Guide to Computer Forensics and Investigations

(4th Edition)

Chapter 4, Problem 2CP | 7 Bookmarks | Show all steps: ON

Problem

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.

Step-by-step solution

Step 1 of 5

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.

Comment

Step 2 of 5

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.

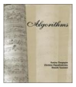
Many time investigators get only one chance to make the copy or image of the disk. So like in this case the investigator get a very less time for the acquisition of the data. Static acquisition is very much used in the digital evidences in these types of cases the data once gone never get the second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

Comment

Step 3 of 5

Tools used in investigation

Guide to Computer...
4th Edition
(1)



Algorithms
1st Edition

Loose Leaf for Digital..
1st Edition

View all solutions

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.

Comment

Step 4 of 5

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, UDF and many more.

6. In integration with the tools of intrusion detection system (IDS) to make the replica of facts of intrusion 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.

Comment

Step 5 of 5

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.

Comment

Was this solution helpful? 0 0

Recommended solutions for you in Chapter 4

Chapter 4, Problem 3RQ

What are two advantages and disadvantages of the raw format?

See solution

Chapter 4, Problem 2RQ

Name the three formats for computer forensics data acquisitions.

See solution

COMPANY

About Chegg
Chegg For Good
College Marketing
Corporate Development
Investor Relations
Jobs
Join Our Affiliate Program
Media Center
Site Map

LEGAL & POLICIES

Advertising Choices
Cookie Notice
General Policies
Intellectual Property Rights
Terms of Use
Global Privacy Policy
DO NOT SELL MY INFO
Honor Code
Honor Shield

CHEGG PRODUCTS AND SERVICES

Cheap Textbooks
Chegg Coupon
Chegg Play
Chegg Study Help
College Textbooks
eTextbooks
Flashcards
Learn
Uversity
Chegg Math Solver
Mobile Apps
Sell Textbooks
Solutions Manual
Study 101
Textbook Rental
Used Textbooks
Digital Access Codes
Chegg Life
Chegg Writing

CHEGG NETWORK

EasyBib
Internships.com
Thinkful

CUSTOMER SERVICE

Customer Service
Give Us Feedback
Manage Subscription