FORENSIC ARTICLE

CYBER FORENSICS

COMPUTER FORENSICS

Computer forensics is a method of extracting and preserving data from a computer so that it can be used in a criminal proceeding as evidence. Read on to find out more about data preservation and practical applications of computer forensics.

OVERVIEW

- **Most people can pick up someone's computer and do a quick search to find out the types of files they have saved and the sites they've visited online. Computer forensics does that and more. This field generally involves recovering data (either lost or deleted) from media, operating systems, peripherals, or disc drives. Files that are hidden from the average person are uncovered through an in-depth search of the computer system. This search can recover or reveal deleted, hidden, encrypted, and protected files. An employer, the IRS, government agencies, and other applicable institutions can use this information to discover fraudulent or criminal activity.**

- **Computer forensics is also a tool for tracking down people who commit identity theft. Even if a criminal uses a different computer system and deletes all incriminating evidence, the information may still reside on the computer and be useful in tracking down the perpetrator. Computer forensics methods have the ability to analyze data left on the system and determine its use, origin, and destination.**

DATA PRESERVATION

Just like with any type of criminal case, there are rules that must be followed in computer forensics. Evidence has to be kept as close to its original format as possible and stay relatively untouched, similar to crime scene preservation. Correctly analyzing the evidence is also important as is following the letter of the law, and respecting the privacy and rights of

individuals. Standard rules of evidence and legal processes are adhered to in cases of computer crime, whether the computer being examined was hacked into or used for a crime.

PRACTICAL APPLICATIONS

Computer forensics is used in many different situations by a wide number of professionals. It is applicable in civil and criminal proceedings, by both the defense the prosecution. Cases could include:

- **Divorce**
- **Financial or insurance fraud**
- **Identity theft**
- **Sexual harassment or child pornography**
- **Arson**
- **Age discrimination**

TYPES OF DIGITAL FORENSICS

- **COMPUTER FORENSICS**
- **NETWORK FORENSICS**
- **FORENSIC DATA ANALYSIS**
- **MOBILE DEVICE FORENSICS**
- **IOT FORENSICS**
- **CLOUD FORENSICS AND MANY MORE**

PROCESS OF DIGITAL FORENSICS

1. **Identification – Crime happen, identify crime scene**
2. **Preservation –Warrant, 1st respondent, seize evidence, transport**
3. **Extraction – bit by bit copy, MD5, SHA, Chain of custody, Storage**
4. **Interpretation – analysis**

5. **Documentation – Report generation 6. Presentation – Show evidence at court.**

MAINTAINING INTEGRITY

Methods used in the collection of evidence and the maintenance of chain of custody are crucial to the integrity of physical evidences.

MAINTAINING CHAIN OF CUSTODY

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analyzing the evidence, and so on.

IMPORTANT POINTS TO REMEMBER FOR FOOLPROOF CHAIN OF CUSTODY

- **Physically inspect the storage medium — take photographs and systematically record observations.**
- **Guard against hazards like theft and mechanical failure. Use good physical security and data encryption. House multiple copies in different locations.**
- **Protect digital magnetic media from external electric and magnetic fields. Ensure protection of digital media particularly optical media from scratches.**
- **Account for all people with physical or electronic access to the data.**
- **Keep the number of people involved in collecting and handling the devices and data to a minimum.**
- **Always accompany evidence with their chain-of-custody forms .**
- **Give the evidence positive identification at all times that is legible and written with permanent ink.**

WRITE BLOCKERS

A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker,

when used properly, can guarantee the protection of the data chain of custody. NIST's general write blocking requirements hold that:

- **The tool shall not allow a protected drive to be changed.**
- **The tool shall not prevent obtaining any information from or about any drive.**
- **The tool shall not prevent any operations to a drive that is not protected.**

Both software and hardware write blockers are available. Software write blockers are versatile and come in two flavors. The other method of software write blocking is to use a forensic boot disk. This will boot the computer from the HD. Developing checklists that can be repeatable procedures is an ideal way to ensure solid results in any investigation. Software write blockers are limited by the port speed of the port they are blocking, plus some overhead for the write-blocking process. But then, all write blockers are limited in this manner.

Hardware write blockers are normally optimized for speed. Forensic copying tools such as Logicube and Tableau are two examples of hardware write blockers, although many companies make them. Logicube will both hash and image a drive at a rate of about 3 GB/min. They are small and portable and can replace the need for bulky PCs on a job site.

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. 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.

STEGANOGRAPHY TECHNIQUES

Depending on the nature of the cover object, steganography can be divided into five types:

- **Text Steganography**
- **Image Steganography**
- **Video Steganography**
- **Audio Steganography**
- **Network Steganography**

BEST TOOLS TO PERFORM STEGANOGRAPHY

There is many software available that offer steganography. Some offer normal steganography, but a few offer encryptions before hiding the data. These are the steganography tools which are available for free:

- **Stegosuite is a free steganography tool which is written in Java. With Stegosuite you can easily hide confidential information in image files.**
- **Steghide is an open source Steganography software that lets you hide a secret file in image or audio file.**
- **Xiao Steganography is a free software that can be used to hide data in BMP images or in WAV files.**
- **SSuite Picsel is another free portable application to hide text inside an image file but it takes a different approach when compared to other tools.**
- **OpenPuff is a professional steganographic tool where you can store files in image, audio, video or flash files.**

IMAGE FORENSICS

- **The trustworthiness of photographs has an essential role in many areas, including: forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging, and journalism. The art of making image fakery has a long history. But, in today's digital age, it is possible to very easily change the information represented by an image without leaving any obvious traces of tampering.**
- **The digital information revolution and issues concerned with multimedia security have also generated several approaches to digital forensics and tampering detection. Generally, these approaches could be divided into active and passive–blind**

approaches. The area of active methods simply can be divided into the data hiding approach and the digital signature approach. We focus on blind methods, as they are regarded as a new direction and in contrast to active methods, they work in absence of any protecting techniques and without using any prior information about the image. To detect the traces of tampering, blind methods use the image function and the fact that forgeries can bring into the image specific detectable changes.

- **When digital watermarks or signatures are not available, the blind approach is the only way how to make the decision about the trustworthiness of the investigated image. Image forensics is a burgeoning research field and promise a significant improvement in forgery detection in the never–ending competition between image forgery creators and image forgery detectors.**

DETECTING TRACES OF RESAMPLING

When two or more images are spliced together, to create high quality and consistent image forgeries, almost always geometric transformations such as scaling, rotation or skewing are needed. Geometric transformations typically require a resampling and interpolation step. Thus, having available sophisticated resampling/interpolation detectors is very valuable.

DETECTING NEAR DUPLICATED IMAGE REGIONS

In a common type of digital image forgery, called copy–move forgery, a part of the image is copied and pasted into the another part of the same image, typically with the intention to hide an object or a region. The copy–move forgery brings into the image several near–duplicated image regions.

NOISE INCONSISTENCIES ANALYSIS

A commonly used tool to conceal traces of tampering is addition of locally random noise to the altered image regions. This operation may cause inconsistencies in the images noise. Therefore, the detection of various noise levels in an image may signify tampering.

FREE FORENSICS INVESTIGATION TOOLS FOT IT EXPERTS

AUTOPSY

Autopsy is a GUI-based open source digital forensic program to analyze hard drives and smart phones efficiently. Autopsy is used by thousands of users worldwide to investigate what happened in the computer.

It's widely used by corporate examiners, military to investigate and some of the features are.

- **Email analysis**
- **File type detection**
- **Media playback**
- **Registry analysis**
- **Photos recovery from memory card**
- **Extract geolocation and camera information from JPEG files**
- **Extract web activity from browser**
- **Show system events in graphical interface**
- **Timeline analysis**
- **Extract data from Android – SMS, call logs, contacts, etc.**

It has extensive reporting to generate in HTML, XLS file format.

Encrypted Disk Detector

Encrypted Disk Detector can be helpful to check encrypted physical drives. It supports TrueCrypt, PGP, BitLocker, Safe boot encrypted volumes.

WIRESHARK

Wireshark is a network capture and analyzer tool to see what's happening in your network. Wireshark will be handy to investigate network related incident.

MAGNET RAM CAPTURE

You can use Magnet Ram Capture to capture the physical memory of a computer and analyze artifacts in memory. It supports Windows operating system.

NETWORK MINER

An interesting network forensic analyzer for Windows, Linux & MAC OS X to detect OS, hostname, sessions and open ports through packet sniffing or by PCAP file. Network Miner provides extracted artifacts in an intuitive user interface.

NMAP

NMAP (Network Mapper) is one of the most popular networks and security auditing tools. NMAP is supported on most of the operating systems

including Windows, Linux, Solaris, MAC OS, HP-UX, etc. It's open source so free.

RAM CAPTURER

Ram Capturer by Belkasoft is a free tool to dump the data from computer's volatile memory. It's compatible with Windows OS. Memory dumps may contain encrypted volume's password and login credentials for webmails and social network services.

FORENSIC INVESTIGATOR

If you are using Splunk, then Forensic Investigator will be a convenient tool. It's Splunk app and has many tools combined.

- **WHOIS/GeoIP lookup**
- **Ping**
- **Port scanner**
- **Banner grabber**
- **URL decoder/parser**
- **XOR/HEX/Base64 converter**
- **SMB Share/NetBIOS viewer**
- **Virus Total lookup**

FAW

FAW (Forensics Acquisition Of Websites) is to acquire web pages for forensic investigation which has the following features.

- **Capture the entire or partial page**
- **Capture all types of image**
- **Capture HTML source code of the web page**
- **Integrate with Wireshark**

HASHMYFILES

HashMyFiles will help you to calculate the MD5 and SHA1 hashes. It works on almost all latest Windows OS.

USB WRITE BLOCKER

View the USB drives content without leaving the fingerprint, changes to metadata and timestamps. USB Write Blocker use Windows registry to write-block USB devices.

CROWD RESPONSE

Response by Crowd Strike is a windows application to gather system information for incident response and security engagements. You can view the results in XML, CSV, TSV or HTML with the help of CRConvert. It runs on 32 or 64 bit of Windows XP above.
Crowd Strike has some other helpful tools for investigation.

- **Totrtilla – anonymously route TCP/IP and DNS traffic through TOR.**
- **Shellshock Scanner – scan your network for shellshock vulnerability**
- **Heartbleed scanner – scan your network for OpenSSL heart bleed vulnerability.**

NFI DEFRASER

Defraser forensic tool may help you to detect full and partial multimedia files in the data streams.

EXIFTOOL

ExifTool helps you to read, write and edit meta information for a number of file types. It can read EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, Photoshop IRB, FlashPix, etc.

TOOLSLEY

Toolsley got more than ten useful tools for investigation.

- **File signature verifier**
- **File identifier**
- **Hash & Validate**
- **Binary inspector**
- **Encode text**
- **Data URI generator**
- **Password generator**

SIFT

SIFT (SANS investigative forensic toolkit) workstation is freely available as Ubuntu 14.04. SIFT is a suite of forensic tools you need and one of the most popular open source incident response platform.

DUMPZILLA

Extract all exciting information from Firefox, Iceweasel and Seamonkey browser to be analyzed with Dumpzilla.

BROWSER HISTORY

1. **Browser history capturer – capture web browser (chrome, firefox, IE & edge) history on Windows OS.**
2. **Browser history viewer – extract and analyze internet activity history from most of the modern browsers. Results are shown in the interactive graph, and historical data can be filtered.**

FORENSIC USER INFO

Extract the following information with ForensicUserInfo.

- **RID**
- **LM/NT Hash**
- **Password reset/Account expiry date**
- **Login count/fail date**
- **Groups**
- **Profile path**

BLACK TRACK

Blacktrack is one of the most popular platforms for penetration testing, but it has forensic capability too.

PALADIN

PALADIN forensic suite – the world's most famous Linux forensic suite is a modified Linux distro based on Ubuntu available in 32 and 64 bit.

SLUETH KIT

The Sleuth Kit is a collection of command line tools to investigate and analyze volume and file systems to find the evidence.

CAINE

CAINE (Computer Aided Investigate Environment) is Linux distro that offers the complete forensic platform which has more than 80 tools for you to analyze, investigate and create an actionable report.

ANTIFORENSICS

Anti-forensics is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found you.

FORENSICS VS ANTIFORENSICS

- **Computer Forensics: "Scientific knowledge for collecting, analyzing, and presenting evidence of the court". (USCERT 2005) .**
- **Anti-Forensics: Tools and techniques that frustrate forensic tools, investigations and investigators.**

GOALS OF ANTIFORENSICS

- **Avoiding Detection**
- **Disrupting Information Collection**
- **Increasing the examiners time**
- **Casting doubt on a forensic report or testimony**

ANTIFORENSICS TECHNIQUE

- **Subverting the tool – Using it to attack the examiner or organization.**
- **Leaving no evidence that the AF tool has been run.**
- **Overwriting: Eliminate data or metadata**
- **Disk sanitizers; Free space**
- **Sanitizers; File Shredders**
- **Microsoft Remove Hidden Data Tool; CCleaner Metadata Erasers**

Examples: Timestamp

LIVE CD

A live CD is an operating system that is packaged on CD or DVD and does not require the use of a traditional hard drive to operate. Unlike traditional operating system that use hard drives to store data, live CD's place all information within the computer's volatile memory (RAM).

Example: tails.boum.org

VIRTUAL MACHINE

Virtual machine is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionally of a physical computer. Their implementations may involve specialized hardware, software or a combination.

Example: www.virtualbox.org

ENCRYPTION

Encryption is the act of turning data into code, intended to prevent access from unauthorized users. Many tools aid with this, some of which reside right on a new version of Windows.

Some of these tools include VeraCrypt, Acrypt, BitLocker, and GNU Privacy Guard.

CHANGING METADATA & TIMESTAMPS

Metadata and timestamps can be manipulated to an attacker's benefit.

Forensic examiners may be able to compile a timeline of an attacker's activity and areas of interest with this information. However, overwriting metadata prevents this. The use of timestamps can also overwrite timestamps and delete entries, making an examiners job more difficult.

ONION ROUTING

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, this allowing both organizations and individuals to share information over public networks without compromising their privacy.

Example: www.torproject.org