Practical No. :- 01

Aim :- Creating a Forensic Image using FTK Imager / Encase Imager :-

- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

Theory :-

FTK Imager :-

FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group It is a tool that helps to preview data and for imaging. Creating forensic images or perfect copies of local hard ~~dis~~ drives, flappy and zip disks, DVDs, ~~flor~~ folders, individual files, etc. without making changes to the original evidence is done by FTK Imager.

With the help of FTK Imager, we can also preview the contents of the forensic images that might be stored on a local machine or drive. We can mount an image for a read-only view that will also allow you to view the contents of the forensic image exactly as the user saw it on the origina drive. Using this, we can export files and folders from forensic images.

A Forensic Image is most often needed to verify the integrity of the image after an acquisition of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a forensic image has been created, its integrity can be checked to verify that it has

not been tampered with.

Forensic Imaging is defined as the processes and tools used in copying an electronic media such as a hard-disk drive for conducting investigations and gathering evidence that will be presentable in the law of court. This copy not only includes files that are visible to the operating system but every bit of data, every sector, partition, files, folders, master boot records and unallocated spaces. The image is an identical copy of all the drive structures and contents. A Forensic image can be backed up and tested on without damaging the original copy or evidence.

Also, We can create a forensic image from a running or dead machine. It is a literal snapshot in time that has integrity checking.

Practical No. :- 02

Aim :- Data Acquisition :-

- Perform data acquisition using :-
- USB Write Blocker + FTK Imager

Theory :-

ProDiscover Basic :-

ProDiscover forensics suite addresses a wide range of cybercrime scenarios encountered by law enforcement and corporate internal security investigators. ProDiscover Basic is widely used in Computer Forensics and Incident Response. The product suite is also equipped with ~~diagon~~ diagnostic and evidence collection tools for corporate policy compliance investigations and electronic discovery.

ProDiscover helps in efficiently uncovering files and data of interest. Wizards, dashboards and timeline views help in speedily discovering vital ~~infora~~ information. Investigators are provided with a wide range of tools and integrated viewers to explore the evidence disks and extract artifacts relevant to the investigation. It combines speed and accuracy, with ease of use and is available at an affordable price.

ProDiscover was launched in 2001 and it has a rich history. It was one of the first products to support remote forensic capabilities. The product suite is used in more than 70 countries in various high profile and complex investigations involving ~~cr~~ cybercrime.

The ARC Group ProDiscover Basic edition is a self-managed tool for the examination of your hard disk security. ProDiscover Basic is designed to operate under the National Institute of Standards' Disk Imaging Tool Specification 3.1.6 to collect snapshots of activities that are critical to taking proactive steps in protecting your data.

ProDiscover Basic has a built-in reporting tool to present findings as evidence for legal proceedings. You gather time zone data, drive information, Internet activity, and more, piece by piece, or in a full report as needed. You have robust search capabilities for capturing unique data, filenames and filetypes, data patterns, data ranges, etc. It gives clients the autonomy they desire in managing their own data security.

Practical No. :- 03

Aim :- Forensics Case Study :- Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy.

Theory :-

Autopsy :-

Autopsy is a forensic-level application that will help to scan raw images, local drives, and logical files for various errors and potential problems. With Autopsy, one can diagnose and scan their raw images, local drives, and files for potential errors and changes.

With the help of Autopsy, one can determine the cause of an event with the use of this application very easily. It supports NTFS, FAT, HFS, Ext2, Ext3 and UFS file systems. The app will investigate these systems and generate reports based on the findings it made during scans. It will analyze the input of different files and disks such as IMG, DD, 001, AA, RAW, E01, and other file types.

Autopsy application is very easy to use, Even if it sounds complicated, it's incredibly simple to use. All need to do is open the built-in wizard, create a new case, and analyze ~~you~~ the drive. From that point, it's just a matter of pressing a few "Next" buttons until you have to wait for the scan to complete. One can choose between a few different styles of scans. One can search for keywords, parse EXIF images, and view unallocated space.

2022.12.28

we can display data based on recent actions, perform a hash lookup, or extract archives, too.

With the ingest method, one can make the analysis results available as soon as they are obtained, so user won't have to wait too long for some quick results. User can also detect malware and potentially threatening files with hash lookup operations. It will process different formats to find this ~~oper~~ information and recognize potential threats.

Overall, Autopsy is one of the best forensic applications user can get for their computer when they want to learn exactly why an ~~error~~ has been shown on its computer. It's very simple to use and provides with accurate and lengthy analyses and reports on the scans made on its computer.

Practical No. :- 04

Aim :- Capturing and analyzing network packets using Wireshark (Fundamentals)

- Identification the live network
- Capture Packets
- Analyze the captured packets

Theory :-

Wireshark is a Network Protocol Analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Wireshark is the most often-used packet sniffer in the World. Wireshark proves to be an effective open source tool in the study of network packets and their behaviour. It can be used in identifying and categorizing various types of attack signatures. It lets administrator to see what's happening on network at a microscopic level.

Wireshark can be used as a tool for hackers. This usually involves reading and writing data transmitted over an unsecure or compromised network. This is a free software that is available for multiple platforms. This free cross-platform packet sniffer can securely analyze data. It can also be used for troubleshooting network issues. Wireshark uses 'pcap' to capture packets, so it can be also capture packets on the types of networks

that pcap supports. Wireshark puts the network traffic under a microscope and provides tool to filter and drill down into that traffic, zooming in on the root cause of the problems, assisting with network analysis and ultimately network security.

Practical No. :- 05

Aim:- Analyze the packets provided in lab and solve the questions using Wireshark :-

- What web server software is used by www.snopes.com?
- About what cell phone problem is the client concerned?
- According to Zillow, what instrument will Ryan learn to play?
- How many web servers are running Apache?

Theory :-

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the Internet. Wireshark is the most often-used packet sniffer in the world. Wireshark proves to be an effective open source tool in the study of network packets and their behavior. It can be used in identifying and categorizing various types of attack Signatures. It lets administrator to see what's happening on network at a microscopic level.

Wireshark can also be used as a tool for hackers. This usually involves reading and writing data transmitted over an unsecure or compromised network. This is a fr software that is available for multiple platforms. This is a free software that is available for multiple platforms. This free cross-platform packet sniffer can

securely analyze data. It can also be used for troubleshooting network issues. Wireshark uses 'pcap' to capture packets, so it can also capture packets on the types of networks that pcap supports. Wireshark puts the network traffic under a microscope, and provides tool to filter and drill down into that traffic, zooming in on the root cause of the problems, assisting with network analysis and ultimately network security.

Practical No. :- 06

Aim:- Using Sysinternals tools for Network Tracking and Process Monitoring :-

- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

Theory :-

The Sysinternals tool is simply a set of windows applications that can be downloaded for free. These tools are portable, which means that you can stick them on a flash drive and use them from any PC. The sysinternals toolset consists of 6 major categories of utilities :- File and Disk, Networking Process, Security, System Information and Miscellaneous utilities. TCP View is a windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.

Sysinternals Process Monitor runs on a windows device and uses a filter driver to log real-time file systems, registry and process/thread monitoring. It is a vital tool for trouble shooting windows and combines the capabilites of two older

sysinternals tools :- filemon and regmon. Process Monitor does not require installation. Cache set is an applet that allows you to manipulate the working-set parameters of the system file cache. Windows sysinternals is a suite of more than 70 freeware utilities that was initially developed by Mark Russinovich and Bryce Cogswell that is used to monitor, manage and troubleshoot the windows operating system.

Syste SysInternal tools are simple yet powerful security tools which tell which access to directories, files and Registory Registry keys on your systems. It is also used to find holes in permissions.

Practical No. :-

Aim:- Acquisition of Cell phones and Mobile devices.

Theory :-

MOBILedit Forensic is a digital forensics product by compelson labs that searches, examines and report on data from GSM / CDMA / PCS cell phone devices. MOBILedit connects to cell phone devices via an Infrared (IR) port, a blutooth link, Wi-Fi, or a cable interface. After connectivity has been established the phone model is identified by its manufacturer, model number and serial number (IMEI) and with a corresponding picture of the phone.

MOBILedit is a platform that works with a variety of phones and smartphones. With MOBILedit Forensic we can view, search for or retrieve all data from a phone with only a few clicks. It supports thousands of different phones including common feature phones. It also supports all smart-phone operating systems. MOBILedit Forensics can go through the protection and retrieve the data. It supports importing the lockdown files that can be found on a suspects computer. These files are operated when you connect an ios device to a PC and authorize the computer by typing the passcode. MOBILedit Forensics will instruct you on how to obtain these files. If you import the lockdown files to the computer where you make acquisition, then you be able to retriere all data from the phone even if it is locked with a passcode.

Practical No. :-

Aim:- Email Forensics
- Mail Service Providers
- Email protocols
- Recovering emails
- Analyzing email header

Theory :-

Email Forensics is exactly what it sounds like. The analysis of emails and the content within to determine the legitimacy, source, date, time, the actual sender, and recipients in a forensically sound manner. The aim of this is to provide admissible digital evidence for use in civil or crime courts. Most organisations have specific internal and external policies in place to help safeguard their data, intellectual property, finances and reputation. However, this does not always stop individuals from violating these policies to the detriment of their employer. These violations can present themselves in the form of forbidden file transfers, data breaches, indecent imagery and incriminating email threads.

Forensic Toolkit or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information. It can locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption. It is court-accepted, digital investigations software that includes many features and

capabilities such as full-disk forensic images, decrypt files and crack passwords, parse registry files, collect, process and analyze datasets, and advanced volatile memory analysis.

FTK is recognized as the standard toolkit for cyber defense forensic analysts, incident responders and other professional working or collecting forensic evidence. This path will cover the basic tools within the FTK suite - FTK Imager, Registry Viewer and Password Recovery Toolkit (PRTK) Then dive into use cases and analysis with FTK Suite.

Forensic Toolkit (FTK) provides you with an entire suite of investigative tools necessary to conduct digital investigations smarter, faster and more effectively. AccessData FTK provides allows to quickly establish case facts through innovative and market leading features such as distributed processing, collaborative case analysis, evidence visualization reports and more; all in one single comprehensive solution. It provides innovative and integrated features to support data processing integrity, speed and analysis depth.

Practical No:-

Aim:- Web Browser Forensics.

- Web Browser working
- Forensics activities on browser
- Cache / Cookies analysis
- Last Internet activity

Theory:-

Browsers have become an inherent part of our virtual life and we all make use of browsers for surfing the internet in some or the other way. Also, browsers can be used not only for surfing, we can make use of browsers for navigating through the file system of the OS. You might have observed by default browsers store data like search queries, username, password, form data, emails and other sensitive information. Also, browsers do contain downloaded media like Images, Videos, Exe's documents etc. Bookmarks and browser history gives an idea of the user's surfing habit and interest.

Browser forensic is mainly used for analyzing things like browsing history and general web activity of a pc to check for suspicious usage or content that has been accessed. This also refers to monitoring traffic on a webpage & analysis of LOG files from server to get actual information about targeted machine.

Before investigating the information of a user gathered by the web browser, it is crucial for us to understand the

mechanism by which the web browser gathers the data initially and how it is subsequently stored in the computer. Let us look at the progression of things. The user enters the website name, the URL onto the browser's address bar or searching for the same using keywords in a search engine. The URL is then searched by the web browser, and is subsequently located and connected to, by breaking it into an IP address, which makes the URL unique and that the user is kept from connecting to the wrong website. While this process happens, the web browser is also simultaneously creating log files, storing data onto the cache files and a few other things in the user's device.

Searching for evidence left by Web browsing activity is typically a crucial component of digital forensic investigations. Almost every movement a suspect performs while using a Web browser leave a trace on the computer, even searching for information using a Web Browser. Therefore, when an investigator analyzes the suspect's computer, this evidence can provide useful information. After retrieving data such as cache, history, cookies and download list from a suspect's computer, it is possible to analyze this evidence Web sites visited, time and frequency of access, and search engine keywords used by the suspect.