Practical No 01

Title: Working with Windows Forensic ToolKit (AccessData FTK)

Theory:

Computer Forensics:

Computer forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Access Data Forensic Toolkit:

FTK is one of the most admired software suites available to digital forensic professionals. This tool is developed by Access Data. FTK is intended to be a complete computer forensics solution. It gives investigators an aggregation of the most common forensic tools in one place. Whether you are trying to crack a password, analyze emails, or look for specific characters in files, FTK has got you covered. And, it comes with an intuitive GUI to boot.

Features of FTK:

1. ***Performance:*** Subscribing to a distributed processing approach, it is the only forensic software that utilizes multi-core CPUs to parallelize actions. This results in a momentous performance boost; – according to FTK's documentation, one could cut case investigation time by 400% compared to other tools, in some instances.
2. ***Shared Case Database:*** FTK uses only a single, central database for a single case. This enables team members to collaborate more efficiently, saving valuable resources. The use of a database also provides stability. FTK's database allows for persistence of data that is accessible even if the program itself crashes.
3. ***Robust searching speeds***: Due to the tool's emphasis on indexing of files up front, investigators can greatly reduce search times. FTK generates a shared index file, which means that you don't need to duplicate or recreate files.

FTK contains following tools:

1. Email Analysis
2. File Decryption
3. Data Carving

4. Data Visualization
5. Web Viewer
6. Cerberus
7. OCR

Practical No 02

Title: Exploring AccessData FTK

Theory:

Data carving

The process of restoring the artifacts is known as carving. More generally, data carving is the process of reconstructing logical objects (such as files, database records, and other data structures) directly from a bulk data capture (such as a disk, or RAM image) without the use of metadata describing the location and layout of the artifacts. File carving is most common and the oldest method that is used in data extraction. It is based on two simple observations:

1. Every file has a header and a footer signature. This signature is present in the form of Hex value which is also called magic number of a file. For example, .PNG file has a header signature: 89 50 4E 47, similarly the footer signature: 49 45 4E 44 AE 42 60 82.
2. Most file system has sequential file layout for better performance. This means that files are stored sequentially in the file system.

With the help of these two observations we can carve a file in just three steps:

1. Scan the data until the known header is found that we are looking for.
2. Scan the data until the known footer is found.
3. Copy the data in between the header and footer in the found offsets as the recovered artifact.

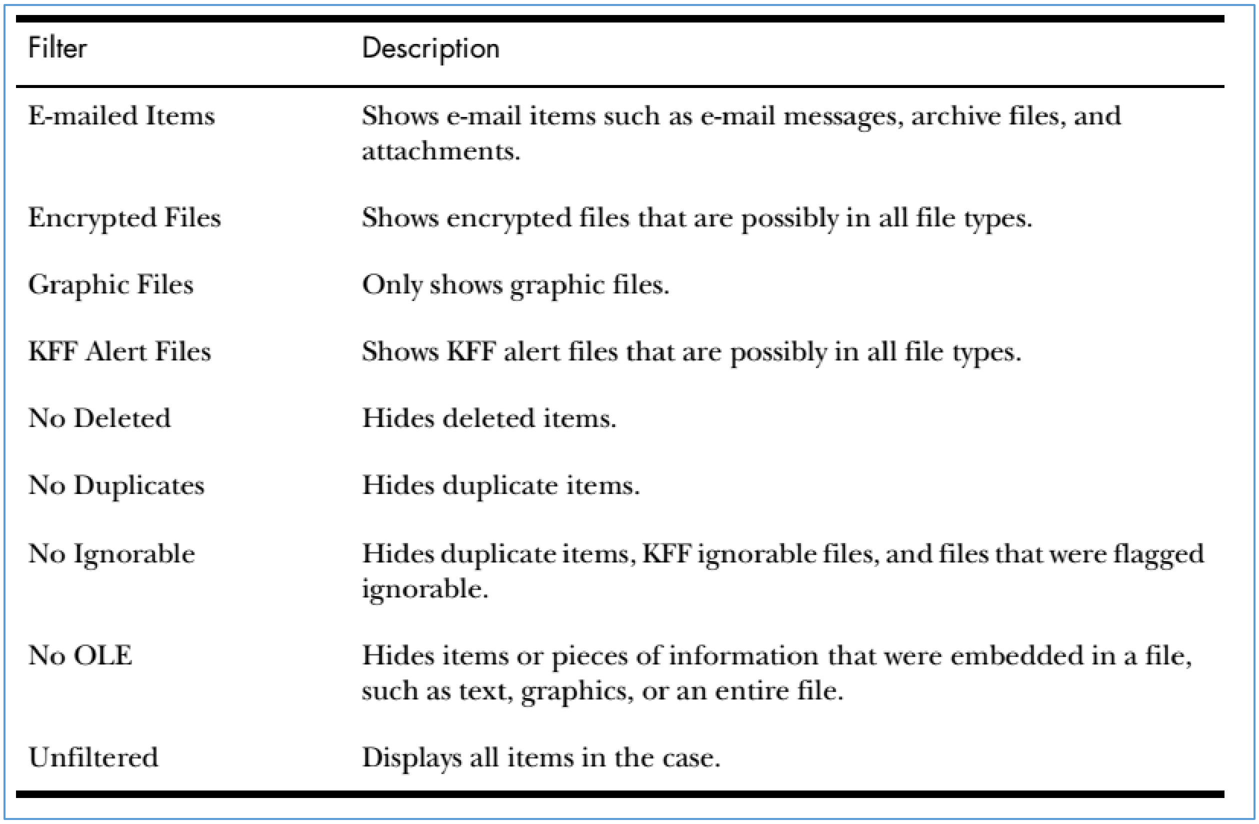
Data Carving can be split into two tasks

1. Data Extraction: identification of the chunks of content to be examined (such as disk block, file content, unallocated block), and
2. Artifact Reconstruction: reassembly of data that is recovered to find the conclusive result.

Using Filter:

If you want to minimize the number of evidence items to examine, you can apply an existing filter or create a customized filter to exclude unwanted items. Forensic Toolkit (FTK) allows you to filter your case evidence by file status, type, size, and date parameters.

FTK contains the following predefined filters:



Filter	Description
E-mailed Items	Shows e-mail items such as e-mail messages, archive files, and attachments.
Encrypted Files	Shows encrypted files that are possibly in all file types.
Graphic Files	Only shows graphic files.
KFF Alert Files	Shows KFF alert files that are possibly in all file types.
No Deleted	Hides deleted items.
No Duplicates	Hides duplicate items.
No Ignorable	Hides duplicate items, KFF ignorable files, and files that were flagged ignorable.
No OLE	Hides items or pieces of information that were embedded in a file, such as text, graphics, or an entire file.
Unfiltered	Displays all items in the case.

Searching the Registry

The Windows Registry allows the Windows operating system to control hardware, software, user information, and the overall functionality of the Windows interface. Unlike Windows Registry Editor, which only displays the current system's registry, Registry Viewer lets you examine registry files from any system. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

Practical No 03

Title: Exploring AccessData FTK (FTK Imager)

Theory:

FTK Imager

FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Access Data Forensic Toolkit (FTK) is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence. With FTK Imager, you can:

- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, and DVDs, entire folders, or individual files from various places within the media.
- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs
- Preview the contents of forensic images stored on the local machine or on a network drive
- Mount an image for a read-only view that leverages Windows Explorer to see the content of the image exactly as the user saw it on the original drive
- Export files and folders from forensic images.
- See and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive.
- Create hashes of files using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1)

Practical No 04

Title: Using Email Forensics Tools (AccessData FTK)

Theory:

Email Forensics:

Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes. Your goal is to find out who's behind the crime or policy violation, collect the evidence, and present your findings to build a case for prosecution or arbitration.

E-mail crimes and violations depend on the city, state, and sometimes country in which the e-mail originated. Committing crimes with e-mail is becoming commonplace, and more investigators are finding communications that link suspects to a crime or policy violation through e-mail. For example, some people use e-mail when committing crimes such as narcotics trafficking, extortion, sexual harassment, stalking, fraud, child abductions, terrorism, child pornography, and so on. Because e-mail has become a major communication medium, any crime or policy violation can involve e-mail.

Steps to examine the email messages:

- Copying an E-mail Message
- Viewing E-mail Headers
- Examining E-mail Headers
- Examining Additional E-mail Files
- Tracing an E-mail Message

Practical No 05

Title: Writing Report using FTK (AccessData FTK)

Theory:

General Guidelines for writing Computer Forensic Report:

- All reports to clients should start with the job mission or goal
    - Find information on a specific subject
    - Recover certain significant documents
    - Recover certain types of files
- Before you begin writing, identify your audience and the purpose of the report
- Hypothetical questions based on factual evidence
    - Less favored today
    - Guide and support your opinion
    - Can be abused and overly complex
- Opinions based on knowledge and experience
- Exclude from hypothetical questions
    - Facts that can change, cannot be used, or are not relevant to your opinion
- As an expert witness, you may testify to an opinion, or conclusion, if four basic conditions are met:
    - Opinion, inferences, or conclusions depend on special knowledge or skills
    - Expert should qualify as a true expert
    - Expert must testify to a certain degree of certainty
    - Experts must describe facts on which their opinions are based, or they must testify to a hypothetical question

Points to be considered while writing report:

- Consider
    - Communicative quality
    - Ideas and organization
    - Grammar and vocabulary
    - Punctuation and spelling
- Lay out ideas in logical order
- Build arguments piece by piece
- Group related ideas and sentences into paragraphs
    - Group paragraphs into sections
- Avoid jargon, slang, and colloquial terms
- Define technical terms
    - Consider your audience

- Consider writing style
    - Use a natural language style
    - Avoid repetition and vague language
    - Be precise and specific
    - Use active rather than passive voice
    - Avoid presenting too many details and personal observations
- Include signposts
    - Draw reader’s attention to a point

Practical No 06

Title: Using Steganography Tools (S-Tools)

Theory:

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. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

Rather than being incomprehensible to an unauthorized third party, as is the case with cryptography, steganography is designed to be hidden from a third party. Not only must the hidden data be discovered—considered a formidable task in and of itself—it must be encrypted, which can be nearly impossible. One use of steganography includes watermarking which hides copyright information within a watermark by overlaying files not easily detected by the naked eye. This prevents fraudulent actions and gives copyright protected media extra protection.

Steganography tools aim to ensure robustness against modern forensic methods, such as statistical steganalysis. Such robustness may be achieved by a balanced mix of:

- a stream-based cryptography process;
- a data whitening process;
- an encoding process.

If the data is detected, cryptography also helps to minimize the resulting damage, since the data is not exposed, only the fact that a secret was transmitted. The sender may be forced to decrypt the data once it is discovered, but deniable encryption can be leveraged to make the decrypted data appear benign.

S-tools:

Steganography using S-tools is the hiding of information within a picture, say a *.bmp file, a *.gif file or a *.wav file. Before using S-Tools understand the caveat that there are other more robust tools out there. The ground rule is that S-Tools requires that both sender and receiver have a shared passphrase.

Practical No 07

Title: File System Analysis (Autopsy)

Theory:

Autopsy is computer software that makes it simpler to deploy many of the open source programs and plugins used in The Sleuth Kit. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data.

Features of Autopsy:

- **Multi-User Cases**: Collaborate with fellow examiners on large cases.
- **Timeline Analysis:** Displays system events in a graphical interface to help identify activity.
- **Keyword Search:** Text extraction and index searched modules enable you to find files that mention specific terms and find regular expression patterns.
- **Web Artifacts:** Extracts web activity from common browsers to help identify user activity.
- **Registry Analysis:** Uses RegRipper to identify recently accessed documents and USB devices.
- **LNK File Analysis:** Identifies short cuts and accessed documents
- **Email Analysis:** Parses MBOX format messages, such as Thunderbird.
- **EXIF:** Extracts geo location and camera information from JPEG files.
- **File Type Sorting:** Group files by their type to find all images or documents.
- **Media Playback:** View videos and images in the application and not require an external viewer.
- **Thumbnail viewer:** Displays thumbnail of images to help quick view pictures.
- **Robust File System Analysis:** Support for common file systems, including NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.
- **Hash Set Filtering:** Filter out known good files using NSRL and flag known bad files using custom hashsets in HashKeeper, md5sum, and EnCase formats.
- **Tags:** Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.
- **Unicode Strings Extraction:** Extracts strings from unallocated space and unknown file types in many languages (Arabic, Chinese, Japanese, etc.).
- **File Type Detection** based on signatures and extension mismatch detection.
- **Interesting Files Module** will flag files and folders based on name and path.
- **Android Support**: Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more.

Practical No 08

Title: Using Data Acquisition Tools (ProDiscover Basic)

Theory:

ProDiscover® Basic 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, date ranges, etc.

ProDiscover Basic gives clients the autonomy they desire in managing their own data security.

- Reads and makes a copy of the disk's contents without altering any data
- Combines older methods used through DOS to easily access and read disk drives

What ProDiscover is used for:-

- Computer Forensics
- View Deleted files
- Search for contents of a disk
- Retrieve a file that was accidentally deleted

Key features of ProDiscover Forensic include:

- Create a Bit-Stream copy of the disk to be analyzed, including hidden HPA section (patent pending), to keep original evidence safe.
- Search files or an entire disk, including slack space, HPA section, and Windows NT/2000/XP Alternate Data Streams for complete disk forensic analysis.
- Preview all files, even if hidden or deleted, without altering data on disk, including file Metadata.
- Examine and cross reference data at the file or cluster level to ensure nothing is hidden, even in slack space.
- Utilize Perl scripts to automate investigation tasks.

Practical No 09 & Practical No 10

Title: Using log capturing and analysis tools & Using traffic capturing and analysis tools (Wireshark)

Theory:

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Colouring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

Practical No 11

Title: Using Password Cracking Tools (Cain and Abel)

Theory:

Cain and Abel (often abbreviated to Cain) is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks. Cryptanalysis attacks are done via rainbow tables which can be generated with the winrtgen.exe program provided with Cain and Abel.

Cain & Abel uses dictionary lists as a basis for cracking passwords, brute-force attacks by trying different passwords many times every second and decoding information stored on the hard drives, the package attempts to determine the correct password. The software also removes the hidden passwords by showing passwords in certain software packages. Learns wireless network keys for forgotten Wi-Fi login information. The software has some security benefits too by indicating where passwords are insecure in an active system.

Cain & Abel Key Features:

- Locate Wi-Fi password information
- Discover likely passwords for Windows operating system
- Dictionary-based words, brute-force password checking and other methods are used
- Reveal hidden password fields
- Sniff out data stored on drives to discover where passwords may be located
- Can be used for security to verify what can be easily discovered on your own system

Practical No 12

Title: Using Mobile Forensic Tools (MOBILedit)

Theory:

MOBILedit Forensic Express automatically uses multiple communication protocols and advanced techniques to get maximum data from each phone and operating system. Then it combines all data found, removes any duplicates and presents it all in a complete, easily readable report.

- Most of your investigative tasks will begin with the Main Connection Screen, which allows you to set up the phone you want to analyse.
- It will automatically search for any physically connected devices, but you can also import logical backups; connect to an iCloud account if you know the credentials for it; or use the Hack Phone option which helps you to get physical data from a phone without breaking any PINs or passcodes.
- The 'Hack Phone' option allows you to extract physical dumps from MTK chipsets (Chinese devices) and LG phones, and backups from Huawei devices.
- To use the Hack Phone option, first of all turn off the phone, then click 'Hack Phone' in MOBILedit Forensic Express and you will then be prompted through a number of screens before being asked to select a destination folder. Once you've done this you will be able to extract data from the phone as normal.
- It is possible to connect phones in recovery mode as well. In this case, you'll need to choose the recovery options on the phone itself, and it will need to fulfil certain requirements, such as having Bootloader open. Recovery mode provides you with more possibilities for data extraction; you can also create a physical image of the phone from recovery mode. It also allows you to access the data without knowing the PIN or pattern unlock sequence.
- If you're performing a normal physical extraction without using the Hack Phone option, first of all select the connected phone or select an import data source.
- If you need to root the phone, there is an option to do this; clicking on it will also provide you with a link to a handy guide showing you how to root the phone.
- Once the phone has been connected you will be able to see the IMEI. Clicking the 'i' icon will bring up some more details, such as which cable you need to use and which data can be extracted from the phone. Again, Forensic Express will warn you if there's something you should be aware of, for example 'You're using an old connector, would you like to update it'.