Low Cost And Ultra Low Cost Digital Forensic Imaging Devices

Prashant Mali
Cyber Law Consulting (Advocates and Attorneys)
A-902, Grenville Co-op

Abstract- *The purpose of this study is to explore the evolving technology and systems to find a low cost, efficient and portable solution for hard disk drive forensic imaging.Hard Disk Drive Imaging is one of the most frequently used forensic process which finds its application in both traditional as well as digital crimes and has found massive implementation in detecting cyber-crime incidents leading to cyber warfare. An empirical research was conducted using combination of hardware's like Intel NUC, Raspberry Pi 3 Model B, Custom Forensic Workstation (CFW), write blockers etc. and software's like ENCASE and FTK imager to do forensic imaging using multiple hard drives. A comparative analysis of the imaging process using same identical media over various platforms was done.The research shows that Raspberry Pi 3 Model B is a cost effective solution when a small device is to be imaged. Intel NUC with its i3 processor performs better than custom forensic work station with i7 processor when imaging using FTK Imager. The process of imaging involves many intricacies in order to prove the authenticity of evidence in a court of law. Problem in this regard arose when imaging was done using FTK on Linux and analyzed using ENCASE. The format generated on Linux and that recognized by ENCASE is different. The integrity of evidence is thus put to question. It was observed that not all components of each system are needed consecutively for the task of imaging. Consequently if a system is assembled with necessary components, it can help in further reducing the cost drastically.*

Keywords- forensics, hard disk drive imaging, digital crimes, cyber warfare, authenticity

I. INTRODUCTION

Forensic Analysis is a developing domain finding its ground in a nation like India. Today electronic evidence has more to divulge in the course of investigations than traditional evidence. However, proving the authenticity and integrity of this evidence in the court of law is a challenging process. Forensic analysis is a process requiring hefty tools. Currently the law enforcement is using tools like TD3 and FTK imager for imaging hard disks. The task force visiting a crime scene comprises of a dedicated forensic investigator whose only task is to collect digital evidence. The major set-back suffered by the team is the difficulty in portability of the forensic tools and devices. Moreover, the forensic acquisition and imaging tools today cost lakhs of rupees. This is the reason police force in limited areas only is equipped with such tools. The major motivation behind this research was to find a combination of hardware and software to perform hard disk imaging that is both light on pocket and allows easy mobility without compromising on efficiency. The advent of Single Board Computers (SBC) with ARM processors has made this possible to an extent. At the time of research, author came across other papers where a study has been conducted to test efficiency of imaging using SBCwith ARM Processors. This paper is a compilation of researchers own findings along with a comparative analysis with the paper, *"Low budget Forensics Drive Imaging Using ARM Based Single Board Computer."* [1]

Understanding SBC

Single Board Computers or SBC are computer systems designed on a single board of circuit which have revolutionized the digital world. A single board computer contains the microprocessor, storage and memory, as well as other necessary components, in a single circuit board.[i] Over the years the SBC have become more sophisticated with their intricately designed circuits thus reducing their over-all costs. SBC while offering the usual functionality such as USB ports, Ethernet, on board support for disk drives etc., have certain limitations when compared to a conventional system. Some of the well-known SBC available in the market right now are Raspberry Pi, Orange Pi, and Odroid etc.

Why DCFLDD over DC3DD

The US Department of Homeland Security in its report of testing dcdldd command states,

"DCFLDD is an enhanced version of GNU dd with features useful for forensics and security. Based on the dd program found in the GNU Coreutils package, dcfldd has the following additional features: hashing on-the-fly, status output, flexible disk wipes, image/wipe verify, multiple outputs, split output

and piped output and logs. DCFLDD was tested only for its disk imaging capabilities and, except for the following anomaly the tool acquired the test media completely and accurately.

i. When a drive with faulty sectors was imaged the tool failed to completely acquire all readable sectors near the location of the faulty sectors. Readable sectors that were near faulty sectors on the source drive were not acquired. The tool wrote zeros to the target drive in place of these sectors.
ii. When a drive with faulty sectors was imaged the data cloned to the target drive became misaligned after faulty sectors were encountered on the source drive. The size of the offset or misalignment between the data on the source and target drives grew as more faulty sectors were encountered on the source."[2]

Irrespective of above stated drawbacks, DCFLDD supports more hashing algorithms than dc3dd which allows the user greater control over how hashes are displayed. This enables us to expand the scope of authentication which is a mandate when producing an image as evidence in the court of law.

1.3 Difference between DD and E01 Format

The process of imaging hard drive yields result in two format, DD and E01. An elementary question before everyone is, which format one should prefer. Thus understanding the difference between two is of paramount importance. Both E01 and DD are formats of images created on bit to bit copy of hard disk drive. E01 format has primarily got two advantages over DD format, firstly, its ability to create a compressed image of the disk; secondly, it also gives a metadata of the image. DD on other hand is a raw disk image, which is an exact copy of the original disk occupying same or more space and giving no metadata along. The DME Forensics Blog [2] shows via an experiment that this should not be the sole reason why one should go for E01. Experiments show that on imaging using AccessData's FTK Imager an entirely located 500 GB 7200 RPM Western Digital SATA hard drive in an un-segmented E01 format using the default compression setting ("6"), the process took about 1 hour and 27 minutes. This resulting image file was approximately 434 GB and 7% compressed, thus saving about 32 GB. When the same was done in a DD format the process took approximately 1 hour 24 minutes. There is no substantial difference in time taken for imaging. Nevertheless, when an attempt was made to search an ASCII value in both format, the E01 format took 1 hour 53 minutes while the DD format took 1 hour 6 minutes.

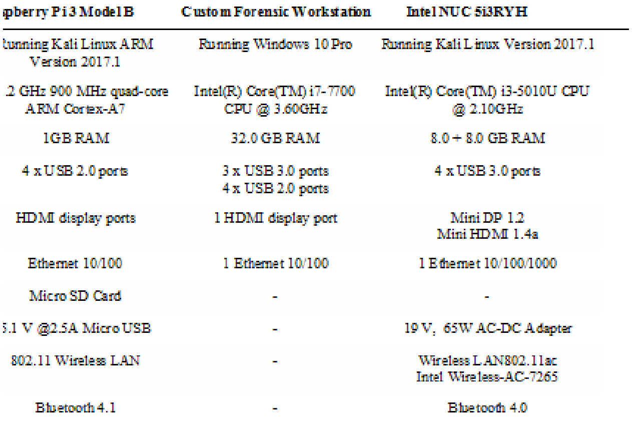
Thus the choice of format depends on what one wants to do after the imaging process. ENCASE reads E01 format. Thus if one wishes to analyze the image using ENCASE or perform several searches on it, E01 is the preferred format. The format created by Linux is DD which cannot be verified in ENCASE. In case one wishes to investigate images using standard Linux tools or third party tools, they may prefer DD format. This is not an efficient process in case when image created is large.

II. LITERATURE SURVEY

2.1 Hardware Requirement

To make the process of imaging light and portable the author has used SBC with ARM Processor. For the research, Raspberry Pi 3 is used, Model B is the latest and cheapest Single Board Computer (SBC) as of date. Apart from that, Intel NUC 5i3RYH and a Custom Forensic Workstation (CFW) hasbeen compiled in research lab. The NUC came with an inbuilt 8GB RAM. Additional 8GB RAM is attached to it so as to improvise its performance. Analysis of the speed of imaging hard disk was then performed on different systems (Table 1).

Table 1. Hardware specifications



pberry Pi 3 Model B	Custom Forensic Workstation	Intel NUC 5i3RYH
Running Kali Linux ARM Version 2017.1	Running Windows 10 Pro	Running Kali Linux Version 2017.1
.2 GHz 900 MHz quad-core ARM Cortex-A7	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz	Intel(R) Core(TM) i3-5010U CPU @ 2.10GHz
1GB RAM	32.0 GB RAM	8.0 + 8.0 GB RAM
4 x USB 2.0 ports	3 x USB 3.0 ports 4 x USB 2.0 ports	4 x USB 3.0 ports
HDMI display ports	1 HDMI display port	Mini DP 1.2 Mini HDMI 1.4a
Ethernet 10/100	1 Ethernet 10/100	1 Ethernet 10/100/1000
Micro SD Card	-	-
5.1 V @2.5A Micro USB	-	19 V, 65W AC-DC Adapter
802.11 Wireless LAN	-	Wireless LAN802.11ac Intel Wireless-AC-7265
Bluetooth 4.1	-	Bluetooth 4.0

Additional accessories used in the process were as follows:

Write Blocker: CoolGear USB 3.0 Hardware Write Blocker with IDE/SATA adapters, hardware write block switches and external power supply

Pendrives: 8 GB Toshiba PenDrive, 32 GB Sandisk Pen Drive

Hard Disks: 320 GB 3.5" SATA III Seagate Hard disk, 500 GB 3.5" SATA III Western Digital Hard disk

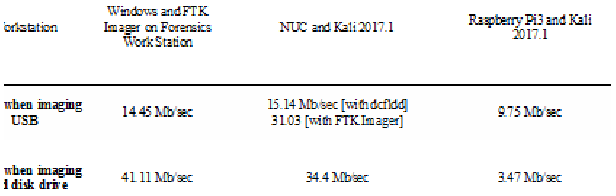
2.2 Software Requirements

The CFW was used to run Windows 10 Pro and FTK Imager. FTK Imager 3.2.0 was downloaded from Access Data’s website [2]. FTK Imager offers a user friendly interface and creates an image of the disk in e01 format and also generates a hash (md5 and SHA1) of the disk. Encase version 8.05 was used for the analysis of disk images. The hash generated by the FTK imager is verified by Encase which helps ensure integrity of the entire process.Kali Linux Version 2017.1 (ARM version) [2] was downloaded from website of offensive security for running on Raspberry Pi 3 Model B while Kali Linux Version 2017[2] was downloaded for Intel NUC. For both the systems, the Source was a 320 GB 3.5” SATA III Seagate Hard Disk and destination was 500 GB 3.5” SATA III Western Digital Hard Disk. The hard disks were connected via Cool Gear Write Blocker to USB 2.0 in the case of Raspberry Pi3 and USB 3.0 in the case of Intel NUC(Appendix A Figures 3 and 5)(Table 3).

III. RESULTS AND DISCUSSION

Speed of imaging a 320 GB hard disk onto a 500 GB Hard Disk with configurations as stated above on different workstations was as follows (Appendix A, Table 3 and Figure 4):

Table 2. Imaging speed over various platform



orkstation	Windows and FTK Imager on Forensics Work Station	NUC and Kali 2017.1	Raspberry Pi3 and Kali 2017.1
when imaging USB	14.45 Mb/sec	15.14 Mb/sec [with dcfldd] 31.03 [with FTK Imager]	9.75 Mb/sec
when imaging l disk drive	41.11 Mb/sec	34.4 Mb/sec	3.47 Mb/sec

3.1 Comparative Analysis of Performance

Analysis of the experiment showed that when similar storage media is used for the process of imaging over various platforms, the custom workstation processed at a speed of 41.06 Mb/sec while the NUC with its i3 processor was not far behind at 34.4 Mb/sec. However, the Raspberry Pi3, which was the major focus of the research processed at a speed of 3.47 Mb/sec, which is approximately 10 times slower than NUC and 12 times slower than the custom work station.In of the leading paper by Olson and Shashidhar (2016), similar research was carried on by imaging USB drive to another attached USB drive using Raspberry Pi 2, Odroid XU4 and Windows Laptop (Intel (R) Core i5-4200U CPU @ 1.60 GHz 2.30 GHz, 6 GB RAM, 500 GB SATA II hard drive, Windows 10 64 bit, 1 x USB 3.0 and 2 x USB 2.0 ports). The Raspberry Pi barely passed speeds of 10 Mb/sec and slowed to speed of 1.5 Mb/sec. The Odroid XU4 occasionally reached 20 Mb/sec but then slowed down to 10 Mb/sec while the windows laptop went up to 60 Mb/sec also. In the current study, when a USB drive was imaged to another attached USB drive, the average speed over Raspberry Pi 3 Model B was 9.75 Mb/sec. which is way more than what was observed by Olson and Shashidhar using Raspberry Pi 2 which went as low as 1.5 Mb/sec. The average speed on our CFW setup was 14.45Mb/sec. The same experiment on NUC gave a speed of 15.14 Mb/sec which to my surprise even surpasses the CFW despite its i3 processor compared to latters i7 processor.

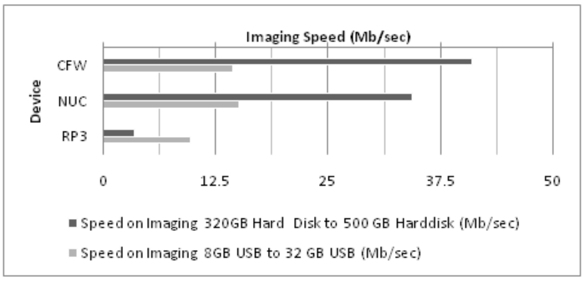


Figure 1. Bar graph showing imaging speed

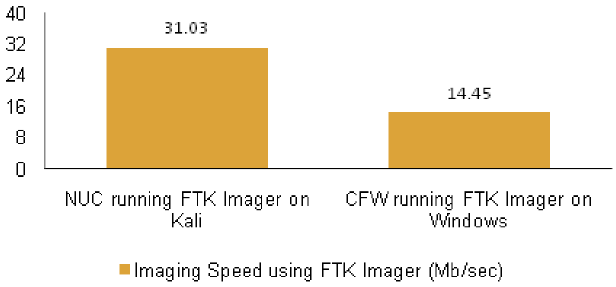


Figure 2. Difference in imaging speed using FTK Imager over NUC and custom forensic workstation

3.2 Comparative Analysis of Price

The Kali for ARM Processor is available free of cost. So the total price of the entire setup is Rs. 2864. Kali and FTK Imager is also available free of cost for NUC running i3 processor, which can be easily downloaded from offensive security and Access Data’s website respectively (Appendix A Tables 4 and 5)

The customized forensic work station cost approximately **Rs.1, 10, 000,**which by default puts it out of the low budget bracket. The only reason why it was made a part of the research was to collate and compare the efficiency with other devices.

IV. CONCLUSION

The series of experiments performed and observations made during research help me culminate that when looking for an ultra-low cost setup Raspberry Pi 3 Model is a go to one if the device to be imaged is not a heavy storage device. Raspberry Pi 3 is not far behind NUC or Windows in this scenario and is a perfect solution when only DD image is needed. Organizations in such scheme can make their SOP circumscribing DD, justifying its use. Subsequent conversion of DD to E01 does not work out owing to the enormous time of conversion, which is more than the imaging time and hash which cannot be verified. However, when price is not such an issue, one should definitely choose NUC which is affordable and whose result are way better than Raspberry Pi 3. The Kali OS for ARM and otherwise and FTK Imager is available free of cost. To my surprise, the performance of NUC with i3 processor and 16 GB RAM, surpassed the CFW with i7 processor and 32 GB RAM. NUC with Kali Linux 2017.1 and FTK imager gave unparalleled speed of 31.03 Mb/sec. Moreover, NUC is equally portable, reliable and way more efficient irrespective of the size of storage media to be imaged. Thus it would not be inappropriate to conclude that while SBC continue to augment, NUC has stupendous scope in the future of forensics.

REFERENCES

[1] Olson E, Shashidhar N. Low Budget Forensic Drive Imaging Using Arm Based Single Board Computers. Journal of Digital Forensics, Security and Law [Internet]. 2016, 11(1).

[2] What is a single board computer, single board computers? http://www.futureelectronics.com/en/display-solutions/single-board-computer.aspx. Date accessed: 28/06/2017.

[3] NIST & US Department of Homeland Security. Test Results for Digital Data Acquisition Tool: DCFLDD 1.3.4-1. Homeland Security: Science and Technology: USA, 2013.

[4] Forensic Images for DVR Analysis - E01 or DD. http://info.dmeforensics.com/blog/forensic-images-for-dvr-analysis-e01-or-dd/. Date accessed: 27/06/2017.

[5] Product Downloads: Forensic Tool Kit. http://www.accessdata.com/product-download. Date accessed: 27/06/2017.

[6] Kali Linux ARM Images. https://www.offensive-security.com/kali-linux-arm-images/. Date accessed: 27/06/2017.

[7] Kali Linux Downloads. Available from: https://www.kali.org/downloads/ Date accessed: 27/06/2017.

[8] Digital Forensics Tutorials – Acquiring an Image with Kali dcfldd. http://nest.unm.edu/files/2713/9251/5584/Tutorial_5_-_Kali_-_dcfldd_Imaging.pdf. Date accessed: 28/06/2017.

[9] Morra S. Confirming the Integrity and Utility of Open Source Forensic Tools. *Utica College, USA*, 2013, pp. 34-40.

[10] Anvar P. K. vs. P.K Basheer &Ors. 10SCC 473. 2014.

[11] Acquiring Data with dd, dcfldd, dc3dd. http://www.cyber-forensics.ch/acquiring-data-with-dd-dcfldd-dc3dd/. Date accessed: 28/06/2017.

[12] RASPBERRY PI 3 MODEL B INBULT BLUETOOTH AND Wifi: Amazon.in: Computers & Accessories. http://www.amazon.in/RASPBERRY-MODEL-INBULT-BLUETOOTH-Wifi/dp/B01G882L3G/ref=sr_1_4?s=computers&ie=UTF8&qid=1498653505&sr=1-4&keywords=raspberry+pi+3+model+b.Dateaccessed: 28/06/2017.

[13] REES52 PI3 Raspberry Pi 2 and 3 Model B/B + Abs Transparent Modular Case. http://www.amazon.in/REES52-Raspberry-Model-Transparent Modular/dp/B01N6AE48Y/ref=sr_1_6?ie=UTF8&qid=1498647674&sr=8-6&keywords=raspberry+pi3+model+B. Date accessed: 28/06/2017.

[14] Buy Segolike 3.5 inch Touch Screen Monitor With Touch Pen For Raspberry Pi 3 Model B Online at Low Prices in India. http://www.amazon.in/Segolike-Touch-Screen-Monitor Raspberry/dp/B071J3R3M5/ref=sr_1_2?s=computers&ie=UTF8&qid=1498649997&sr=1-2&keywords=raspberry+pi+3+model+b+display. Date accessed: 28/06/2017.

[15] ePro Labs Raspberry Pi 3 Model B Price in India. https://www.flipkart.com/epro-labs-raspberry-pi-3-model b/p/itmejquwfunx6hhz?pid=ETYEJQUWMNH5VMRT&srno=s_1_1&otracker=search&lid=LSTETYEJQUWMNH5VMRTTIZP7O&qH=d216d7d596dfa2bb. Date accessed: 28/06/2017.

[16] SB COMPONENTS Clear Closed Case for Raspberry Pi Model B+ Price in India. https://www.flipkart.com/sb-components-clear-closed-case-raspberry-pi-model-b/p/itmep3buckgfkrtw?pid=ETYEP3BUBUXSMTA9&srno=s_1_2&otracker=search&lid=LSTETYEP3BUBUXSMTA9RIS9Y0&qH=9079060d4b8e9f18. Date accessed: 28/06/2017.

[17] Raspberry Pi 3 Model B 64-bit Quad core 1.2 GHz ARM CPU with WiFi and Bluetooth. http://www.ebay.in/itm/Raspberry-Pi-3-Model-B-64-bit-Quad-core-1-2-GHz-ARM-CPU-with-WiFi-and-Bluetooth-

/122463763202?hash=item1c8368bb02:g:rBsAAOSwtZJY~0rG. Date accessed: 28/06/2017.

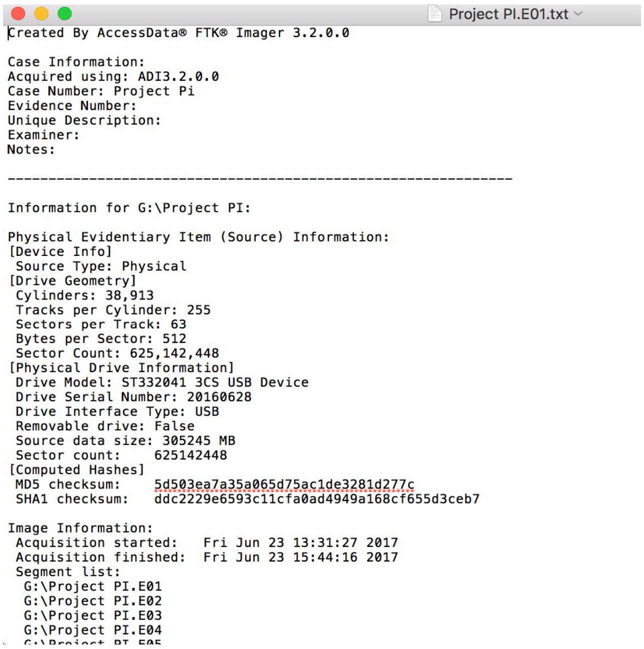
[18] Intel BOXNUC5i3RYH Next Unit of Computing Kit. http://www.amazon.in/Intel-BOXNUC5i3RYH-Next-Unit-Computing/dp/B00S1ISFOQ/ref=sr_1_fkmr0_3?s=computers&ie=UTF8&qid=1498649305&sr=1-3-fkmr0&keywords=Intel+NUC+5i3RYH. Date accessed: 28/06/2017.

[19] HyperX FURY Memory - 8GB Module - DDR3 1866MHz CL10 DIMM. http://www.amazon.in/HyperX-FURY-Memory-Module-1866MHz/dp/B00J8E91UO/ref=sr_1_fkmr0_2?ie=UTF8&qid=1499244468&sr=8-2-fkmr0&keywords=8GB+Kingston+HyperX+Fury+DDR4+2133+Mhz+Desktop+Pc+Ram+%2B+BILL. Date accessed: 05/07/2017.

[20] Intel NUC Kit NUC5i3RYH 5th Gen Core i 3 5010u /GigE- WLAN +BT 4.0 (Barebone PC). http://www.ebay.in/itm/Intel-NUC-Kit-NUC5i3RYH-5th-Gen-Core-i-3-5010u-GigE-WLAN-BT-4-0-Barebone-PC-/152520369756?_trksid=p2059707.m48543.l9013. Date accessed: 05/07/2017.

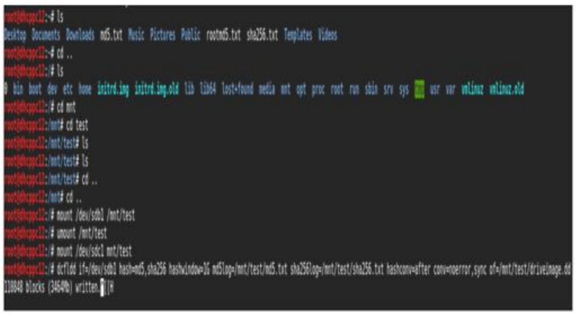
[21] 8GB Kingston HyperX Fury DDR4 2133 Mhz Desktop Pc Ram. http://www.ebay.in/itm/8GB-Kingston-HyperX-Fury-DDR4-2133-Mhz-Desktop-Pc-Ram-BILL-/232014877154?hash=item36052a11e2:g:czwAAOSwGtNXifcC. Date accessed: 05/07/2017.

Appendix A



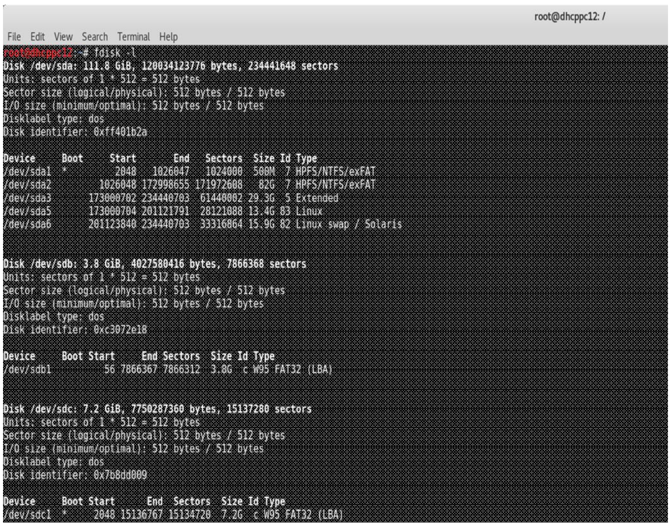
```
Project PI.E01.txt
Created By AccessData® FTK® Imager 3.2.0.0

Case Information:
Acquired using: ADI3.2.0.0
Case Number: Project Pi
Evidence Number:
Unique Description:
Examiner:
Notes:

----------------------------------------------------------------

Information for G:\Project PI:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 38,913
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 625,142,448
[Physical Drive Information]
 Drive Model: ST332041 3CS USB Device
 Drive Serial Number: 20160628
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 305245 MB
 Sector count:    625142448
[Computed Hashes]
 MD5 checksum:    5d503ea7a35a065d75ac1de3281d277c
 SHA1 checksum:   ddc2229e6593c11cfa0ad4949a168cf655d3ceb7

Image Information:
 Acquisition started:   Fri Jun 23 13:31:27 2017
 Acquisition finished:  Fri Jun 23 15:44:16 2017
 Segment list:
  G:\Project PI.E01
  G:\Project PI.E02
  G:\Project PI.E03
  G:\Project PI.E04
  G:\Project PI.E05
```

Figure 3. Log file generated by FTK imager



```
root@dhcppc12:~# ls
Desktop  Documents  Downloads  md5.txt  Music  Pictures  Public  rootmd5.txt  sha256.txt  Templates  Videos
root@dhcppc12:~# cd ..
root@dhcppc12:/# ls
0  bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
root@dhcppc12:/# cd mnt
root@dhcppc12:/mnt# cd test
root@dhcppc12:/mnt/test# ls
root@dhcppc12:/mnt/test# ls
root@dhcppc12:/mnt/test# cd ..
root@dhcppc12:/mnt# cd ..
root@dhcppc12:/# mount /dev/sdb1 /mnt/test
root@dhcppc12:/# umount /mnt/test
root@dhcppc12:/# mount /dev/sdc1 mnt/test
root@dhcppc12:/# dcfldd if=/dev/sdb1 hash=md5,sha256 hashwindow=1G md5log=/mnt/test/md5.txt sha256log=/mnt/test/sha256.txt hashconv=after conv=noerror,sync of=/mnt/test/driveimage.dd
110848 blocks (3464Mb) written.
```

Figure 4. Imaging process has started



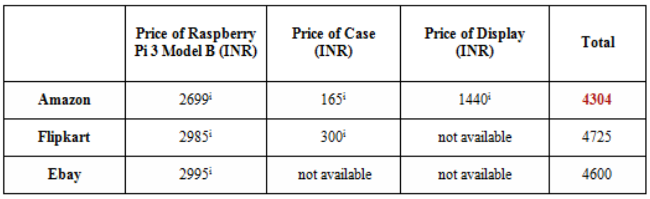
```
root@dhcppc12: /
File  Edit  View  Search  Terminal  Help
root@dhcppc12:~# fdisk -l
Disk /dev/sda: 111.8 GiB, 120034123776 bytes, 234441648 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xff401b2a

Device     Boot     Start       End   Sectors  Size Id Type
/dev/sda1  *         2048   1026047   1024000  500M  7 HPFS/NTFS/exFAT
/dev/sda2         1026048 172998655 171972608   82G  7 HPFS/NTFS/exFAT
/dev/sda3       173000702 234440703  61440002 29.3G  5 Extended
/dev/sda5       173000704 201121791  28121088 13.4G 83 Linux
/dev/sda6       201123840 234440703  33316864 15.9G 82 Linux swap / Solaris


Disk /dev/sdb: 3.8 GiB, 4027580416 bytes, 7866368 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc3072e18

Device     Boot Start     End Sectors  Size Id Type
/dev/sdb1          56 7866367 7866312  3.8G  c W95 FAT32 (LBA)


Disk /dev/sdc: 7.2 GiB, 7750287360 bytes, 15137280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x7b8dd009

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdc1  *     2048 15136767 15134720  7.2G  c W95 FAT32 (LBA)
```

Figure 5. Output for fdisk –l

Table 3. Table of parameters[i]

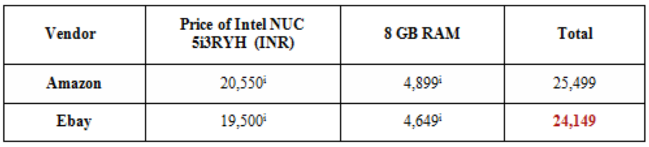
if	source file
/dev/sdb	source /suspect drive (whole disk)
Hash	Definition of hash algorithms
Hashwindows	Will hash data chunks of 1 GB
md5log	Saves all md5 hashes in a file called md5.txt
shc56log	Saves all sha hashes in a file called sha256.txt
Hashconv	Hashing AFTER or BEFORE the conversion
Conv	conversion
Noerror	will continue even with read errors
Sync	if there is an error, NULL fill the rest of the block
Of	destination file

Table 4. Comparison of price for setting up raspberry pi 3 workstation



	Price of Raspberry Pi 3 Model B (INR)	Price of Case (INR)	Price of Display (INR)	Total
Amazon	2699[i]	165[i]	1440[i]	4304
Flipkart	2985[i]	300[i]	not available	4725
Ebay	2995[i]	not available	not available	4600

Table 5. Comparison of price for setting up NUC workstation



Vendor	Price of Intel NUC 5i3RYH (INR)	8 GB RAM	Total
Amazon	20,550[i]	4,899[i]	25,499
Ebay	19,500[i]	4,649[i]	24,149