**PROJECT REPORT**

**1.Case Project 3-6**

Your supervisor has asked you to list the acquisition tools available on a forensic Linux Live

CD. Download the current ISO version of Deft (www.deftlinux.net), CAINE (www.caine-live.net),

Kali Linux (www.kali.org), or Penguin Sleuth (www.linux-forensics.com), and then create a

bootable CD or DVD of it. Start it on your workstation and survey its tools. Then write a oneto

two-page report containing a brief description of each acquisition utility on the CD or DVD.

Description

**Bulk Extractor** is a computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. The results can be easily inspected, parsed, or processed with automated tools. **Bulk Extractor** also created a histograms of features that it finds, as features that are more common tend to be more important. The program can be used for law enforcement, defense, intelligence, and cyber-investigation applications.

Bulk extractor tool extracts credit card numbers, URL links, email addresses, which are used as digital evidence. This tool lets you identify malware and intrusion attacks, identity investigations, cyber vulnerabilities, and password cracking. The specialty of this tool is that not only does it work with normal data, but it also works on compressed data and incomplete or damaged data.

It is distinguished from other forensic tools by its speed and thoroughness. Because it ignores file system structure, bulk\_extractor can process different parts of the disk in parallel. In practice, the program splits the disk up into 16MiByte pages and processes one page on each available core. This means that 24-core machines process a disk roughly 24 times faster than a 1-core machine. bulk\_extractor is also thorough. That’s because bulk\_extractor automatically detects, decompresses, and recursively re-processes compressed data that is compressed with a variety of algorithms. Our testing has shown that there is a significant amount of compressed data in the unallocated regions of file systems that is missed by most forensic tools that are commonly in use today.

Another advantage of ignoring file systems is that bulk\_extractor can be used to process any digital media. We have used the program to process hard drives, SSDs, optical media, camera cards, cell phones, network packet dumps, and other kinds of digital information.

**HashDeep tool:**

The hash deep tool is a modi ed version of the dc3dd hashing tool designed especially for digital forensics. This tool includes auto hashing of les, i.e., sha-1, sha-256, and 512, tiger, whirlpool, and md5. An error log le is auto written. Progress reports are generated with every output.

**Magic rescue tool:**

Magic rescue is a forensic tool that performs scanning operations on a blocked device. This tool uses magic bytes to extract all the known le types from the device. This opens devices for scanning and reading the le types and shows the possibility of recovering les deleted or corrupted partition. It can work with every le system.

**Scalpel tool:**

This forensic tool carves all the les and indexes those applications which run on Linux and windows. The scalpel tool supports multithreading execution on multiple core systems, which help in quick executions.

File carving is performed in fragments such as regular expressions or binary strings.

**Scrounge-NTFS tool:**

This forensic utility helps in retrieving data from corrupted NTFS disks or partitions. It rescues data from a corrupted le system to a new working le system.

**Guymager tool:**

This forensic utility is used to acquire media for forensic imagery and has a graphical user interface. Due to its multi-threaded data processing and compression, it is a very fast tool. This tool also supports cloning. It generates at, AFF, and EWF images. The UI is very easy to use.

**Pd d tool:**

This forensic tool is used in pdf les. The tool scans pdf les for speci c keywords, which allows you to identify executable codes when opened. This tool solves the basic problems associated with pdf les. The suspicious les are then analyzed with the pdf-parser tool.

**Pdf-parser tool:**

This tool is one of the most important forensic tools for pdf les. pdf-parser parses a pdf document and distinguishes the important elements utilized during its analysis, and this tool does not render that pdf document.

**Peepdf tool:**

A python tool that explores pdf documents to nd whether it is harmless or destructive. It provides all the elements needed to perform pdf analysis in one single package. It shows suspicious entities and supports various encodings and lters. It can parse encrypted documents too.

**Autopsy tool:**

An autopsy is all one forensic utility for fast data recovery and hash ltering. This tool carves deleted les and media from unallocated space using PhotoRec. It can also extract EXIF extension multimedia. Autopsy scans for compromise indicator using STIX library. It is available in the command line as well as GUI interface.

**img\_cat tool:**

img\_cat tool gives the output content of an image le. The image les recovered will have meta-data and embedded data, which allows you to convert them into raw data. This raw data helps in piping the output to calculate the MD5 hash.

**ICAT tool:**

ICAT is a Sleuth Kit tool (TSK) that creates an output of a le based on its identi er or inode number. This forensic tool is ultra-fast, and it opens the named le images and copies it to standard output with a speci c inode number. An inode is one of the data structures of the Linux system which stores data and information about a Linux le such as ownership, le size, and type, write and read permissions.

**Srch\_strings tool:**

This tool looks for viable ASCII and Unicode strings inside binary data and then prints the offset string found in that data. srch\_strings tool will extract and retrieve the strings present in a le and gives offset byte if called upon.

**2.Case Project 3-2**

At a murder scene, you have started making an image of a computer’s drive. You’re in the

back bedroom of the house, and a small fire has started in the kitchen. If the fire can’t be

extinguished, you have only a few minutes to acquire data from a 10 GB hard disk. Write one

to two pages outlining your options for preserving the data.

**Case Description**

A person is murdered while he was in the back room in his home. When it is informed to the investigating agency and they reach to the crime scene the house gets caught by the fire. The fire is such as it cannot be extinguished.

Now, the investigator has only some time to acquire the data which is 10GB in size and stored in the system at the crime place. There are many techniques that are used by the criminals so that they can get the data before the fire spread throughout the house.

**Methods of data acquisition**

Data acquisition means acquiring the data from the place of crime to solve the case. Data acquisition has two types static and live acquisition. For the cases in which there is less time for the acquisition of the data the static acquisition is used.

As in the case the investigator gets less time because of the fire which is not possible to extinguish. Static acquisition is the one of the type of data acquisition in this case. Static acquisitions primary objective is to preserve the data evidences which can be used further for the purpose of future investigation.

Many time investigators get only one chance to make the copy or image of the disk. So like in this case the investigator get a very less time for the acquisition of the data. Static acquisition is very much used in the digital evidences in these types of cases the data once gone never get the second chance to recover it.

While solving the case the investigator keeps all the protective measures to save the evidences which will prove the crime in the court. In storage of evidences plans are made so that the evidences doesn’t get destroyed or contaminated. Most of the investigator doesn’t make the duplicate copy of the image files because of the less time.

For the acquisition various types of tools can be used because different forensic company has developed different acquisition tools like ProDiscover, EnCase, FTK Imager, etc.

1. **FTK:** FTK imager is a windows program for data gathering which includes the copy of AccessData Forensic toolkit with license.

FTK is designed for viewing evidences and the disks and disk-to-image files are generated from other proprietary formats of files.

This program gives a view of a disk partition or an image files as through its mounted partition.

2. **EnCase:** EnCase is the software which is used for the remote acquisition. It is developed by

Guidance software which developed the first remote acquisition forensic tool. It comes with lots of capabilities like:

1. It can get the data at the remote location from the media or the RAM of any computer.
2. It has an option for creating the data from many systems.
3. Preview of the system for the decision of the further action.
4. RAID support both for hardware and software.
5. It supports a many types of formats of files such as: NTFS, FAT, FFS, LVM8, DVD, Palm, UDFand many more.
6. In integration with the tools of intrusion detection system (IDS) to make the replica of facts ofintrusion to an investigation workstation automatically further testing over the concerned network.

3. **ProDiscover:** ProDiscover is the software which is developed for the purpose of remote access of data. It is developed in two versions which are as:

1. ProDiscover Investigator
2. ProDiscover incident Response.

As the ProDiscover software connects to the computer at remote location, both the tools perform the same process for the acquisition. ProDiscover investigator is designed to capture data from the computer of suspected people while the user operating it, it is a live acquisition.

For the access of data at the remote location the ProDiscover utility is works as the PDServer agent. The PDServer must be enhanced on the suspect’s computer before ProDiscover incident response and ProDiscover investigator can use it.

ProDiscover Investigator encrypts the link between the examiner and suspect’s computer using the 256-bit advance encryption standard. All the communication between the PDServer and investigator computer are encrypted. In this case ProDiacover Basic is used.

**Procedure of acquiring the data using ProDiscover**

ProDiscover is the tool developed by the Technology Pathways and its latest version is 7.04 this tools have worked as to convert a raw image of a disk into a bootable VMware Machine.

This software makes the image of the suspect’s file. ProDiscover automates the many acquisition function. The size of the USB drives is typically smaller than the disks so it can contain without segmentation.

Before acquiring the data from the suspect drive with ProDiscover Basic, always use a hardware write-blocker device or write-protection method for USB-connected drives. ProDiscover creates

the image file with .eve extension. A log file contains a list of errors that occurred at the time of gathering of data. It also contains a unique file for the inventory that gives the information about the segmented volumes to the ProDiscover.

ProDiscover makes four files. Two of them are the parts of the spited image of the disk of suspected person and third is the log file and the next one is .psd file. A larger drive would have more than two segmented volumes. The extension of the segmented volumes is .eve and for other volumes the extensions are suffix –Split1, –Split2, –Split3, and so on with the .eve extension file.

During the extraction of the files it may be possible that the data get altered to solve this problem hardware write-blocker device is used with the ProDiscover. At last the hash value is extracted using the hashing algorithm then the file is examined and at last when the evidences are shown into the court hash value is matched. If same the data is not altered.

Case Project 3-3

You need to acquire an image of a disk on a computer that can’t be removed from the scene,

and you discover that it’s a Linux computer. What are your options for acquiring the image?

Write a brief paper specifying the hardware and software you would use.

Simply turning on the machine can already alter/destroy data that can be potential evidence, let alone booting its original OS.

The best solution is to remove the hard drive, connect it to another computer through a [hardware write blocker](http://www.forensicswiki.org/wiki/Write_Blockers) and then grab a complete image of it with dd or some equivalent. The write blocker is necessary to prevent accidental write to the device that may alter potential evidence (although a basic Linux installation that doesn't mount drives automatically won't do any writes by itself, Mac OS and Windows will definitely do).

If that's not possibly then you need to go with the forensics Live-CD route, but since it involves booting the computer you may already trigger some firmware-embedded code designed to alter/destroy potential evidence (hard but not impossible to do, it depends on what kind of criminal you're after).

Note that in the end, it doesn't matter what OS was installed on the computer since you shouldn't boot that OS anyway, and a bit-by-bit copy doesn't care about the data or even the filesystem that's on the drive (you can copy encrypted drives, but that won't help you much if you don't have the key since the copy is still encrypted)

3.Case Project 3-4

A bank has hired your firm to investigate employee fraud. The bank uses four 20 TB

machines on a LAN. You’re permitted to talk to the network administrator, who is familiar

with where the data is stored. What diplomatic strategies should you use? Which acquisition

method should you use? Write a two-page report outlining the problems you expect to

encounter, explaining how to rectify them, and describing your solution. Be sure to address

any customer privacy issues.

3.1. Data Acquisition:

Data acquisition means acquiring the data from the place of crime to solve the case. In the computer forensics tool evidences are stored as the image file one of three formats. Out of three formats two are open source and third is proprietary.Proprietary format was different because each vendor have different unique feature. Data acquisition takes place in four methods:

1. Create disk to image file.
2. Creating disk-to-disk copy.
3. Creating logical disk to disk or disk-to-data file.
4. Creating a sparse copy of a folder or file.

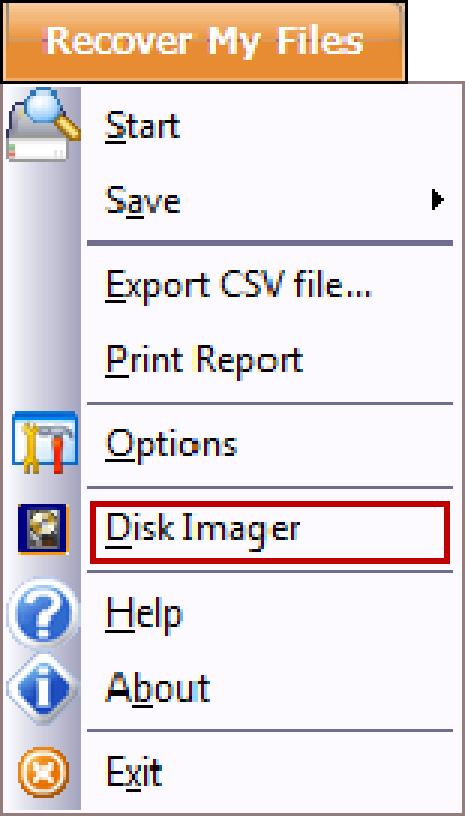
Disk imaging

Included in the Recover My Files installation folder is the stand alone drive imaging program “Forensic Imager”. Forensic Imager is a Windows based program that will acquire a sector copy (“image”) of a drive into one of the following common forensic file formats:

* DD /RAW (Linux “Drive Dump”)
* AFF (Advanced Forensic Format)
* E01 (EnCase) [Version 6.xx format]

3.2. Running Forensic Imager

Forensic Image is run from the Recover My Files drop down menu by selecting the “Disk Image” option:



Or by selecting the Disk Imager shortcut from the “Windows Start > All Programs > Recover My Files v5 > Disk Imager” shortcut.

When Forensic Imager is run the wizard presents 3 options:

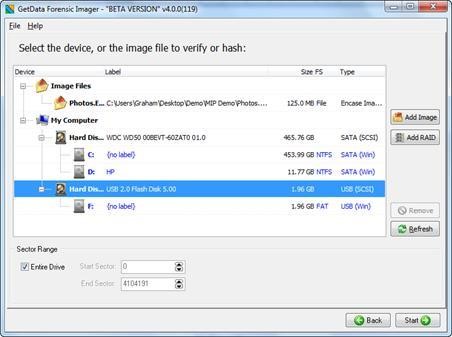
Acquire: The acquire option is used to take a forensic image (an exact copy) of the target media into an image file on the investigators workstation;

Convert: The convert option is used to copy an existing image file from one image format to another, e.g. DD to E01;

Hash or verify: The hash or verify option is used to calculate a hash value for a device or an existing image file.

When the “Acquire”, “Convert” or “Hash or Verify” button is selected, the source selection screen is displayed enabling selection of the source media:

1. When “Acquire” is selected, the source window shows the available physical devices (hard drives, USB drives, camera cards, etc.) and logical devices (partitions or volumes on the physical devices, e.g. "C:" drive) attached to the forensic workstation.
2. When “Convert” is selected, the source window allows the selection of the source image file. Click the “Add Image” button to add the required image file to the selection list.
3. When the “Hash or Verify” button is selected, the source window allows the selection of either a physical or logical drive, or an image file.



Label:

Physical drives are listed with their Windows device number. Logical drives display the drive label (if no label is present then "{no label}" is used). Image files show the path to the image.

Size:

The size column contains the size of the physical or logical device, or the size of the image file. Note that the actual size of the drive is usually smaller than what the drive is labeled. Drive manufactures usually round up the drive capacity, so a 2 GB drive in this screen may be sold as 2 GB+.

FS:

The File-system on the drive, e.g. FAT, NTFS or HFS; Type:

Describes the way in which the drive is connected to the computer. An image file will show the type of image (e.g. EnCase or RAW).

Copy a Disk to a Disk

The Copy Disk to Disk Wizard steps you through the process of transferring data from one disk or partition to another with an option to resize partitions. Essentially it is like creating a disk image of one partition or a whole disk and subsequently restoring it to another disk or partition except there is no intermittent image created.

You may use the Copy Disk to Disk Wizard to make a copy of the same configuration from one hard drive onto multiple other hard drives. For example, you may duplicate a hard drive configuration over several workstations on a network. If you are trying to recover data from a damaged hard drive or partition, you may clone the damaged partition to a number of other hard drives in order to experiment with different data recovery techniques on the copy rather than on the original.

To open the Copy Disk to Disk Wizard, do one of the following:

* In the main program window, double-click Copy Disk to Disk.
* From the Tools menu, choose Copy Disk to Disk

A logical disk, logical volume or virtual disk (VD or vdisk for short) is a virtual device that provides an area of usable storage capacity on one or more physical disk drives in a computersystem. The disk is described as logical or virtual because it does not actually exist as a single physical entity in its own right. The goal of the logical disk is to provide computer software with what seems a contiguous storage area, sparing them the burden of dealing with the intricacies of storing files on multiple physical units. Most modern operating systems provide some form of logical volume management.

A sparse file is a type of computer file that attempts to use file system space more efficiently when the file itself is mostly empty.

This is achieved by writing brief information (metadata) representing the empty blocks to disk instead of the actual "empty" space which makes up the block, using less disk space. The full block size is written to disk as the actual size only when the block contains "real" (non-empty) data. Sparse file in UNIX -Creation theUNIX command

dd of=sparse-file bs=.5k seek=2560 count=0

Will create a file of 2 GB in size, but with no data stored on disk (only metadata). (GNU dd has this behavior because it calls truncate to set the file size; other implementations may merely create an empty file.)

Detection

The -s option of the ls command shows the occupied space in blocks.

ls -ls sparse-file

Copying

Normally, the GNU version of cp is good at detecting whether a file is sparse, so

cp sparse-file new-file

Creates new-file, which will be sparse. However, GNU cp does have a --sparse=WHEN option. This is especially useful if a file containing long zero blocks is saved in a non-sparse way (i.e. the zero blocks have been written out to disk in full). Disk space can be saved by doing:

cp --sparse=always file1 file1\_sparsed

Some cp implementations, like FreeBSD's cp, do not support the --sparse option and will always expand sparse files. A partially viable alternative on those systems is to use sync with its own -sparse option instead of cp. unfortunately --sparse cannot be combined with --in place, so syncing huge files across the network will always be wasteful of either network bandwidth or disk bandwidth.

cp --sparse=always /proc/self/fd/0 new-sparse-file <somefile

3.3. Sets the segment size of the created forensic image file:

This setting enables the forensic image file to be broken into segments of a specific size. Setting an image segment size is primary used when the forensic image files will later be stored on fixed length media such as CD or DVD.

For the EnCase-.E01 image format, Forensic Imager uses the EnCase-v6 standard 2 GB and is not limited to a 2 GB segment size. However, if an investigator plans to use larger file segments they should give consideration to the limitations (RAM etc.) of the systems on which the image files will be processed.

3.4. Sets the destination path and file name for the image file:

The output file name is the name of the forensic image file that will be written to the investigators forensic workstation. Click on the folder icon to browse for the destination folder.

3.5. Calculates an MD5 and/or SHA256 acquisition hash of the imaged data:

A hash value is a mathematical calculation that is used for identification, verification, and authentication of file data. A hash calculated by Forensic Imager during the acquisition of a device (the “acquisition hash”) enables the investigator, by recalculating the hash at a later time (the “verification hash”), to confirm the authenticity of the image file, i.e. that the file has not changed. Any change to the acquired image will result in a change to the hash value.

3.6. Report

This guide describes best practices for copying file and investigating a case involving a 2 GB drive. These include

* Evaluating the scene.
* Using media storage for the scene.  Coping the drive accurately.
* Completing and recording the scene investigation.
* Sets the destination path and file name for the image file.
* Sets the segment size of the created forensic image file.
* Calculates an MD5 and/or SHA256 acquisition hash of the imaged data.

4.Case Project 3-5

You’re investigating a case involving a 2 GB drive that you need to copy at the scene. Write

one to two pages describing the three types of acquisitions—physical, logical, and sparse—

you can use to copy the drive accurately. Be sure to include your software and media choices.

Now that you have identified the requirements of the Domain Name case, you can plan your investigation. You have already determined the kind of evidence you need; now you can identify the specific steps to gather the evidence, establish a chain of custody, and perform the forensic analysis. These steps become the basic plan for your investigation and indicate what you should do and when. To investigate the Domain Name case, you should perform the following general steps. Most of these steps are explained in more detail in the following sections.

1. Acquire the USB drive from George’s manager.

2. Complete an evidence form and establish a chain of custody.

3. Transport the evidence to your computer forensics lab.

4. Place the evidence in an approved secure container.

5. Prepare your forensic workstation.

6. Retrieve the evidence from the secure container.

7. Make a forensic copy of the evidence drive (in this case, the USB drive).

8. Return the evidence drive to the secure container.

9. Process the copied evidence drive with your computer forensics tools

5.Case Project 3-6

Your supervisor has asked you to list the acquisition tools available on a forensic Linux Live

CD. Download the current ISO version of Deft (www.deftlinux.net), CAINE (www.caine-live.net),

Kali Linux (www.kali.org), or Penguin Sleuth (www.linux-forensics.com), and then create a

bootable CD or DVD of it. Start it on your workstation and survey its tools. Then write a oneto

two-page report containing a brief description of each acquisition utility on the CD or DVD.

Description

**HashDeep tool:**

The hash deep tool is a modi ed version of the dc3dd hashing tool designed especially for digital forensics. This tool includes auto hashing of les, i.e., sha-1, sha-256, and 512, tiger, whirlpool, and md5. An error log le is auto written. Progress reports are generated with every output.

**Magic rescue tool:**

Magic rescue is a forensic tool that performs scanning operations on a blocked device. This tool uses magic bytes to extract all the known le types from the device. This opens devices for scanning and reading the le types and shows the possibility of recovering les deleted or corrupted partition. It can work with every le system.

**Scalpel tool:**

This forensic tool carves all the les and indexes those applications which run on Linux and windows. The scalpel tool supports multithreading execution on multiple core systems, which help in quick executions.

File carving is performed in fragments such as regular expressions or binary strings.

**Scrounge-NTFS tool:**

This forensic utility helps in retrieving data from corrupted NTFS disks or partitions. It rescues data from a corrupted le system to a new working le system.

**Guymager tool:**

This forensic utility is used to acquire media for forensic imagery and has a graphical user interface. Due to its multi-threaded data processing and compression, it is a very fast tool. This tool also supports cloning. It generates at, AFF, and EWF images. The UI is very easy to use.

**Pd d tool:**

This forensic tool is used in pdf les. The tool scans pdf les for speci c keywords, which allows you to identify executable codes when opened. This tool solves the basic problems associated with pdf les. The suspicious les are then analyzed with the pdf-parser tool.

**Pdf-parser tool:**

This tool is one of the most important forensic tools for pdf les. pdf-parser parses a pdf document and distinguishes the important elements utilized during its analysis, and this tool does not render that pdf document.

**Peepdf tool:**

A python tool that explores pdf documents to nd whether it is harmless or destructive. It provides all the elements needed to perform pdf analysis in one single package. It shows suspicious entities and supports various encodings and lters. It can parse encrypted documents too.

**Autopsy tool:**

An autopsy is all one forensic utility for fast data recovery and hash ltering. This tool carves deleted les and media from unallocated space using PhotoRec. It can also extract EXIF extension multimedia. Autopsy scans for compromise indicator using STIX library. It is available in the command line as well as GUI interface.

**img\_cat tool:**

img\_cat tool gives the output content of an image le. The image les recovered will have meta-data and embedded data, which allows you to convert them into raw data. This raw data helps in piping the output to calculate the MD5 hash.

**ICAT tool:**

ICAT is a Sleuth Kit tool (TSK) that creates an output of a le based on its identi er or inode number. This forensic tool is ultra-fast, and it opens the named le images and copies it to standard output with a speci c inode number. An inode is one of the data structures of the Linux system which stores data and information about a Linux le such as ownership, le size, and type, write and read permissions.

**Srch\_strings tool:**

This tool looks for viable ASCII and Unicode strings inside binary data and then prints the offset string found in that data. srch\_strings tool will extract and retrieve the strings present in a le and gives offset byte if called upon.

**6.Case Project 3-3**

You need to acquire an image of a disk on a computer that can’t be removed from the scene,

and you discover that it’s a Linux computer. What are your options for acquiring the image?

Write a brief paper specifying the hardware and software you would use.

Simply turning on the machine can already alter/destroy data that can be potential evidence, let alone booting its original OS.

The best solution is to remove the hard drive, connect it to another computer through a hardware write blocker and then grab a complete image of it with dd or some equivalent. The write blocker is necessary to prevent accidental write to the device that may alter potential evidence (although a basic Linux installation that doesn't mount drives automatically won't do any writes by itself, Mac OS and Windows will definitely do).

If that's not possibly then you need to go with the forensics Live-CD route, but since it involves booting the computer you may already trigger some firmware-embedded code designed to alter/destroy potential evidence (hard but not impossible to do, it depends on what kind of criminal you're after).

Note that in the end, it doesn't matter what OS was installed on the computer since you shouldn't boot that OS anyway, and a bit-by-bit copy doesn't care about the data or even the filesystem that's on the drive (you can copy encrypted drives, but that won't help you much if you don't have the key since the copy is still encrypted).

Subject Code:: CIS8708Subject Name ::Digital ForensicsQuestion 1You need to acquire an image of a disk on a computer that can’t be removed from the scene, and youdiscover that it’s a Linux computer. What are your options for acquiring the image? Write a briefresponse specifying the hardware and software you would use.Solution 1Description of the Linux OS and the best-suited commands for acquisitionThe Linux OS has predefined features which offer essential forensic tools which can be used for dataacquisition. For instance, the OS is capable of acquiring data through an unmounted drive, and it alsocontains a unique feature which can read as well as mount the majority of drives. The access gainedthrough physical address can be achieved through the use of various external storage devices such asexternal hard drives, USB drives, and disk drives. For this case, where the computer is categorized as asuspect computer, the technique used to access the data is "Linux base acquisition technique.”Tools required in data acquisition are:a.Forensic live CDb.SATA external drives, USB, cablesc.Ability to change the suspect computer’s BIOS in order to run the live CDd.Familiarity with the shell command necessary for the acquisition of dataData Acquisition commands.The data dump, "dd", a command with several switches and functions which entails reading and writingdata from media devices are used for data acquisition. The dd command generates raw file formatswhich the forensic tools can read since the physical structure of the file does not bound the command.Thus, making the command useful for the acquisition of data. However, the command is ineffective andis only used for data acquisition instead of forensic acquisition. Detectives opt for the “dcfldd” commandfor data acquisition purposes and to increase effectiveness and robustness of forensic acquisitionsdeveloped by, Nicolas harbour and can

A.Stipulate the vital hexadecimal pattern as well as text used for cleaning

B.Use the MD5, SHA-384, SHA-512, SHA-256 and SHA-1 with logging.

C.Show the precise process progress

D.Fragment into several sections with each section given a number then make a copy. Thissegmentation is suitable for data acquisition.

E.Compare original data to the acquired data to check for exactness.

F.Log all output errors for ease of comparison, discussion and examination after the acquisition