**Practical 1**

**File system analysis using Sleuth kit**

**Description**

The Sleuth Kit provides a plug-in framework that makes it easier to build end-to-end digital forensics solutions. The framework makes it easier to integrate the various analysis modules that each focus on different file types and analysis techniques.

[Autopsy](https://www.sleuthkit.org/autopsy/index.php) is a graphical interface to the tools in The Sleuth Kit, which allows you to more easily conduct an investigation. Autopsy provides case management, image integrity, keyword searching, and other automated operations.

**Why Is It Needed?**

The Sleuth Kit has historically focused on volume and file systems and the end result is information about files. The user must then use a variety of different tools with different interfaces and requirements to analyze at the application-layer. There are too many file types and analysis techniques at the application-layer for a single tool to be able to provide all of the solutions.

The Sleuth Kit Framework provides an open platform for application-layer modules to operate. The modules do not need to worry about getting access to files (the framework takes care of that) and users do not need to worry about copy data in between various tools.

Input Data

* Analyzes raw (i.e. dd), Expert Witness (i.e. EnCase) and AFF file system and disk images.
* Supports the NTFS, FAT, ExFAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS, ISO 9660, and YAFFS2 file systems
* Tools can be run on a live Windows or UNIX system during Incident Response. These tools will show files that have been "hidden" by rootkits and will not modify the A-Time of files that are viewed.

Search Techniques

* List allocated and deleted ASCII and Unicode file names.
* Display the details and contents of all NTFS attributes.
* Display file system and meta-data structure details.
* Create time lines of file activity, which can be imported into a spread sheet to create graphs and reports.
* Lookup file hashes in a hash database, such as the [NIST NSRL](http://www.nsrl.nist.gov/), [Hash Keeper](http://www.hashkeeper.org/), and custom databases that have been created with the 'md5sum' tool.
* Organize files based on their type (for example all executables, jpegs, and documents are separated). Pages of thumbnails can be made of graphic images for quick analysis
* The Sleuth Kit is written in C and Perl and uses some code and design from The Coroner's Toolkit (TCT).

The Sleuth Kit has been tested on:

* Linux
* Mac OS X
* Windows (Visual Studio and mingw)
* CYGWIN
* Open & FreeBSD
* Solaris

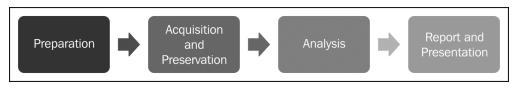
The framework is based on three phases of the analysis process:

* File Extraction: The framework uses TSK and carving tools to analyze disk images and identify the files. Information about each file is added to a central database (SQLite, PostgreSQL, etc.).
* File Analysis: Each file is analyzed by running it through a framework pipeline, which is a series of modules. Each module has a specific analysis task, such as calculating a hash value, looking up a hash value, or calculating entropy. Each file is processed by the pipeline and the module results are saved to the database.
* Post Processing / Reporting: After all files have been analyzed, another pipeline is run with post processing tasks. These modules may merge results together or may make final reports.

**Practical NO 2**

## Introducing computer forensics and FTK

* Computer forensics is a digital forensic science that relates to the generation of legal evidence found in computers and the digital media. The computer forensics process aims at examining the digital media in a forensically sound manner with the goal of acquiring, preserving, analyzing, and presenting relevant facts about a specific case; for example, digital crime, fraud, misuse of resources, and so on.
* The steps presented in the following diagram are intended to help drive the research process and get the evidence that could be presented in court, demonstrating that the best practices of computer forensics were followed. The computer forensics process can be explained using the steps shown in the following diagram:



## Key Product Features

FTK provides real-world features that help teams make sense of and manage massive data sets, separate critical data from trivial details, and protect digital information while complying with regulations.

* Unmatched speed through distributed processing engines
* Unique architecture provides better stability
* Wizard-driven to ensure no data is missed
* State-of-the-art data visualization to highlight relationships and patterns
* Only solution that utilizes a single case database, reducing cost and complexity of multiple case datasets
* Faster learning with easy-to-use GUI

## Data storage media

It is important to realize that data acquisition may be performed not only on hard disks, but also across other devices that have the storage capacity, few of which are listed as follows:

Magnetic media:

* Floppy disks
* Hard drives
* USB/PC cards
* ZIP and tape drives

Optical media:

* CDs
* CD-Rs and CD-RWs
* DVDs

Alternative media:

* MP3 players
* Tablets
* Smartphones
* Video games, TVs, and so on

## Image formats:

* FTK Imager can support almost all types of images used in the market. The main types are filesystems supported, Imager creates formats supported, and Imager read formats. These are listed as follows:

Filesystems supported FTK Imager supports the following filesystems:

* DVD (UDF)
* CD (ISO, Joliet, and CDFS)
* FAT (12, 16, and 32)
* exFAT
* VXFS
* EXT (2, 3, and 4)
* NTFS (and NTFS compressed)
* HFS, HFS+, and HFSX

FTK Imager can create evidence files of the following formats:

* E01, S01, and L01
* AF
* AD1
* RAW/DD

## What Is the FTK Imager? How Is the FTK Imager used?

Though we’ve established just how versatile a toolkit FTK is for forensic investigations, it is never a good idea to start feeding it the original files. A sound forensic practice is to acquire copies (images) of the affected system’s data and operate on those copies. To aid in this process, Access Data offers investigators a standalone disk imaging software known as FTK Imager.

In addition to creating images of hard drives, CDs and USB devices, FTK Imager also features data preview capabilities. This can be used to preview both files/folders and the contents residing in those files. FTK Imager also supports image mounting, which enhances its portability. The tool is one of very few that can create multiple file formats: EO1, SMART, or DD raw. You can also easily track activities through its basic text log file.

While creating copies of original disk drives, a critical aspect is to check file integrity. FTK Imager also assists in this area, with support for creating MD5 and SHA1 hashes. Furthermore, you can generate hash reports that can be archived for later use. For instance, if you want to check whether an image has been changed since its acquisition.

Once you’ve created images of disk drives using FTK Imager, you can then move on to a more thorough investigation of the case with FTK.

**Practical 3:**

**Data acquisition**

Data acquisition is the process of making a forensic image from computer media such as a hard drive, thumb drive, CDROM, removable hard drives, thumb drives, servers and other media that stores electronic data including gaming consoles and other devices.

The forensic image is made using specialized hardware that prevents any data from being written to the source media so it remains pristine. The forensic image, not the original media, is used by the forensic examiner to conduct the examination. The data acquisition process includes the recording of all serial numbers and other markings using a digital camera.

The forensic image is verified against the original to ensure the forensic image is an exact duplicate of the original media.

**Prodiscover basic**

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 have robust search capabilities for capturing unique data, filenames and filetypes, data patterns, date ranges, etc. ProDiscover Basic gives clients the autonomy they desire in managing their own data security.

With ProDiscover Basic, professional consultants, system administrators, and investigators take the upper hand to manage cyber security at every level and protect information in the case of impending legal actions. The program can quickly search large data sets and find the documents you need and also it can preserve critical "last accessed" metadata and document your results.

**Practical 4**

**File Recovery**

Data recovery refers to the process of rescuing inaccessible data from corrupted/damaged/formatted/wiped/dead drives, such as internal hard drive and removable USB device.

**Forensic Data Recovery Analysis**

With the rapid development of computer & network, we can easily find out the fact in cyber crimes and civil disputes by taking advantage of network are increasing in recent years. In this context, electronic evidence (digital evidence) obtained by electronic forensic starts to step into

judicial authentication filed.

After the digital evidence acquired by electronic forensic during judicial identification was deleted or formatted accidentally , we’re now able to get it back by using relevant techniques and tools. Under the proper operations of electronic forensic, reliable evidence can be found to justice criminals through judicial identification.

**Forensic Toolkit**, or FTK, is a [computer forensics](https://en.wikipedia.org/wiki/Computer_forensics) software made by [AccessHYPERLINK "https://en.wikipedia.org/w/index.php?title=AccessData&action=edit&redlink=1" HYPERLINK "https://en.wikipedia.org/w/index.php?title=AccessData&action=edit&redlink=1"Data](https://en.wikipedia.org/w/index.php?title=AccessData&action=edit&redlink=1).

FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence .For example, it can locate deleted emails and scan a disk for text strings to use them as a [password dictionary](https://en.wikipedia.org/wiki/Password_dictionary) to crack encryption.

The toolkit also includes a standalone [disk imaging](https://en.wikipedia.org/wiki/Disk_imaging) program called FTK Imager. The FTK Imager is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later reconstructed. It calculates MD5 hash values and confirms the integrity of the data before closing the files. The result is an image file(s) that can be saved in several formats, including DD raw.

FTK provides real-world features that help teams make sense of and manage massive data sets, separate critical data from trivial details, and protect digital information while complying with regulations.

**Practical 5**

**Forensic Toolkit**, or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information.[[1]](https://en.wikipedia.org/wiki/Forensic_Toolkit) It can locate deleted emails[[2]](https://en.wikipedia.org/wiki/Forensic_Toolkit) and scan a disk for text strings to use them as a password dictionary to crack encryption.[[3]](https://en.wikipedia.org/wiki/Forensic_Toolkit)

The toolkit also includes a standalone disk imaging program called **FTK Imager**. The FTK Imager is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later on reconstructed. It calculates MD5 hash values and confirms the integrity of the data before closing the files.

**Features of FTK**

**Unmatched Speed and Stability**

FTK uses distributed processing and is the only forensics solution to fully leverage multi-thread/multi-core computers. FTK uses 100 percent of its hardware resources, helping investigators find relevant evidence faster.

**FASTER SEARCHING**

Since indexing is done up front, filtering and searching are completed more efficiently than with any other solution. Whether you’re investigating or performing document review, you have a shared index file, eliminating the need to recreate or duplicate files.

**DATABASE DRIVEN**

FTK is truly database driven, using one shared case database. All data is stored securely and centrally, allowing your teams to use the same data. This reduces the cost and complexity of creating multiple data sets.

**BENEFITS**

Integrated Computer Forensic Solution.

Unmatched Processing.

Handle massive data sets without crashing or loosing work.

Feature rich out of the box.

Fast, Comprehensive index and Binary searching.

File and Disk Encryption Support.

Advanced gallery view for images and video with eid.

Microsoft® PhotoDNA®.

Superior Email Analysics.

Single-Node enterprise (Remote Investigration).

Volatile and Memory Analysics.

Internet Artifact Analysics.

Broad Support and OS Analysics.

**Practical 6**

**Encase**

EnCase is the shared technology within a suite of digital investigations products by Guidance Software. Encase is traditionally used in forensics to recover evidence from seized hard drives. Encase allows the investigator to conduct in depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.

**EnCase Forensic Investigation Lifecycle:**

* Triage

EnCase Forensic enables you to quickly search, identify, and prioritize potential evidence, in computers and mobile devices, to determine whether further investigation is warranted. This will result in a decreased backlog so that investigators can focus on getting to case closed.

* Collect

EnCase Forensic helps you acquire more evidence than any product on the market. You can collect from a wide variety of operating and file systems, including over 25 types of mobile devices with EnCase Forensic. Parse the most popular mobile apps across iOS, Android, and Blackberry devices so that no evidence is hidden.

* Decrypt

EnCase Forensic is unmatched in its decryption capabilities, offering the broadest support of any forensic solution. Encryption support includes products such as Dell Data Protection, Symantec, McAfee, and many more. You can further expand the decryption power of EnCase Forensic with Tableau Password Recovery

* Process

The EnCase Forensic evidence processor provides industry-leading processing capabilities that can automate the preparation of evidence, making it easier to complete the investigation.

* Investigate

EnCase Forensic is built with the investigator in mind, providing a wide range of capabilities that enables you to perform deep forensic analysis as well as fast triage analysis from the same solution.

* REPORT

EnCase Forensic provides a flexible reporting framework that empowers you to tailor case reports to meet your specific needs. With comprehensive and triage reporting options built in, you can create reports for a wide range of audiences and easily share them across your organization

**Practical 7**

**Steganography**

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

Steganography techniques can be applied to images, a video file or an audio file. steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

The goal of **steganography** is to hide a message in one-to-one communications and the goal of watermarking is to hide message in one-to-many communications. Shortly, one can say that cryptography is about protecting the content of messages, **steganography** is about concealing its very existence.

**Steganography Tools**

**Xiao Steganography**

Xiao Steganography can be used to hide secret files in BMP images or in WAV files. You can just open the software, load any BMP image or WAV file to its interface. Then add a file, which you want to hide. It also supports encryption. So, you can select from various algorithms like RC4, Triple DES, DES, Triple DES 112, RC2 and hashing SHA, MD4, MD2, MD5.

**Image Steganography**

Image Steganography is open source software for hiding your information in image files. You can hide text message or files inside an image file. Just select the source file in which you want to hide the secret message, and then select the file to hide or write the text message to hide. Select the output image location and then click on start button to start encoding the file. Encoded image will have the secret message inside the image. You can use the decode option of the same tool to decode the hidden file or message from the image.

**Practical 8**

**Password cracking**

Forensic specialists may encounter different protection systems for data access. The most common and simple system of protection is compressing archives by a password. At present, ZIP and RAR are two most commonly used archive managers. Russian archive manager (RAR) has a stronger encryption mechanism (AES-128 standard) which implies 128 bits encryption. This archive manger protects not only the access to files, but to other sensitive information like file name, time of creation, etc.

Passwords are also used for other purposes, like accessing the operating system, network environment, distant disks, distant servers, particular partitions/devices, particular databases, particular applications

**Cain & Abel**

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. its main purpose is the simplified recovery of passwords and credentials from various sources.

This cracking tool allows us to crack the password using different kind of methods.   
Some of them are:

* Brute Force Attack
* Dictionary attack
* Crypt Analysis attack
* recording VoIP conversations
* sniffing the network
* decoding scrambled passwords
* recovering wireless network keys
* revealing password boxes
* uncovering cached passwords
* analyzing routing protocols

**Requirements**  
The system requirements needed to successfully setup Cain & Abel are:

– At least 10MB hard disk space

– Microsoft Windows 2000/XP/2003/Vista OS

– Winpcap Packet Driver (v2.3 or above).

– Airpcap Packet Driver (for passive wireless sniffer / WEP cracker).

**Practical 9 & 10**

**Wireshark**

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Wireshark is cross-platform, runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark.

**Functionality**

Wireshark lets the user put network interface controllers into promiscuous mode, so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

If a remote machine captures packets and sends the captured packets to a machine running Wireshark using the TZSP protocol or the protocol used by Omni Peek, Wireshark dissects those packets, so it can analyze packets captured on a remote machine at the time that they are captured.

**Features**

Wireshark is a data capturing program that "understands" the structure of different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.

Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.

Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.

Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.

**Live capture from many different network media**

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. Which media types are supported, depends on many things like the operating system you are using.

**Practical 11**

**Email forensics**

Email has become the primary source of communication and almost everyone who owns a computer sends or receives emails on regular basis. One can imagine how email has become core part of communication with the fact that close to 3 million messages are sent every single second. Such widespread email penetration has resulted in various misuse of the technology. People with malafide intention use emails to commit the crime.

E-mail forensic analysis is used to study the source and content of e-mail

message as evidence, identifying the actual sender, recipient and date and time it was sent, etc. to collect credible evidence to bring criminals to justice.

AccessData Forensics Toolkit (FTK) is market leading tool for IT forensics examiners for many years.

Where to look for evidence:

Email received from headers will contain the actual IP address of the originating system, you just won’t know which header is correct

} Trace backwards by looking at the log files of the servers the mail claims to have passed through: once you get to a server that has no record of the email, the previous system is the originating IP

The email headers and web mail log files will point back to the anonymizer

} You will need to look at the anonymizer’s log files to determine what IP address accessed the web email account at the specific time the email was sent

} If the anonymizer is a paying service then you can also request subscriber information for the account that was using the anonymizer to send the web based email.

**Forensic Toolkit**, or FTK, is a computer forensics software made by AccessData. It can locate deleted emails[[2]](https://en.wikipedia.org/wiki/Forensic_Toolkit) and scan a disk for text strings to use them as a password dictionary to crack encryption.[[3]](https://en.wikipedia.org/wiki/Forensic_Toolkit)

**Features of FTK**

**Unmatched Speed and Stability**

FTK uses distributed processing and is the only forensics solution to fully leverage multi-thread/multi-core computers. FTK uses 100 percent of its hardware resources, helping investigators find relevant evidence faster.

**FASTER SEARCHING**

Since indexing is done up front, filtering and searching are completed more efficiently. Whether you’re investigating or performing document review, you have a shared index file, eliminating the need to recreate or duplicate files.

**DATABASE DRIVEN**

FTK is truly database driven, using one shared case database. All data is stored securely and centrally, allowing your teams to use the same data.

**Practical 12**

**Mobile forensics**

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, [SMS](https://en.wikipedia.org/wiki/SMS) and [MMS](https://en.wikipedia.org/wiki/Multimedia_messaging_service) messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

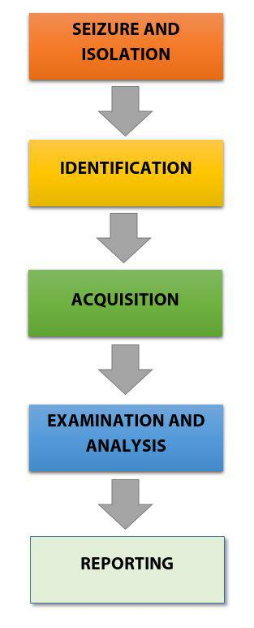
There is growing need for mobile forensics due to several reasons and some of the prominent reasons are:

* Use of mobile phones to store and transmit personal and corporate information
* Use of mobile phones in online transactions
* Law enforcement, criminals and mobile phone devices[2]

Mobiledit

[Forensic Express](http://www.mobiledit.com/forensic-express), you can extract all the data from a phone with such as deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from apps such as Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Signal, WeChat and many others.

The production process of the forensic evidence is divided in five main phase: the seizure, the identification, the acquisition and the examination or analysis. Once the data is extracted from a device, different methods of analysis are used based on the underlying case. As each investigation is distinct, it is not possible to have a single definitive procedure for all cases.



the two first steps involved in the production of a forensic evidence. In the next lessons will be explained in detail the remaining three steps.

Handling the device during seizure is one of the important steps while performing forensic analysis. It is important, for device seizure on the crime scene, to document with pictures, writing the “where and when”, mobile condition, if it was damaged, turned on or switched off, picture of the display if switched on, document the event of memory cards.

It is necessary to seizure cables, chargers, SIM card data or any papers or notes which may contain access codes that can also be deduced from the personal papers of the criminals whose devices were confiscated. Statistically many users use password similar on date of birth, celebrations, names, number plates and other personal information to remind themselves of passwords. Look for PIN and password can save much time later to investigators.

On the crime scene, it is fundamental to use proper techniques to protect the device from communicating with other devices, which may be phone calls, SMS, Wi-Fi Hotspot interferences, Bluetooth, GPS and many more. It is necessary to place the device into a Faraday bag and if it is possible add the use of a jammer, to avoid the alteration of the original state of the device. A phone call, an SMS, an email may overwrite the previous ones during the evidence collection phase if the phone was not isolated.

**Practical 13**

**Forensic Toolkit**, or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information.[[1]](https://en.wikipedia.org/wiki/Forensic_Toolkit) It can locate deleted emails[[2]](https://en.wikipedia.org/wiki/Forensic_Toolkit) and scan a disk for text strings to use them as a password dictionary to crack encryption.[[3]](https://en.wikipedia.org/wiki/Forensic_Toolkit)

The toolkit also includes a standalone disk imaging program called **FTK Imager**. The FTK Imager is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later on reconstructed. It calculates MD5 hash values and confirms the integrity of the data before closing the files.

**Features of FTK**

**Unmatched Speed and Stability**

FTK uses distributed processing and is the only forensics solution to fully leverage multi-thread/multi-core computers. FTK uses 100 percent of its hardware resources, helping investigators find relevant evidence faster.

**FASTER SEARCHING**

Since indexing is done up front, filtering and searching are completed more efficiently. Whether you’re investigating or performing document review, you have a shared index file, eliminating the need to recreate or duplicate files.

**DATABASE DRIVEN**

FTK is truly database driven, using one shared case database. All data is stored securely and centrally, allowing your teams to use the same data. This reduces the cost and complexity of creating multiple data sets