

[17] A. M. Bossler, T. J. Holt, and K. C. Seigfried-Spellar, Cybercrime and Digital Forensics: An introduction, New York, NY: Routledge, 2018. p. 530-531

[18] "[MS-FSA]: Appendix A: Product Behavior", Docs.microsoft.com, 2021. [Online]. Available: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-fsa/4e3695bd-7574-4f24-a223-b4679c065b63. [Accessed: 01- Apr- 2022].

[19] P. Bhardwaj and K. Andreou, How to cheat at Windows system administration, Using command-line scripts, 1st ed. Rockland, MA: Syngress, 2006, pp. 140 - 141.

[20] V. Damjanovski, CCTV, 3rd Edition, 3rd ed. Butterworth-Heinemann, 2014, pp. 335 - 339.

[21] K. Laine Rusbarsky, "A Forensic Comparison of NTFS and FAT32 File Systems", Marshall University, 2012.

[22] "One-way ANOVA - An introduction to when you should run this test and the test hypothesis | Laerd Statistics", Statistics.laerd.com, 2022. [Online]. Available: https://statistics.laerd.com/statistical-guides/one-way-anova-statistical-guide.php. [Accessed: 05- May- 2022].

[23] "LibGuides: SPSS Tutorials: One-Way ANOVA", Libguides.library.kent.edu, 2022. [Online]. Available: https://libguides.library.kent.edu/spss/onewayanova. [Accessed: 05- May- 2022].

[24] "Post Hoc Definition and Types of Tests", Statistics How To, 2022. [Online]. Available: https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/post-hoc/. [Accessed: 05- May- 2022].

[25] Homeland Security, "Test results for disk imaging tool: OSForensics 8.0.1007", Homeland Security, 2021.

[26] Homeland Security, "EnCase Forensic Version 7.12.01.18, Windows 7", Homeland Security, 2018

[27] E. Akbal and S. Dogan, "Forensics Image Acquisition Process of Digital Evidence", International Journal of Computer Network and Information Security, vol. 10, no. 5, pp. 1-8, 2018. Available: https://www.mecs-press.org/ijcnis/ijcnis-v10-n5/IJCNIS-V10-N5-1.pdf. [Accessed 20 January 2022].

Appendices

Appendix 1: Interview with Peter Bergström from the National Forensic Center (in Swedish)

1. Hur påverkar hastigheten av de diskavbildningsverktyg ni använder ert arbete?

Svar: För att på bästa sätt stödja arbetet med brottsutredningar ska verksamheten vara rättssäker och effektiv. Det är därför viktigt att diskavbildningar blir så korrekta som möjligt och att det går snabbt så att det inte blir en flaskhals i verksamheten.

2. Finns det något verktyg som används oftare än andra?

Svar: Vi använder ett flertal olika verktyg då de ofta kompletterar varandra. Vilka och hur flödena ser ut varierar över tid.

3. Ligger det i ert intresse att få reda på vilket eller vilka diskavbildningsprogram som är snabbast?

Svar: Viktigast är hur korrekt resultatet är. Har vi dock två likvärdiga verktyg är hastigheten viktigt för att få en så effektiv verksamhet som möjligt.

Appendix 2: Test computer system information

The system Information report was written at 04/01/22 17:46:06

[System Summary]

OS Name: Microsoft Windows 10 Home

Version: 10.0.19044 Build 19044

OS Manufacturer: Microsoft Corporation

System Manufacturer: HP

System Model: OMEN by HP Laptop 15-dc0xxx

System Type: x64-based PC

System SKU: 4KG70EA

Processor: Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz, 2208 MHz, 6 Core(s), 12 Logical Processor(s)

BIOS Version/Date: AMI F.15, 2020-11-02

SMBIOS Version: 3.2

Embedded Controller Version: 93.24

BIOS Mode: UEFI

BaseBoard Manufacturer: HP

BaseBoard Product: 84DB

BaseBoard Version: 93.24

Platform Role: Mobile

Hardware Abstraction Layer: Version = "10.0.19041.1566"

Installed Physical Memory (RAM): 16,0 GB

Total Physical Memory: 15,9 GB

Available Physical Memory: 10,7 GB

Total Virtual Memory: 17,1 GB

Available Virtual Memory: 9,88 GB

Page File Space: 1,24 GB

Appendix 3: Disk imaging results tables

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase	FEX Imager

EWF_E01-Test1	22m 12s	20m 10s	17m 44s	18m 37s	16m 12s	45m 23s
EWF_E01-Test2	15m 13s	15m 17s	14m 37s	18m 2s	15m 2s	*
EWF_E01-Test3	17m 59s	14m 53s	20m 49s	20m 56s	15m	*
DD-Test1	17m 15s	16m 3s	15m 10s	18m 33s	N/A	44m 14s
DD-Test2	14m 25s	18m 1s	20m 20s	14m 40s	N/A	*
DD-Test3	19m 15s	17m 12s	20m 58s	19m 33s	N/A	*

Appendix 3 – Table 1 – Acquisition time for disk 1 at 100%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase	FEX Imager
EWF_E01-Test1	96.0960961	105.785124	120.3007519	114.5926589	131.6872428	47.00697759823724
EWF_E01-Test2	140.1971522	139.5856052	145.9521095	118.2994455	141.9068736	*
EWF_E01-Test3	118.6283596	143.3370661	102.4819856	101.910828	142.2222222	*
DD-Test1	123.6714976	132.9179647	140.6593407	115.0044924	N/A	48.22908816880181
DD-Test2	147.9768786	118.4088807	104.9180328	145.4545455	N/A	*
DD-Test3	110.8225108	124.0310078	101.7488076	109.1219096	N/A	*

Appendix 3 – Table 2 - MB/s for disk 1 at 100%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	15m 8s	10m 53s	15m 35s	17m 27s	14m 42s
EWF_E01 - Test 2	15m 12s	11m 20s	18m 12s	17m 32s	14m 55s
EWF_E01 - Test 3	15m 22s	11m 45s	17m 10s	17m 41s	14m 44s
DD-Test 1	15m 12s	16m 26s	15m 33s	17m 17s	N/A
DD-Test 2	16m 31s	18m 40s	15m 33s	17m 22s	N/A
DD-Test 3	15m 12s	17m 48s	15m 14s	17m 25s	N/A

Appendix 3 – Table 3 - Acquisition time of disk 1 at 50%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	140.969163	196.0183767	136.8983957	122.2540592	145.1247166
EWF_E01 - Test 2	140.3508772	188.2352941	117.2161172	121.6730038	143.0167598
EWF_E01 - Test 3	138.8286334	181.5602837	124.2718447	120.6409048	144.7963801
DD - Test 1	140.3508772	129.8174442	137.1918542	123.4329797	N/A
DD - Test 2	129.1624622	114.2857143	137.1918542	122.840691	N/A
DD - Test 3	140.3508772	119.8501873	140.0437637	122.4880383	N/A

Appendix 3 – Table 4 - MB/s for disk 1 at 50%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	49m 17s	50m 41s	51m 5s	52m 11s	50m 37s
EWF_E01 - Test 2	50m 13s	50m 41s	51m 1s	51m 8s	51m 10s

EWF_E01 - Test 3	51m 58s	50m 42s	51m 5s	52m 11s	50m 45s
DD-Test1	54m 41s	50m 40s	52m 41s	51m 44s	N/A
DD-Test2	51m 57s	52m 9s	51m 6s	51m 43	N/A
DD-Test3	54m 31s	50m 41s	50m 46s	51m 21s	N/A

Appendix 3 – Table 5 – Acquisition time for disk 2 at 100%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	84.54514711	82.20979941	81.56606852	79.84669435	82.31807705
EWF_E01 - Test 2	82.97378029	82.20979941	81.67265599	81.4863103	81.43322476
EWF_E01 - Test 3	80.17960231	82.18277449	81.56606852	79.84669435	82.10180624
DD - Test 1	76.19628162	82.23684211	79.08889592	80.54123711	N/A
DD - Test 2	80.20532563	79.8977309	81.5394651	80.56719304	N/A
DD - Test 3	76.42922654	82.23684211	81.5394651	81.14248621	N/A

Appendix 3 – Table 6 - MB/s for disk 2 at 100%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	50m 40s	51m 12s	50m 59s	51m 4s	50m 46s
EWF_E01 - Test 2	50m 50s	50m 52s	50m 50s	51m 3s	50m 46s
EWF_E01 - Test 3	50m 56s	50m 43s	50m 59s	51m 35s	50m 46s
DD - Test 1	51m 44s	50m 50s	51m 0s	51m 34s	N/A
DD - Test 2	51m 50s	50m 41s	50m 54s	51m 23s	N/A
DD - Test 3	51m 41s	50m 41s	50m 53s	51m 27s	N/A

Appendix 3 – Table 7 – Acquisition time for disk 2 at 50%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	82.23684211	81.38020833	81.72605427	81.5926893	82.07485227
EWF_E01 - Test 2	81.96721311	81.91349934	81.96721311	81.61932746	82.07485227
EWF_E01 - Test 3	81.80628272	82.15576733	81.72605427	80.77544426	82.07485227
DD - Test 1	80.54123711	82.23684211	81.69934641	80.80155139	N/A
DD - Test 2	80.61915511	82.20979941	81.85985593	81.08984755	N/A
DD - Test 3	80.38585209	82.20979941	81.88666885	80.98477486	N/A

Appendix 3 – Table 8 - MB/s for disk 2 at 50%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	22m 39s	22m 54s	23m 34s	32m 40s	22m 38s
EWF_E01 - Test 2	22m 38s	22m 37s	23m 46s	32m 40s	22m 57s
EWF_E01 - Test 3	22m 38s	22m 37s	23m 42s	32m 40s	22m 39s
DD - Test 1	24m 49s	22m 36s	23m 36s	32m 49s	N/A
DD - Test 2	22m 47s	22m 37s	23m 33s	32m 53s	N/A

DD - Test 3	22m 49s	22m 36s	23m 32s	32m 57s	N/A

Appendix 3 – Table 9 - acquisition time for the SD-card at 100%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	94.18690213	93.1586608	90.52333805	65.30612245	94.2562592
EWF_E01 - Test 2	94.2562592	94.3257185	89.76157083	65.30612245	92.9557008
EWF_E01 - Test 3	94.2562592	94.3257185	90.0140647	65.30612245	94.18690213
DD - Test 1	85.96373405	94.39528024	90.39548023	65.00761808	N/A
DD - Test 2	93.63569861	94.3257185	90.58740269	64.87582362	N/A
DD - Test 3	93.49890431	94.39528024	90.65155807	64.74456247	N/A

Appendix 3 – Table 10 - MB/s for the SD-card at 100%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	22m 38s	22m 37s	24m 3s	32m 40s	22m 42s
EWF_E01 - Test 2	22m 44s	22m 38s	23m 32s	32m 41s	23m 27s
EWF_E01 - Test 3	22m 40s	22m 38s	23m 36s	32m 44s	22m 37s
DD - Test 1	22m 59s	23m 20s	23m 43s	33m 7s	N/A
DD - Test 2	22m 58s	22m 36s	23m 35s	33m 5s	N/A
DD - Test 3	22m 57s	22m 36s	23m 41s	32m 35s	N/A

Appendix 3 – Table 11 – Acquisition time for the SD-card at 50%, all tests

	FTK Imager	Guymager	OSForensics	Magnet Acquire	EnCase
EWF_E01 - Test 1	94.2562592	94.3257185	88.7040887	65.30612245	93.979442
EWF_E01 - Test 2	93.84164223	94.2562592	90.65155807	65.27281999	90.97370291
EWF_E01 - Test 3	94.11764706	94.2562592	89.76157083	65.17311609	94.3257185
DD - Test 1	92.8208847	91.42857143	89.95080815	64.41872169	N/A
DD - Test 2	92.88824383	94.39528024	90.45936396	64.4836272	N/A
DD - Test 3	94.3257185	94.39528024	90.07741027	65.47314578	N/A

Appendix 3 – Table 12 - MB/s for the SD-card at 50%, all tests

Appendix 4: ANOVA and post hoc

EWF_E01 Disk 1, 100%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	354.9216	118.3072	486.3031
Guymager	3	388.7078	129.5693	427.7824
OSForensics	3	368.7348	122.9116	477.5254
Magnet Acquire	3	334.8029	111.601	73.85931
EnCase	3	415.8163	138.6054	35.92102

SUMMARY

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1294.399	4	323.5997	1.077666	0.417542	3.47805
Within Groups	3002.782	10	300.2782			
Total	4297.181	14				

DD Disk 1, 100%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	382.470887	127.4902957	356.0491756
Guymager	3	375.3578531	125.1192844	53.51663933
OSForensics	3	347.3261811	115.7753937	466.9191095
Magnet Acquire	3	369.5809475	123.1936492	380.3118231

ANOVA

Source of variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	230.5265043	3	76.8421681	0.24456514	0.862955241	4.066180551
Within Groups	2513.593495	8	314.1991869			
Total	2744.119999	11				

EWF_E01 Disk 1, 50%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	420.1487	140.0496	1.213562
Guymager	3	565.814	188.6047	52.36143
OSForensics	3	378.3864	126.1288	99.43419
Magnet Acquire	3	364.568	121.5227	0.66752
EnCase	3	432.9379	144.3126	1.286389

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	8489.44	4	2122.36	68.47953	3.16E-07	3.47805
Within Groups	309.9262	10	30.99262			
Total	8799.367	14				

Post-hoc table:

Groups	P-value	Significant?
FTK Imager – Guymager	0.006348	Yes
FTK Imager – OSForensics	0.135152	No
FTK Imager – Magnet Acquire	3.8E-05	Yes
FTK Imager – EnCase	0.009538	Yes
Guymager – OSForensics	0.001392	Yes
Guymager – Magnet Acquire	0.003506	Yes
Guymager – EnCase	0.007614	Yes

OSForensics – Magnet Acquire	0.507887	No
OSForensics – EnCase	0.085468	No
Magnet Acquire - EnCase	2.16E-05	Yes

DD Disk 1, 50%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	409.8642	136.6214	41.72688
Guymager	3	363.9533	121.3178	61.92403
OSForensics	3	414.4275	138.1425	2.711129
Magnet Acquire	3	368.7617	122.9206	0.228014

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	706.1806	3	235.3935	8.833602	0.006419	4.066181
Within Groups	213.1801	8	26.64751			
Total	919.3607	11				

Post-hoc table:

Groups	P-value	Significant?
FTK Imager – Guymager	0.062103	No
FTK Imager – OSForensics	0.72693	No
FTK Imager – Magnet Acquire	0.065997	No
Guymager – OSForensics	0.060261	No
Guymager – Magnet Acquire	0.758163	No
OSForensics – Magnet Acquire	0.002128	Yes

EWF_E01 Disk 2, 100%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	247.6985297	82.56617657	4.889100945
Guymager	3	246.6023733	82.2007911	0.000243449
OsForensics	3	244.804793	81.60159768	0.003786963
Magnet Acquire	3	241.179699	80.393233	0.896113488
EnCase	3	245.8531081	81.95103602	0.212789639

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*

Between Groups	8.317007932	4	2.079251983	1.732122657	0.21912688	3.478049691
Within Groups	12.00406897	10	1.200406897			
Total	20.3210769	14				

DD Disk 2, 100%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	232.8308	77.61028	5.06427
Guymager	3	244.3714	81.45714	1.823814
OSForensics	3	242.1678	80.72261	2.001763
Magnet Acquire	3	242.2509	80.75031	0.115523

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	26.53847	3	8.846156	3.929281	0.054017	4.066181
Within Groups	18.01074	8	2.251342			
Total	44.54921	11				

EWF_E01 Disk 2, 50%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	246.0103379	82.00344598	0.047329963
Guymager	3	245.449475	81.81649167	0.157430807
OsForensics	3	245.4193217	81.80644055	0.019385862
Magnet Acquire	3	243.987461	81.32915367	0.230122984
EnCase	3	246.2245568	82.07485227	0

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.016277351	4	0.254069338	2.796459735	0.085283508	3.478049691
Within Groups	0.908539231	10	0.090853923			
Total	1.924816582	14				

DD Disk 2, 50%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	241.5462	80.51541	0.014108
Guymager	3	246.6564	82.21881	0.000244
OSForensics	3	245.4459	81.81529	0.010262
Magnet Acquire	3	242.8762	80.95872	0.021288

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	5.454096	3	1.818032	158.4305	1.84E-07	4.066181
Within Groups	0.091802	8	0.011475			

Total	5.545898	11

Post-hoc table:

Groups	P-value	Significant?
FTK Imager – Guymager	0.00138	Yes
FTK Imager – OSForensics	0.000157	Yes
FTK Imager – Magnet Acquire	0.016361	No
Guymager – OSForensics	0.018441	No
Guymager – Magnet Acquire	0.004088	Yes
OSForensics – Magnet Acquire	0.001828	Yes

EWF_E01 SD-card, 100%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	282.6994	94.23314	0.001603
Guymager	3	281.8101	93.9367	0.454008
OSForensics	3	270.299	90.09966	0.150567
Magnet Acquire	3	195.9184	65.30612	0
EnCase	3	281.3989	93.79962	0.535353

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1877.324	4	469.3311	2055.708	1.58E-14	3.47805
Within Groups	2.283063	10	0.228306			
Total	1879.607	14				

Post-hoc table:

Groups	P-value	Significant?
FTK Imager – Guymager	0.25812574	No
FTK Imager – OSForensics	0.002685008	Yes
FTK Imager – Magnet Acquire	6.3875E-07	Yes
FTK Imager – EnCase	0.412708629	No
Guymager – OSForensics	0.002635392	Yes
Guymager – Magnet Acquire	0.00018457	Yes
Guymager – EnCase	0.823144007	No
OSForensics – Magnet Acquire	8.16354E-05	Yes
OSForensics – EnCase	0.004269706	Yes
Magnet Acquire - EnCase	0.000219728	Yes

DD, SD-card, 100%:

Summary

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	273.0983	91.03278	19.27609
Guymager	3	283.1163	94.37209	0.001613
OSForensics	3	271.6344	90.54481	0.017754
Magnet Acquire	3	194.628	64.876	0.0173

ANOVA

Source of variation	*SS*	*df*	*MS*	*F*	*p-value*	*F-crit*
Between groups	1679.341	3	559.7804	115.94	6.23E-07	4.066181
Within groups	38.62551	8	4.828189			

Total	1717.967	11

Post-hoc table:

Groups	P-value	Significant?
FTK Imager – Guymager	0.318386854	No
FTK Imager – OSForensics	0.865154842	No
FTK Imager – Magnet Acquire	0.009213094	Yes
Guymager – OSForensics	0.000141198	Yes
Guymager – Magnet Acquire	1.05634E-06	Yes
OSForensics – Magnet Acquire	1.8923E-09	Yes

EWF_E01 SD-card, 50%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	282.2155	94,07185	0,04455
Guymager	3	282.8382	94,27941	0,001608
OSForensics	3	269.1172	89,70574	0,950497
Magnet Acquire	3	195.7521	65.25069	0.00479
EnCase	3	279.2789	93.09295	3.398397

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1860.259	4	465.0647	528.5016	1.38E-11	3.47805
Within Groups	8.799685	10	0.879969			
Total	1869.059	14				

Post-hoc table:

Groups	P-value	Significant?
FTK Imager – Guymager	0.227821	No
FTK Imager – OSForensics	0.013119	No
FTK Imager – Magnet Acquire	2.69E-06	Yes
FTK Imager – EnCase	0.455177	No
Guymager – OSForensics	0.014689	No
Guymager – Magnet Acquire	2.84E-09	Yes
Guymager – EnCase	0.380948	No
OSForensics – Magnet Acquire	0.0005	Yes
OSForensics – EnCase	0.066151	No
Magnet Acquire - EnCase	0.001439	Yes

DD SD-card, 50%:

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
FTK Imager	3	280.0348	93.34495	0.722566
Guymager	3	280.2191	93.40638	2.933787
OSForensics	3	270.4876	90.16253	0.070091
Magnet Acquire	3	194.3755	64.79183	0.349195

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1723.799	3	574.5998	563.9359	1.21E-09	4.066181
Within Groups	8.151278	8	1.01891			
Total	1731.951	11				

Post-hoc table:

Groups	P-value	Significant?
FTK Imager – Guymager	0.959204	No
FTK Imager – OSForensics	0.016095	No
FTK Imager – Magnet Acquire	3.89E-06	Yes
Guymager – OSForensics	0.078415	No
Guymager – Magnet Acquire	0.000396	Yes
OSForensics – Magnet Acquire	1.51E-05	Yes