Digital Forensics Short Course

Module 1: Introduction to digital forensics

OUTLINE:-

- INtroduction to digital Forensics
- Selected Topics from ITC597
- Introduction to forensic tools

Digital forensics - definition

The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.

Digital Forensics - NIST defination

Digital Forensics - NIST definition

• The application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatabilitu, reporting, and possibly expect testimony
• The application of science to the identification, collection, examination, and analysis, of daya while preserving the integrity of the information and maintaining a strict chain of custody for the data

* National Insititute of standards of technology: https://www.nist.gov

What you need to be a successful digital forensics practitioner?

What you need to be a successful digital forensics practitioner?

• Lots of Knowledge about computers, technology (contemporary and legacy)
• Professional conduct
• Common-sense
• Ability to think outside the box

• Attention to detail
• Persistence

Maintaining Professional Conduct

Maintaining Professional Conduct

• Professional conduct - includes ethics, morals, and standards of behavior
• An investigator must exhibit the highest level of professional behavior at all times
  ◇ Maintain Objectivity
  ◇ Maintain credibility by maintaining confidentiality
• Traning to update skills - Investigators should also attend tranings to stay current with the latest technical changes in computer hardware and software, networking, and forensic tools

Digital Forensics Roadmap

Digital Forensics Roadmap

Typically 8 steps in the roadmap:

1. Search authority (Search warrant or an authorisation letter (in case of corporate investigations))
2. Chain of custody
3. Imaging / hashing function (Golden step)
4. Validated tools
5. Analysis
6. Repeatability (Quality Assurance)
7. Reporting
8. Possible expert presentation

Digital Forensics vs Other Disciplines

Digital forensics VS Other Disciplines

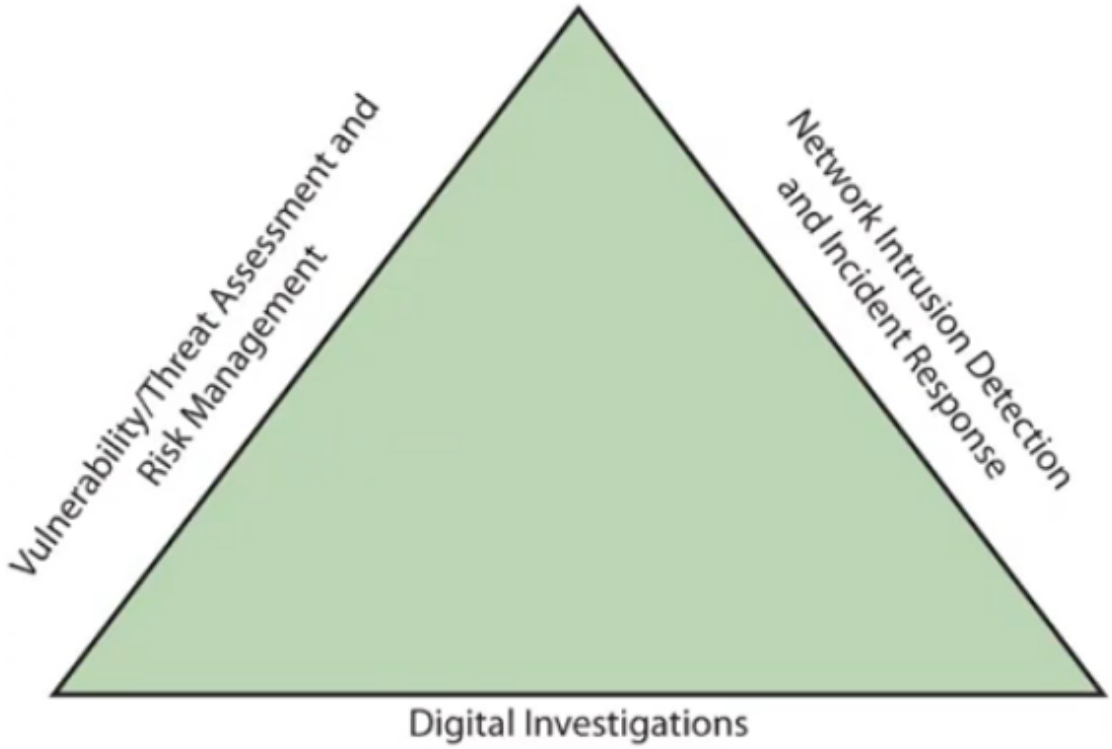


Figure 1-1 The investigations triad

Developing Digital Forensics Resources

Developing Digital Forensics Resources

• You must know more then one computing platform
  ◇ Such as DOS, Windows 9x, linux, Macintish, and current windows platforms
• you also must be familiar with new technologies e.g. cloud, social media, smart devices etc

• join as many computer user groups as you can
  ◇ Australian Information Security Association (AISA) (https://www.aisa.org.au/)
  ◇ Forensics Focus (https://forensicfocus.com)
  ◇ Magnet Forensics (magnetforensics.com) - Look for their whitepapers under resources
  ◇ High Tech Crime Group (https://htcia.org/)

• Exchanges information about techniques related to computer investigations and security
• User groups can be helpful
• Build a netword of computer forensics experts and other professionals
• and keep in touch through emails / OSNs
• Get professional certifications such as CISSP (certified information system security professional)
  ◇ https://www.isc2.org/Certifications/CISSP

Types of Digital Investigations

Types of Digital Investigations

☐ Digital investigations and forensics falls into two categories
  ☐ public investigations
  ☐ private or corporate investigations

• Public investigations
  ◇ Involve government agencies responsible for criminal investigations and prosecution
  ◇ Search warrents are required

• Private or corporate investigations
  ◇ Deal with provate companies, non-law-enforcement government agencies, and lawyers
  ◇ Are not governed directly by criminal law mostly, but can end up as a criminal investigation
  ◇ Governed by internal policies of an organisation that define expected employee behavior and conduct in the workplace

Investigations (some definitions)

Understanding Law Enforcements Agency
Investigations (some definitions)

• Digital Evidence First Responder (DERF)
  ◇ Arrives on an incident scene, assesses to situation, and take precautions to acquire and preserve evidence.
• Digital Evidence Specialist (DES)
  ◇ Has the skill to analyze the data and determine when another specialist should be called in to assist.
• Affidavit
  ◇ A swrom statement of support of fact about or evidence of a crime. Must include exhibits that supports the allegation.

Understanding Law Enforcements Agency Investigations

Understanding Law Enforcements
Agency Investigations

In a **criminal case**, a suspect is trailed for a criminal offense
  - such as burglary, murder, or molestation.

Computers are networks are only tools that can be used to commit crimes
  - Many states have added specific language to criminal codes to define crimes

involving computers.

Following the legal process
- Legal processes depends on local custom , legislative standards, and rules of evidence.

Following are the legal process
• A criminal case begins when someone finds evidence of an illegal act
• Complainant makes an **allegation**, an accusation or supposition of fact
• A police officer interviews the complainant and writes a report avout the crime
• Investigators delegate, collect and process the information relates to the complaint

Understanding Corporate Investigations

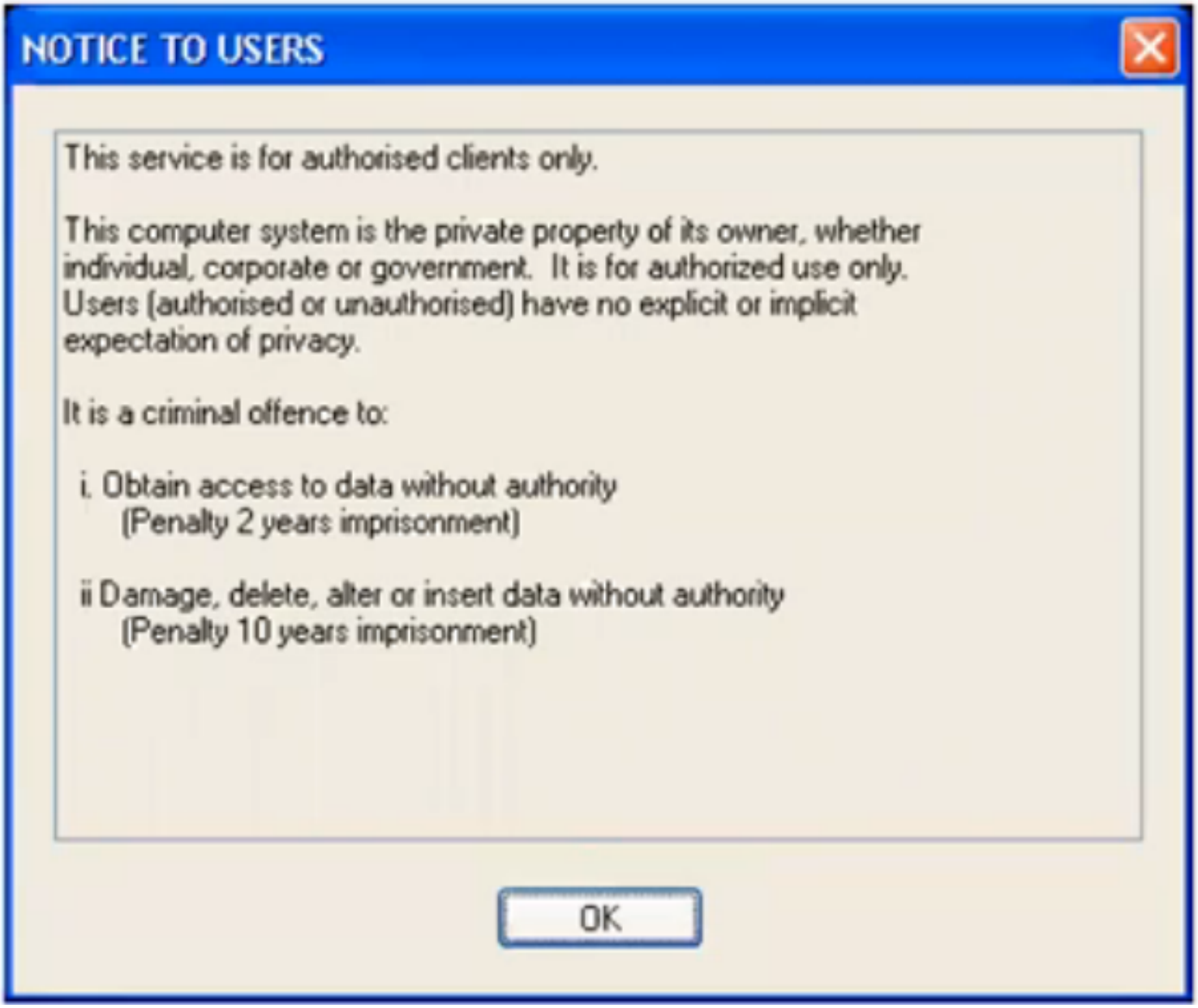
Understanding Corporate Investigations

• **Private or corporate investigations**
◇ Involves private companies and lawyers who address company policy violations and litigation disputes

• **Corporate computer crimes can involve:**
◇ E-mail harassment
◇ Falsifications of data
◇ Gender and age discrimination
◇ Embezzlement
◇ Sabotage
◇ Industrial espionage

• **Estabishing company policies**
• One way to avoid litigation is to publish and maintain policies that employees find easy to read and follow
• Published company policies provide a line of authority
◇ for a business to conduct internal investigations
• Well-defined polices
◇ Give computer investigators and forensic exminers the authority to conduct an investigation

for example, business can avoid litigation by displaying a **warning banner** computer screens
• Informs end users that organization reserves that right to inspect computer systems and network traffic at will



Designating an authorized requester

- **Authorized requester** has the power to conduct investigations
- policy should be defined by executive management
- Groups that should have direct aurthority to request computer investigations
  - ◇ Corporate Security Investigations
  - ◇ Corporate Ethics Office
  - ◇ Corporate Equal Employment Opportunity Office
  - ◇ Internal Auditing
  - ◇ The gernal counsel or legal Department

Condicting security investigations

- Types of situtions
  - ◇ Abuse or misuse of corporate assets
  - ◇ E-mail abuse
  - ◇ Internet abuse
- Be sure to distinguish between a company's abuse problems and pontential criminal problems
- What happnes when a civilian or corporate investigative agent delivers evidence to a law enforcement officer

Distinguishing personal and company property
• Many company policies distinguish between personal and company computer property
• One aera that's difficult to distinguish involves BYOD's: mobile phones, tablets and personal notebook computers
• The safe policy is to not allow any personally owned devices to be connected to company-owned resources
  ◇ Limiting the possibility of commingling personal and company data

Some useful forensics tools for learning

Some useful forensics tools for learning

• Autopsy:- https://www.sleuthkit.org/autopsy/
• OSForensics:- https://www.osforensics.com/index.html
• WinHex:- https://www.x-ways.net/winhex/
• FTK Imager Liter:- https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

Module 2: Data Acquisition

Outline

• Data acquisition introduction
• Data storage formats
• Data acquisition methots
• Determining the best data acquisition method
• Data acquisition from new platforms
• Data validation (hashing functions / algorithms)

Data storage formats for digital evidence

Data storage formats for digital evidence

Three data storaeg formates for digital evidence:

1. Raw format
2. Proprietary formats
3. Advanced Forensics Format (AFF)

Types of data Acquisition

Three types of data acquisition

1. Static acquisition
2. Live acquisition
3. Logical acquisition and/or sparse acquisition

Static Acquisition Method

1. Static Acquisition Method

• Typically, a atatic acquisition is done on a computer sezied during a police raid
• Static acquisitions are always the preferred way to collect digital evidence
• you have already acquired the system, know the passwords if any, and are only interested in data on storage media such as hard disks, flash drives etc
• Static acquisition does not provide a clear picture of the running system, e.g. you may be interested in RAM contents, or the web browser contents at a particular instant of time

Live Acquisition Methods

Live Acquisition Methods

Performing Live Acquisition:

when is it required/important to perform live acquisition?

• when you are dealing with active network intrusions and attacks or if you suspect employees are accessing network areas they shouldn't
• When you think that attackers may wipe-off evidence if the system goes offline
• information in RAM is lost after you turn off suspect system.
• When you don't know the password of the system.

Steps required to perform a live acquisition:

1. Create or download a bootable forensic CD or USB drive
2. Make sure you keep a log of all your actions
3. A network drive is ideal as a place to send the information you collect
4. Copy the physical memmory (RAM)
5. The next step varies, depenfing on the incident you're investigating, for example, with instrusion you might want to see wheather a rootkit exixts. You can also access the system's firmware to see wheather it has changed, create an image of the drive over network, or shut down the system and make a atatic acquisition later.
6. Be sure to get a forensic digital hash of all files you recover during the live acquisition.

Logical or sparse acquisition

Logical or spaese acquisition

1. can be done during atatic or live acquisition

2. collecting evidence from large drives can take several hrs; if your time is limited, use logical or spare acquisition
3. Use this method when you do not need to exmine the entire drive
4. Logical acquisition captures only spacific files of interest to the case
5. Sparse acquisition collects fragments of unallocated (deleted) data
6. For large disks
7. For example, for e-mail investigation you will only need .pst or .ost files

Determining the best acquisition method

Determining the best acquisition method

For any type of acquisition, data can be collected with four methods.

1. Creating a disk-to-image file
2. Creating a disk-to-disk
3. Creating a logical disk-to-disk or disk-to-data file
4. Creating a spare data copy of a file or folder

Determining the best method depends on the circumstances of the investigation

Creating a disk-to-image file

Creating a disk-to-image file

• Most common method and offers most flexibility
• Should make more than one copy - more the better!
• copies are bit-for-bit replications of the original drive
• ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLooklX

Creating disk-to-disk

Creating disk-to-disk

• When disk-to-image copy is not possible
• Tools can adjust disk's geometry config
• EnCase, SafeBack, SnapCopy

When making a copy, consider

When making a copy, consider

• Size of the source disk
  ◇ Lossless compression might be useful
  ◇ Use digital signatures for verification

• When working with largr drive's an altervative is using lossless compression
  ◇ Whether you can retain the disk
  ◇ Time to perform the acquisition
  ◇ Where the evidence is located

Data acquisition from new & emerging platforms

Data acquisition from new & emerging platforms

☐ Data acquisition from clouds

  ☐ digital investigators should firstly locate relevant Cloud's data centers
  ☐ Legal and technical challenges related to cloud Service provider (CSP)

☐ Data acquisition from Online Social Networks (OSNs)

☐ Data acquisition from smart Phones

  ☐ it can include acquiring messages, phone, contacts, images / videos stored in smart phones, web browsing history, OSN related data etc

Contingency planning for image acquisitions

Contingency planning for image acquisitions

• Create a duplicate copy of your evidence image file

• Make atleast two images of digital evidence
  ◇ Use different tools or techniques

• Copy **host protected area (HPA)** of a disk drive as well
  ◇ Consider using a hardware acquisition tool that can access the drive at the BIOS level

• Be prepared to deal with encrypted drives
  ◇ **Whole disk encryption** feature in Windows called BitLocker makes static acquisition more dissicult
  ◇May require user to provide decryption key

Hashing the data

Hashing the data

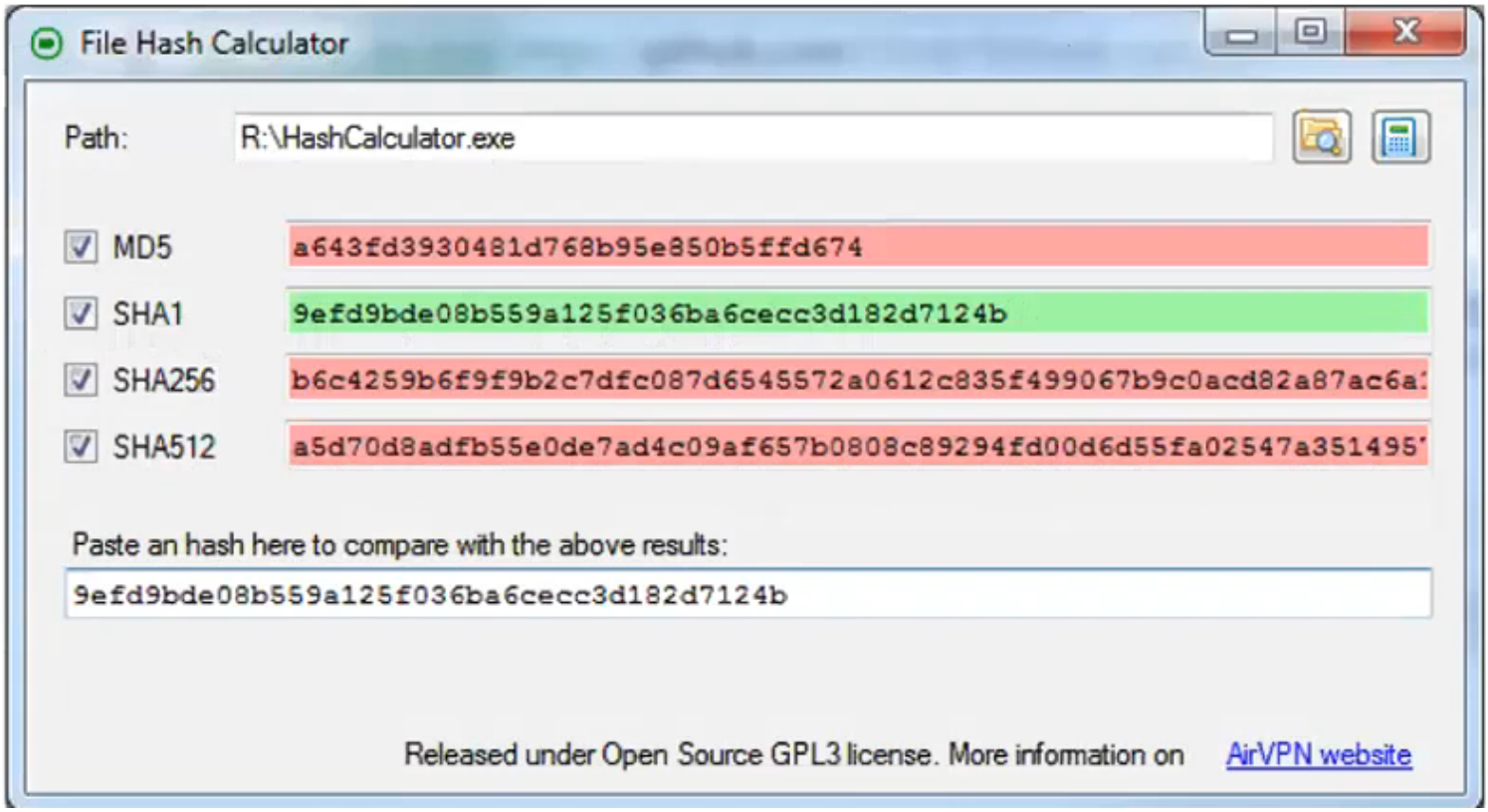
• Ensuring the integrity of data collected is essential for presenting evidence in court
• Most forensic tools offer hashing of image files

• Explain - Autopsy's hashing freature
• Using advanced hexadecimal edioters ensure data integrity
• Raw formate image files don't contain metadata
• Separate manual validation is recommended for all raw acquisitions

Validating data acquisitions

Validating data acquisitions

• Validating evidence may be the most critical aspect of computer forensics
• Requires using a hashing algorithm/function
• A hashing algorithm is a mathematical function that calculates a fix lenght output
  ◇ CRC-32, MD5, and SHA-1 to SHA-512



Performing RAID data acquisitions

Performing RAID data acquisitions

Acquisitions of RAID (Redundant Array of Independent Disk) drives can be challenging and frustrating because of how RAID systems are
• Designed
• Configured
• Sized

Size is the biggest concern
• Many RAID systems now have terabytes of data

Remote network acquisition tools

Remote network acquisition tools

• You can remotely connect to a suspect computer via a network connection and copy data from if
• Remote acquisition tools vary configurations and capabilities

• Drawbacks
  ◇ Antivirus, antispyware, and firewall tools can be config to ignore remote access programs
  ◇ Suspects could easily install their own security tools that trigger an alarm to notify them of remote access intrusions

Validating with hexadecimal editors

Validating with hexadecimal editors

• Advanced hex edioters offer features not avaliable in some digital forensics tools such as: Hashing specific liles or sectors

• With the hash value in hand
  ◇ you can use a forensics tool to search for a suspicious file that might have had its name changes to look like a safe file

• WinHex provides MD5 and SHA-1 hashing algorithms

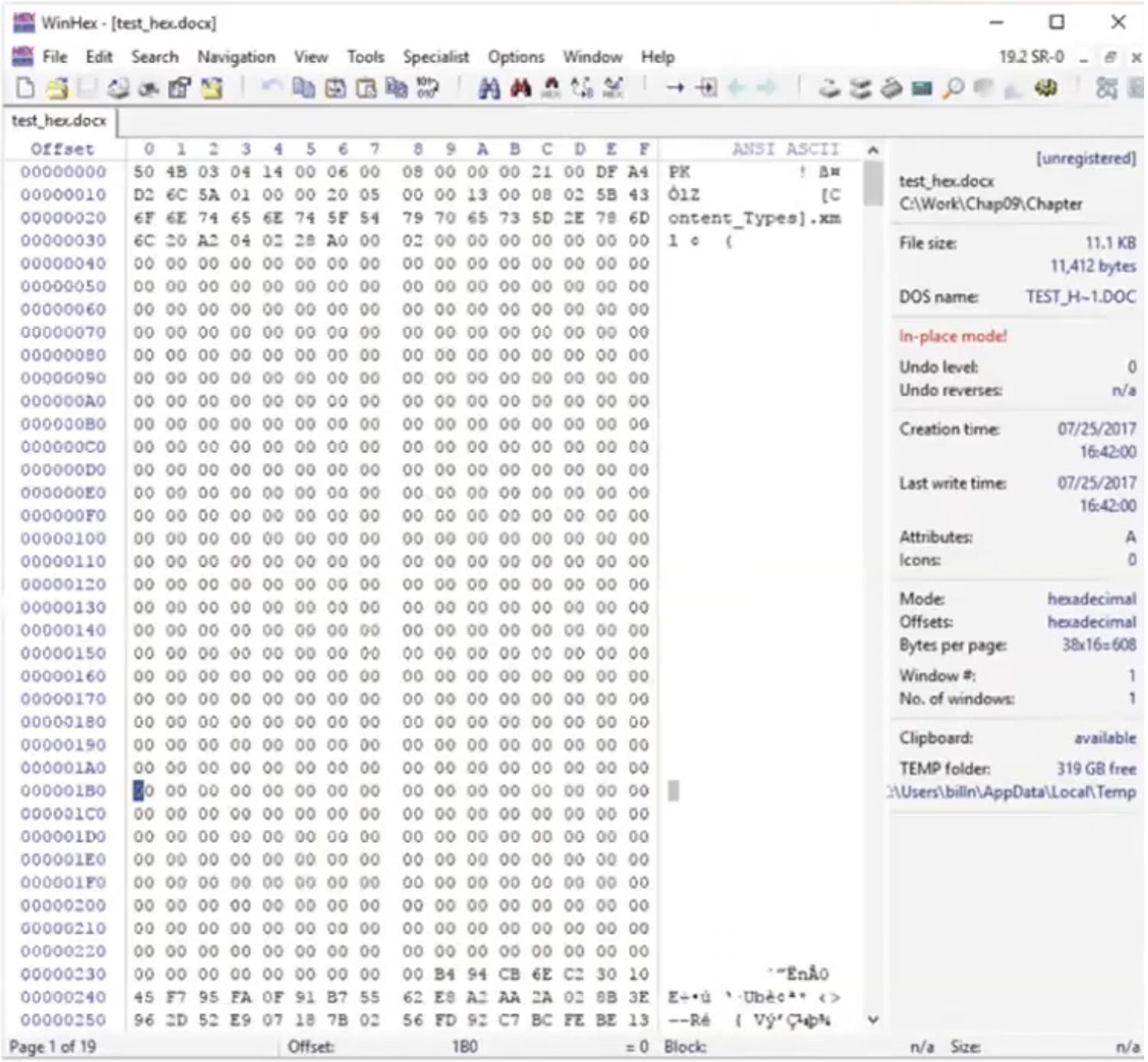


Figure 9-10 Viewing a file opened in WinHex

Source: X-Ways AG, *www.x-ways.net*

Using acquisition tools

Using acquisition tools

Acquisition tools for Windows
- Advantages
  - ◇ Make acquiring evidence from a suspect drive more convenient
    - ■ Especially when used with hot-swappable devices

- Disadvantages

◇ Must protect acquired data with a well-tested write-blocking hardware device
◇ Tools can't acquire data from a disk's host protected area
◇ Some contries haven't accepted the use of write-blocking device for data acquisitions

Mini-WinFE

Mini-WinFE

Mini-WinFE
◇ Enables you to build a Windows forensic boot CD/DVD or USB drive so that connected drives are mounted as read-only

Before booting a suspect's computed:
◇ Connect your target drive, such as a USB drive

After Mini-WinFE is booted
◇ You can list all connected drives and alter your target USB drive to read-write mode so you can run an acquisition program

Capturing an image with AccessData FTK Imager Lite

Capturing an image with AccessData FTK Imager Lite

• Included with AccessData Forensic toolkit
• Designed for viewing evidence disk and disk-to-image files
• make disk-to-image copies of evidence drives
◇ At logical partition and physical drive level
◇ can segment the image file
• Evidence drive must have a hardware write-blocking device
• Or run from a live CD, such as Mini-WinFE

Approaching digital forensics cases

Approaching digital forensics cases

Following these basic steps for all digital forensics investigations:
1. For target drives, use recently wiped media that have been reformatted and inspected for viruses
2. Inventory that hardware on the suspect's computer, and note condition of seized computer

3. For static acquisitions, remove original drive and check the date and time values in system's CMOS
4. Record how you acquired data from the suspect drive
5. process drive's contents methodically and logically

Module 3: Digital Forensics Contexts

Topics

☐ OS and file systems
☐ Virtual platforms
☐ E-mail and social media

File Syatems

File Systems

• The purpose and structure of OS file systems
• Understanding and analysing Windows OS file structure
  ◇ Clusters and Disk Partitioning
  ◇ FAT (File Allocation Table) file system
  ◇ NTFS (Windows NT) file system

The purpose and role of file systems

The purpose and role of file systems

• A file system is merely a system of organising and storing files in a logical structure.
• Type of file system an OS uses determines how data is stored on the storage of choice.
• Forensics investigatators should understand how data is stored and managed in various OS.
• When investigating you should be familiar with both the OS and file Systems.

Digital Forensics Related File Systems Attributes

Digital Forensics Related File Systems Attributes

☐ As a digital forensics investigator, you may be interested in the following file / file system

attributes

◇ File creation/modification/deletion and associated details re time/date etc.
◇ Sudden file growth
◇ file replacement
◇ Archive
◇ Hiddne
◇ Read only
◇ Compression

Physical Structure of Hard Disk Drives

Physical Structure of Hard Disk Drives

• Most commonly used storade devices are hard disk drives (HDDs)
◇ made up of one or more plates coated with magnetic material

• Disk drives components
◇ Geometry - refers to disk's logical structure of platters, tracks, and sectors
◇ Head - is the device that reads and writes data to a drive, There are two heads per platter that read and write the top and bottom side
◇ Tracks - are concentric circles on a disk platter where data is located
◇ Cylinders - is a column of tracks on two or more disk platters
◇ Sectors - is a section on a track, usually made up of 512 bytes.

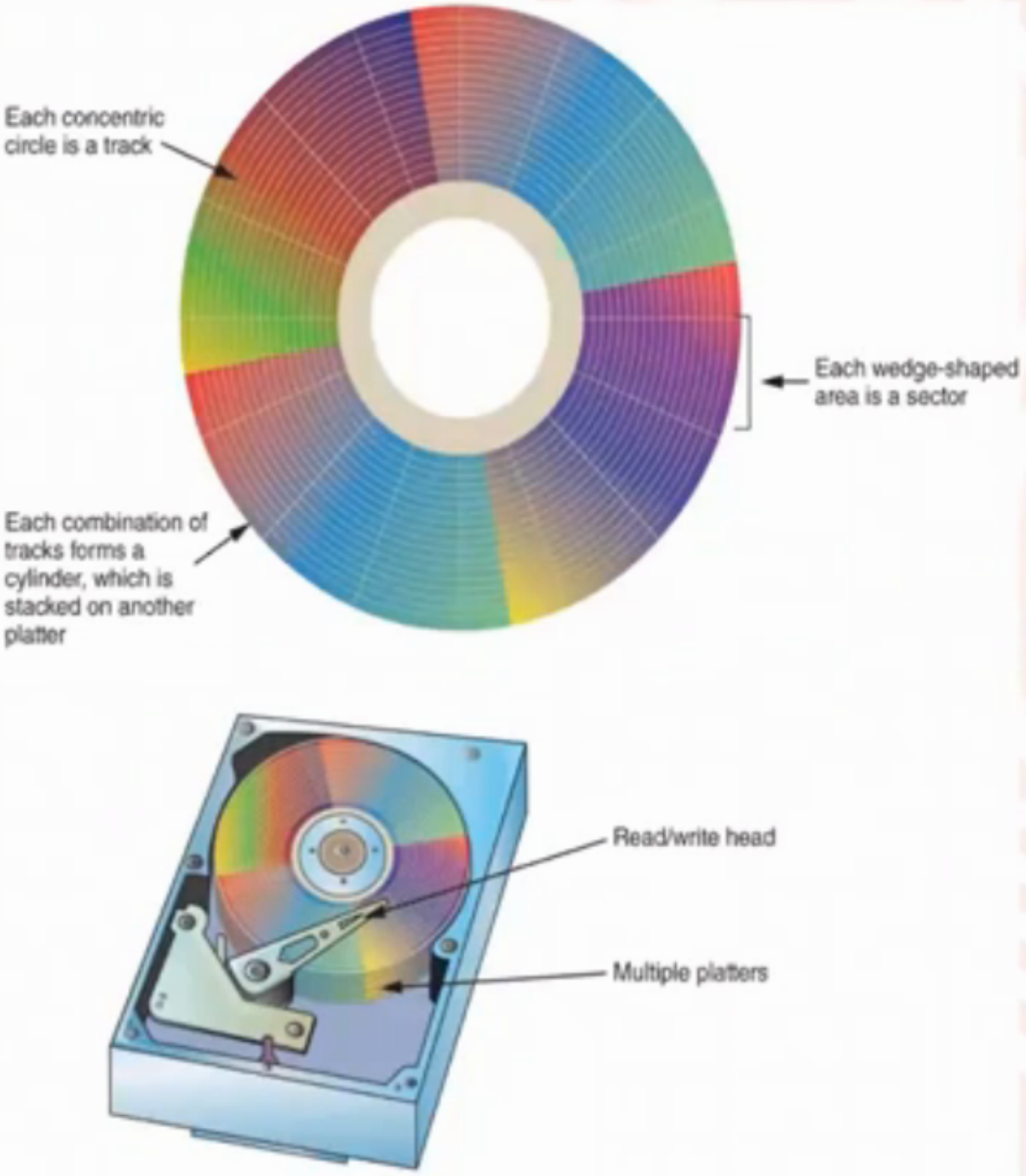


Figure 5-2 Components of a disk drive

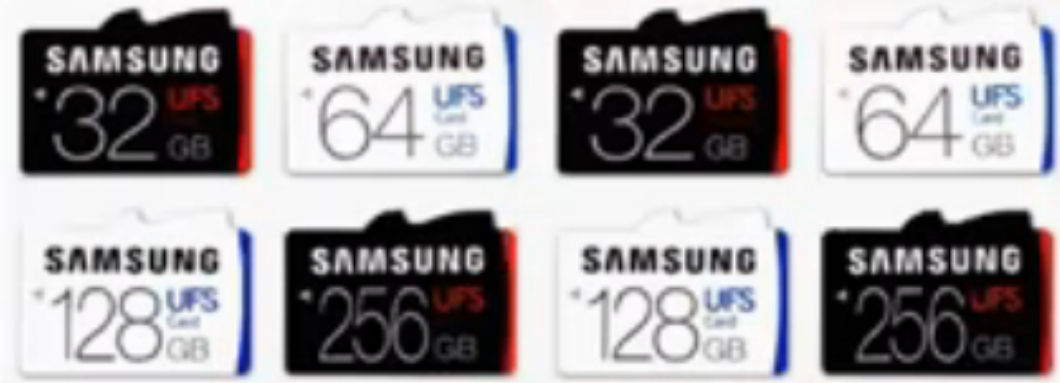
Solid-State Storage Devices (SSDs)

Solid-State Storage Devices (SSDs)

• Flash memory storage devices used in USB devices, laptops, tablets and cell phones.
• can be a challenging for digital forensics exminers because if delated data is not recoverd immediately, it can be permanently lost.
  ◇ This lost of data is due to a feature all flash memory devices have called ware-levelling that ensures even ware of read/writes for all memory cells.
• When dealing with solid-state devices, making a full forensic copy as soon as possible.
  ◇ Assists when recovering data from unallocated disk space.
• For mobile devices forensics, this feature is extremely important in some circumstances.
  ◇ e.g. a suspect deletes incriminating messages before the device is seized.


RS MMC
512
512
256
128
512 MB
Solid State Devices


Extreme
SanDisk


SAMSUNG
32 GB UFS
SAMSUNG
64 GB UFS
SAMSUNG
32 GB UFS
SAMSUNG
64 GB UFS
SAMSUNG
128 GB UFS
SAMSUNG
256 GB UFS
SAMSUNG
128 GB UFS
SAMSUNG
256 GB UFS

Microsoft File Structure

Microsoft File Structure

• Most **commonly** used OS and file system.
• Important to understand the concept of clusters, and the two main variants of the file systems used: **FAT, NTFS**
• The file system used determines where hidden data can be reside.
  ◇ Finding the data is key for any forensics investigator.
• Explore these hidding places to determine whether they contain files or files fragments that might be evidence of a crime or policy violation.

Sectors and clusters

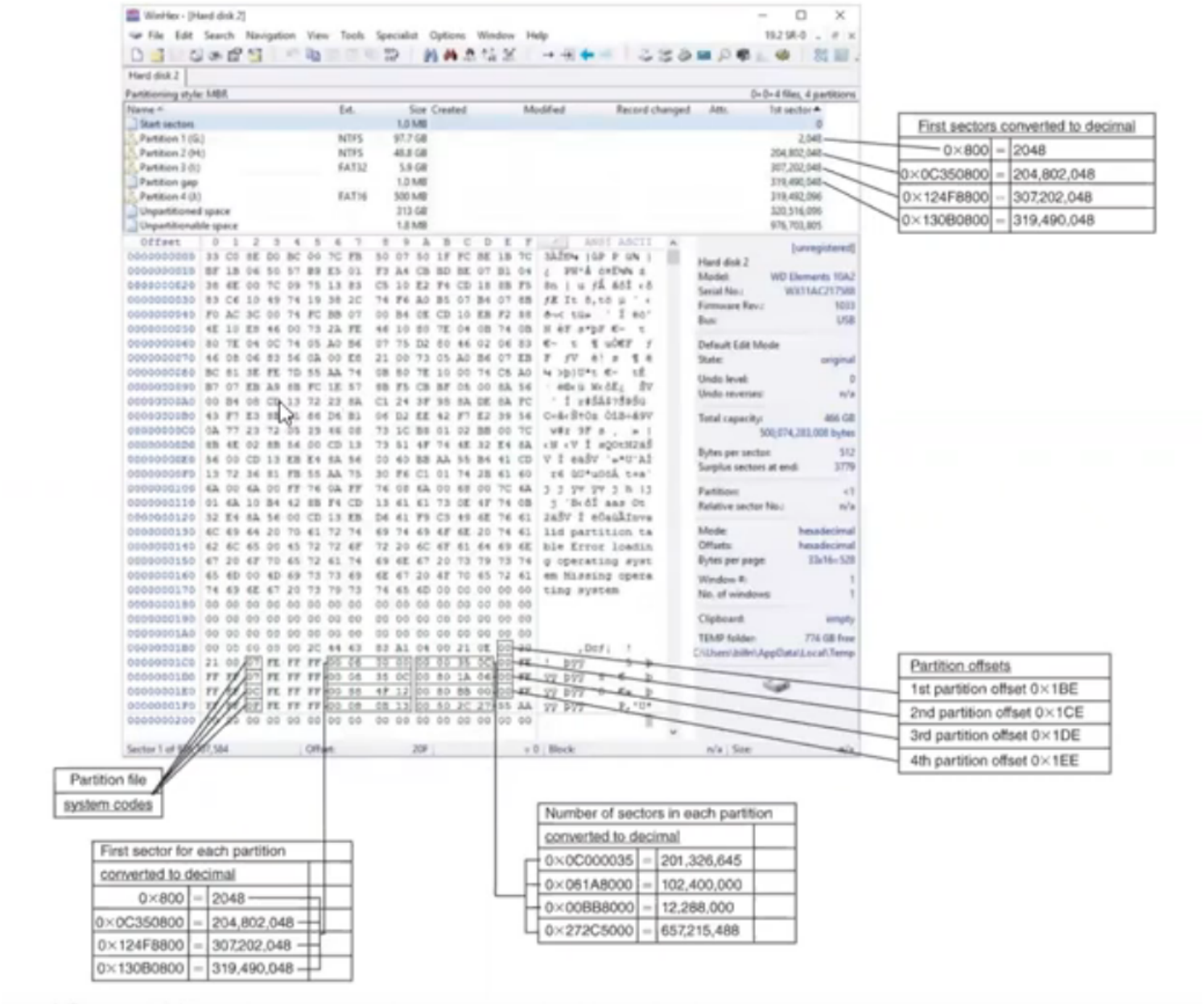
Sectors and Clusters

• A sector is the smallest physical data storage unit on the disk.
• Size of a cluster -512 bytes or more(always exponent of 2), e.g. 512 is 2 powrers to 9, 1024 is 2 powers to 10 and so on.
• Sectors indetifies data is written to the area immeditately before the contents of the sectors and identifies the starting address of the sector.
• In MS file system a cluster is a group of sectors. A cluster can consist of one or more consecutive(contiguous) sector. The # of sectors is always an expinent fo 2.
• Clusters and numbered sequentially starting at 0 in NTFS and 2 in FAT.

Disk Partitions

Disk Partitions

• Many hard disks are logically divided into 2 or more sections - where each logical division is known as a partition.
• Winsows OS can have three primary partition followed by an extended partition that can contain one or more locical drives.
• Hidden partitions or voids - large unsed gaps between partitions on a disk
• The partitions table is in the Master Boot Record (MBR)
  ◇ holds the information about disk partitions, start/end of a disk partition, supports up to four primary partitions.
• In WinHex, you can see first partition starts at offset value 0x1BE, second partition starts at 0x1CE, third partition starts at 0x1DE and fourtg partition starts at 0x1EE.



FAT (File Allocation Table) File System

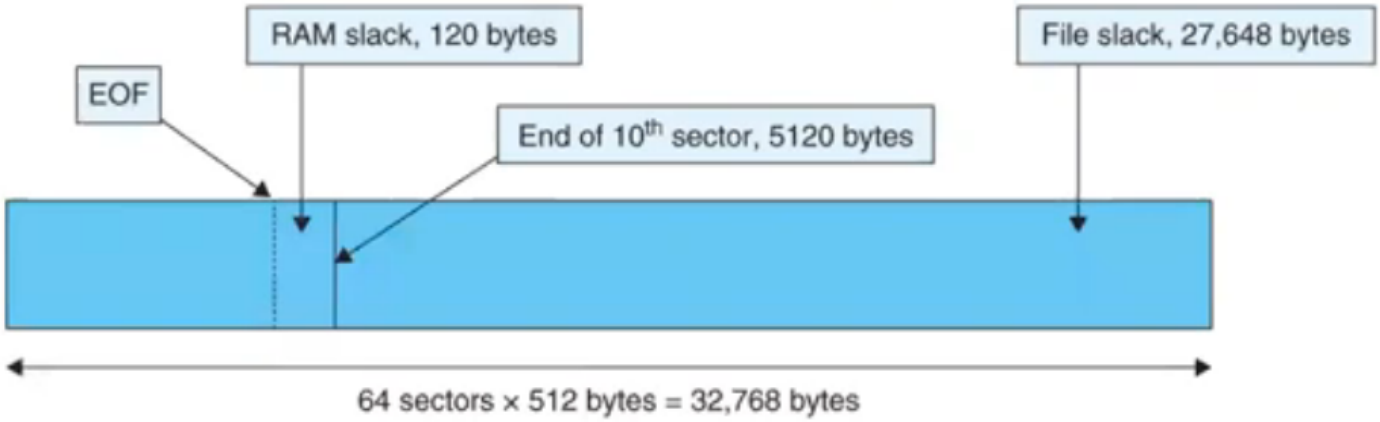
FAT (File Allocation Table) File System

• Simple, low overhead, file strecture that MS originally designed for floppy disks.
• FAT database is typically written to a disk's outermost track and containd:
  ◇ Filename, directory name, date and time stamps, the starting cluster number, and file attributes.
• Three current versions:
  ◇ FAT16.
  ◇ FAT32 (can access disks larger than 2gb; can be used with newer Windows OS).
  ◇ exFAT (used for mobile personal storage devices).
• Three old versions:
  ◇ FATX.
• Virtual FAT (VFAT).
• FAT12.

Examining FAT Disks

Examining FAT Disks

• Microsoft OS allocated disk space for files by clusters.
• Resukts in drive slack.
  ◇ Unsend space in cluster between the end of an active file's content and the end of the cluster
• Drive slack includes RAM slack and file slack.
• An unintentional side effect of FAT16 allowing larg clusters was that it reduces fragmentation.
  ◇ As cluster size increased.



Windows NT File System (NTFS)

Windows NT File System (NTFS)

• New Technology file system(NTFS).
  ◇ introduced with Windows NT in early 1990s.
  ◇ primary file system for current MS OS.
• Improvements over FAT file systems.
  ◇ Additional file information.
  ◇ Better security restrictions over files/folders.
• MS stratregic move toward a journaling file system
  ◇ Records transactions before the system carries it out.
  ◇ NTFS log any transation that alters important file system data structures.
    ■ This is done before operations are written to disk and ensures when the system crashes, partial transactions can be recoverd.

Some Features of NTFS

Some Features of NTFS

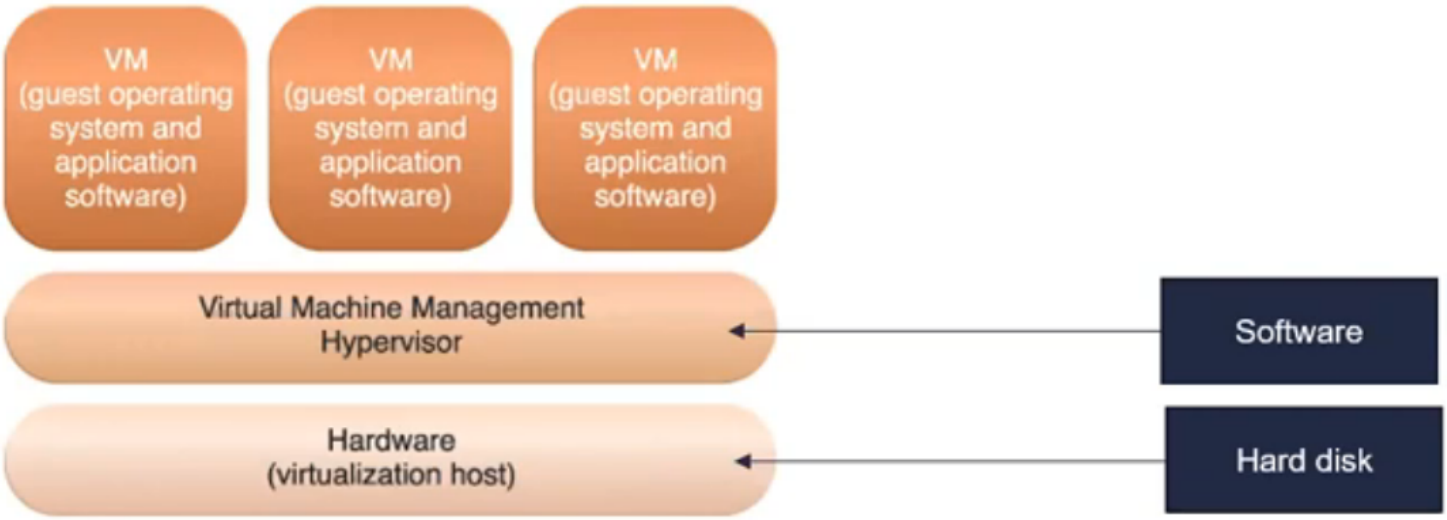
- In NTFS, everything written to the disk is considered a file.
- On an NTFS disk
  - ◇ First data set is the partition BOOT SECTOR.
  - ◇ Next is Master File Table(MFT).
- NTFS results in much less file slack space.
- Clusters are smaller for smaller disk drives.
- NTFS also uses Unicode.
  - ◇ An internartional data formate.
  - ◇

Virtual Platforms

Virtual Platforms

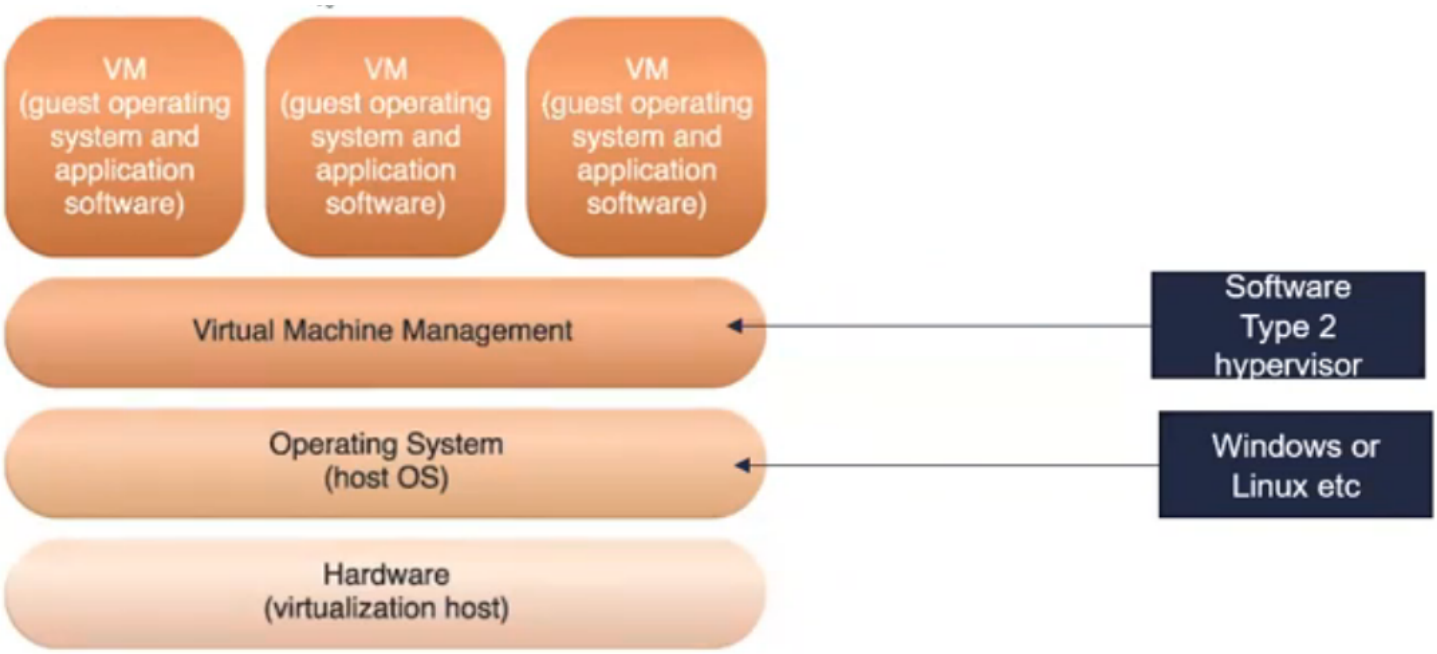
Virtualisation Concepts

- Hardware-Based Virtualisation (Type 1 hypervisor)



- No requirement for a host OS.

- Operating system-based virtualisation (type 2 hypervisor).



• Requires a host OS.

Hypervisors

Hypervisors

• Software that runs virtual machine is called the ‘hypervisior’.
• Two types of hypervisors.
  ◇ Type 1 Hypervisors (No OS).
    ■ Usually installed on server or workstations with copious RAM and storeage.
    ■ E.g. VMware vSphere, IBM PowerVM,
  ◇ Type 2 Hypervisors (Required OS).
    ■ Most likely to be found on suspect machines.
    ■ E.g. Microsoft Hyper V, VMware Workstation, VirtualBox.
    ■ Come with templates for different OS.

VM Investigation

VM Investigation

• Acquire a forensic image of the host computer and abtain network logs.
  ◇ Link the VM's IP address to log file and determine what web site the VM accessed.
• To detect whether a VM is on a host computer:
  ◇ Look in the Users or Documents folders (in windows).
  ◇ Check the host's registry for clues that VM's have been installed or not.
  ◇ Existence of a virtual network adapter.
• Determine whether USB drivers have been attached to the host.
  ◇ They could have live VM's running on them.
• A VM can also be nested inside other VM's on the host machine or a USB drive.

◇ Some newer Windows system log when USB drives are attached.

☐ Follow the consistent procedure:
☐ Image the host machine/computer e.g. FTK imager.
☐ Locate the virtualization software and VMs, using information from registry, VM related file extensions and network adapters.
☐ Export from the host machine all files associated with VMs.
☐ Record the hash values of associated files.
☐ Open a VM as an image file in forensics software and create a forensic image or mount the VM as a drive.

☐ Live acquisitions of VMs are often necessary to include all snapshots.
☐ Static acquisitions may not include snapshots.
☐ Using VMs as forensic Tools
☐ Investigators can use VMs to run forensics tools stored on USB drives.

Performing Live Acquisitions

Performing Live Acquisitions

• Live Acquisitions are especially useful when you're dealing with active network intrusions or attack.
• Live Acquisitions done before taking a system offline are also valuable.
◇ Attacks can leave footprints in running processes or RAM.
• Order of volatility (OOV).

• Steps for performing Live Acquisitions:
◇ Create or download a bootable forensic CD orUSB drive.
◇ Make sure you keep a log of all actions.
◇ Anetwork drive is ideal as a place to send the information you collect.
◇ Copy the physical memory (RAM).
◇ Look elsewhere according to the evidence you seek.
◇ Be sure to get a forensic digital hash value of all files you recover during the live acquisition.

Network Forensics

Network Forensics

• Network Forensics.
◇ Monitoring, collecting and analyzing n/w activites, network data and tracking n/w traffic.
◇ TO ascertain how an attack was carrid out or how an event occurred on a network.
• Intruders leave a tail behind.
◇ Knowing your n/w typical traffic patterns is important in spotting variations in n/w traffic.
◇ Can also help you determine whether a n/w is truly under attack.

Procedures for Network Forensics

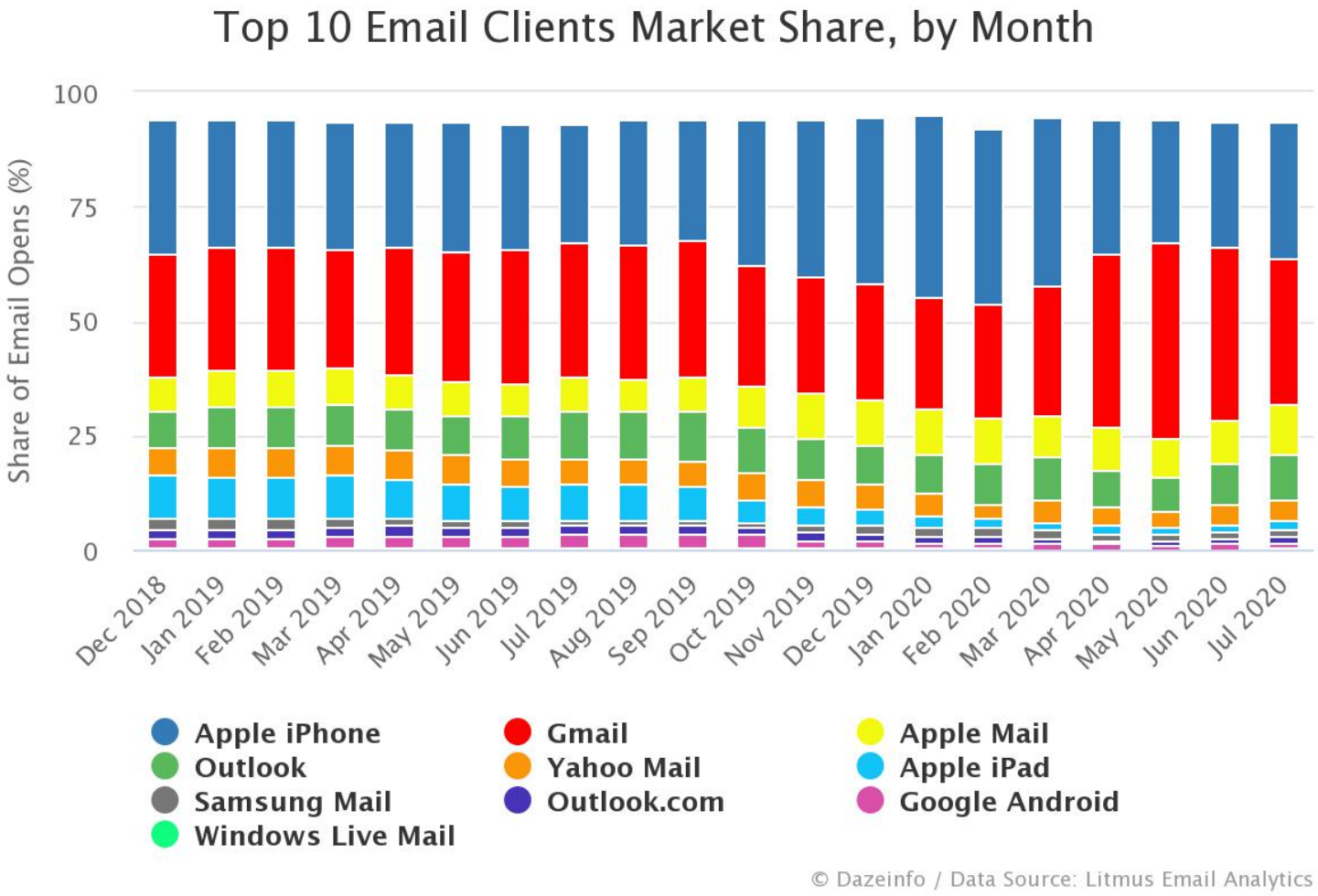
Procedures for Network Forensics

- Network forensics can be a long, tedious process.
- Standard procedure that is often used:
  - ◇ Always use a standard installation image fro systems on a n/w
  - ◇ Fix any vlunerability after an attack.
  - ◇ Attempt to retreve all volatile data.
  - ◇ Acquire all compromised drives.
  - ◇ Compare file on the forensic image to the original installation image.
- In digital forensics.
  - ◇ You can work from the image to find most of the deleted or hidden files and partitions.
- In network forensics.
  - ◇ You have to restore drives to understand attack.

Email and social media

Top 10 Email Clients Market Share by Month

Top 10 Email Clients Market Share by Month



Email Forensics Introduction

Email Forensics Introduction

• E-mail fraudsters use phshing, pharming, and spoofing scam techniques.
• In both internet or intranet e-mail environments, e-mail messages are distributed from one central server to connected client computers.
• E-mail investigations are similar to other kinds of investigations.
• Forensics linguistics is a field where language and the law intresect to determine the author of the e-mails, text messages, and other online communications.
• Access victim's computer to recover evidence.
  ◇ Copy and print the e-mail message involved in the crime or policy violation.

SPAM Email Example

SPAM Email Example

AP

APD Payroll <APD-payroll@apd-alerts.com>
Fri 3/19/2021 12:03 PM
To: Matt Constable

The link below is a summary of Origination activity for the past 7 days.
Previous 7 Days ACH Notifications

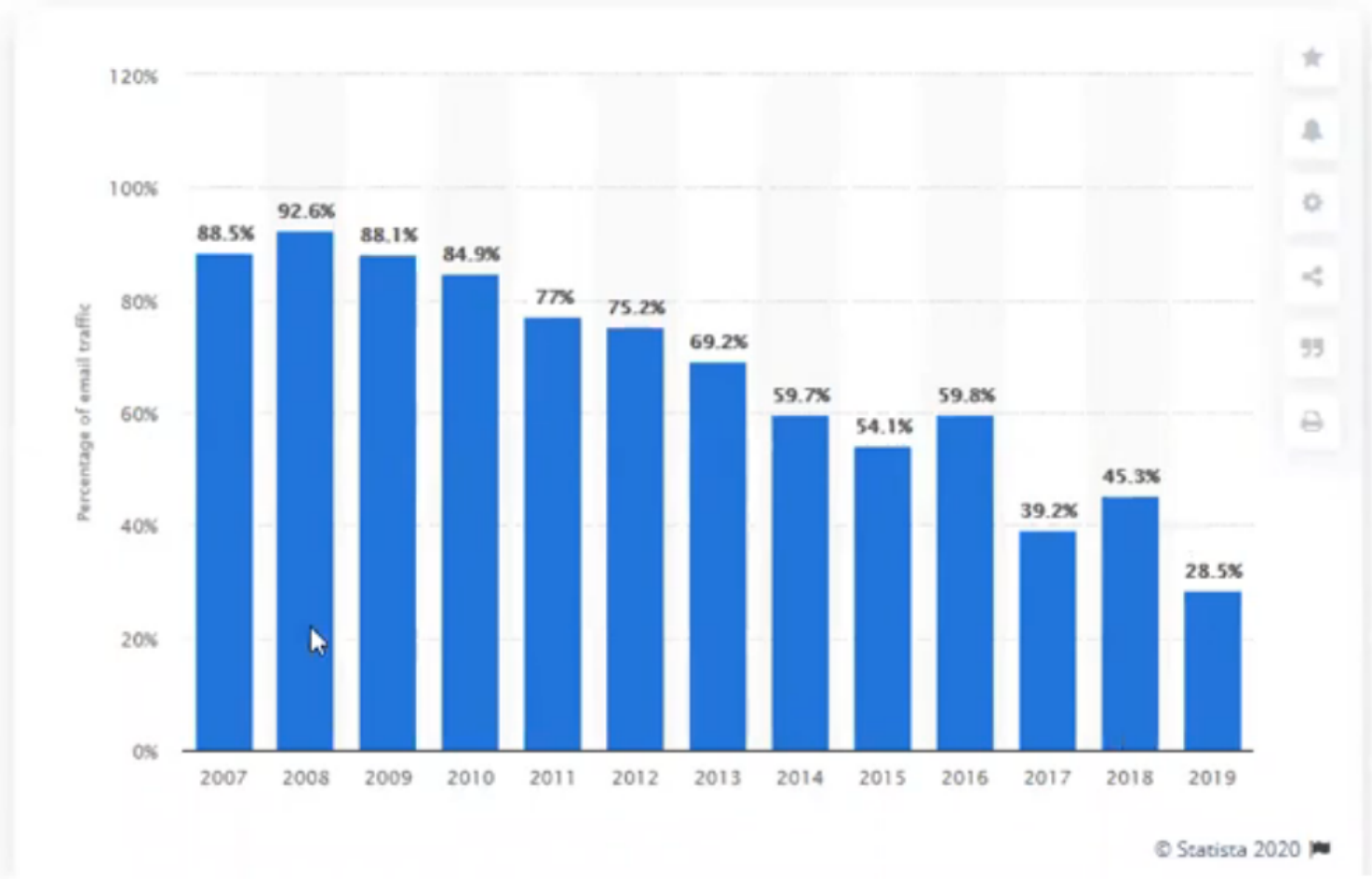
Due to recent security policy changes we no longer attach documents to emails.

If you need assistance please visit our site at APD.com

Reply | Forward

Global Spam Volume

Global Spam Volume



Email Investigations

Email Investigations

• E-mail is asynchronous communication - sender and recerve connects to the internet when required.
• Phishing:- e-mails contain links to illegitimate web pages.
  ◇ Attempts to get personal information from reader.
• Pharming:- Domain Name System(DNS) poisoining takes user to a fake site (redirecting a website traffic to another site).
• Spoofing:- e-mail can be used to commit fraud (creating an email message with a forged sender address that looks legitimate).
• Investigators can use the Enhanced/Extended simple Mail transfer protocol(ESMTP) numver in the message's header to check for legitimacy of email.
• Use the e-mail program that create the message to find the email headers.
  ◇ Provides supporting evidence.
  ◇ Assists to track the suspect to the originating location.
• Investigating e-mail abuse.
  ◇ Be familar with e-mail server and clients operations.
• For many email investigations you can rely on email message files, headers, and server log files.

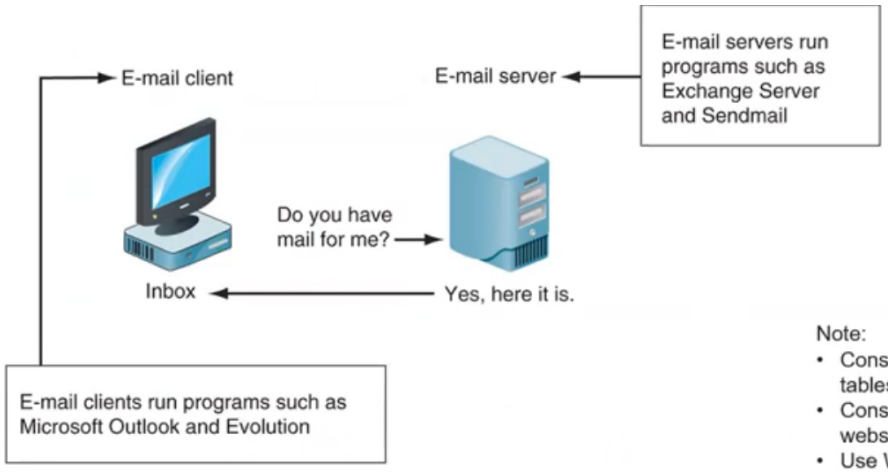


Figure 11-1 E-mail in a client/server architecture

Note:
- Consider getting information (IP address dynamic and static, routing tables, users etc) from routers.
- Consider viewing cookies – Cookies are commonly used to record websites that a user visits and are spyware.
- Use Windows Registry to look for websites a user has visited (HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs).
- Analysing index.dat file for websites visited by a user.

Examining Email Messages

Examining Email Messages

• Access victim's computer and mobile device to recover the evidence.
• Using the victim's e-mail client

  ◇ FInd and copy any potential evidence.
  ◇ Access protected or encrypted matetial.
  ◇ Print e-mails
• Guide victim on the phone
  ◇ Open and copy e-mail including headers.
• You may have to recover deleted e-mails.

Viewing Email Headers

Viewing Email Headers

• Investigators should learn how to find e-mail headers.
  ◇ GUI clients.
  ◇ Web-based clients.
• After you open e-mail headers, copy and paste them into a text document
  ◇ So that you can read them with a text editor.
• Become familiar with as many e-mail programs as possible.
  ◇ Often more than one e-mail program is installed, e.g. Outlook, Gmail, Yahoo etc.
• Headers contain useful information.
  ◇ The main piece of information you’re looking for is the originating e-mail’s IP address.
  ◇ Date and time the message was sent.
  ◇ Filenames of any attachments.
  ◇ Unique message number (if supplied).

Example:-

Received: from SYAPR01MB2382.ausprd01.prod.outlook.com (2603:10c6:1:5::10) by
 MEXPR01MB1255.ausprd01.prod.outlook.com with HTTPS; Wed, 17 Mar 2021 02:11:40
 +0000
Authentication-Results: latrobe.edu.au; dkim=none (message not
 signed) header.d=none; latrobe.edu.au; dmarc=none action=none
 header.from=latrobe.edu.au;
Received: from SY4PR01MB6443.ausprd01.prod.outlook.com (2603:10c6:10:109::8)

by SYAPR01MB2382.ausprd01.prod.outlook.com (2603:10c6:1:5::10) with Microsoft
SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.3933.32; Wed, 17 Mar 2021 02:11:39 +0000
Received: from SY4PR01MB6443.ausprd01.prod.outlook.com
([fe80::8013:db8a:5693:cecc]) by SY4PR01MB6443.ausprd01.prod.outlook.com
([fe80::8013:db8a:5693:cecc%3]) with mapi id 15.20.3933.032; Wed, 17 Mar 2021
02:11:39 +0000
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Danny Boy <D.Boy@latrobe.edu.au>
To: Matti Man <M.Man@latrobe.edu.au>
Subject: RE: Exercise Physiology student research projects
Thread-Topic: Exercise Physiology student research projects

Social Media Forensics

Social Media Forensics

- Online social networks (OSNs) are used to conduct business, brag about criminal activities, raise money, have class discussions and many more.
- Law enforcement, companies and criminals can use OSNs to find out about individuals.
- Criminals even don’t need to crack the password, they can use individual profile to reset the password for social media or e-mail accounts.
- Social media can contain:
  - Evidence of cyberbullying and witness tampering.
  - A company’s position on an issue.

- Whether intellectual property rights have been violated.
- Who posted information and when.

• Social media can often substantiate a party’s claims.
• OSNs involve multiple jurisdictions that might even international boundaries.

Social Media Forensics on Mobile Devices

Social Media Forensics on Mobile Devices

• Digital forensics investigators require to acquire digital evidence from a variety of sources, e.g. computers, mobile devices, website (HTML documents), web servers, IP addresses, digital images, videos, voice messages, chat messages and many more.
• Mobile devices are the common mode for accessing social media sites .
• iPhone and Android devices.
- Yielded the most information, and much of the data was stored in SQLite databases.
- Evidence artifacts vary depending on the social media channel and the device used.

• Charging a mobile device to extract evidence – caution never charge a mobile device which is evidence through a computer, it will change the evidence.

Forensic Tools for Social Media Investigations

Forensic Tools for Social Media Investigations

• Software for social media forensics is being developed.
-

◇ Not many tools are available now.
• There are questions about how the information these tools gather can be used in court or in arbitration.
• Using social media forensics software might also require getting the permission of the people whose information is being examined.

DIgital Forensic Tools

DIgital Forensic Tools

Outline

• Evaluate your DFT needs
• DFTs functions
• DFT types
• Validation
• Demo

Evaluate DFT needs

Evaluate DFT needs

• First consider open-source tools; the best value for as many features as possible.
• When open source DFTs not available, consider commercial DFTs, but be aware of the cost.
• Questions to ask when evaluating tools:
  ■ On which OS does the forensics tool run ?
  ■ Is the tool versatile?
  ■ Can the tool analyze more than one file system?
  ■ Can a scripting language be used with the tool to automate repetitive functions and tasks?
  ■ Does it have automated features?
  ■ What is the vendor's reputation for providing product support?

Other Considerations for DFTs

Other Considerations for DFTs

• Apart from the questions discussed on previous slide, also consider:
  ■ Flexibility.
  ■ Reliability.

- Future expandability.

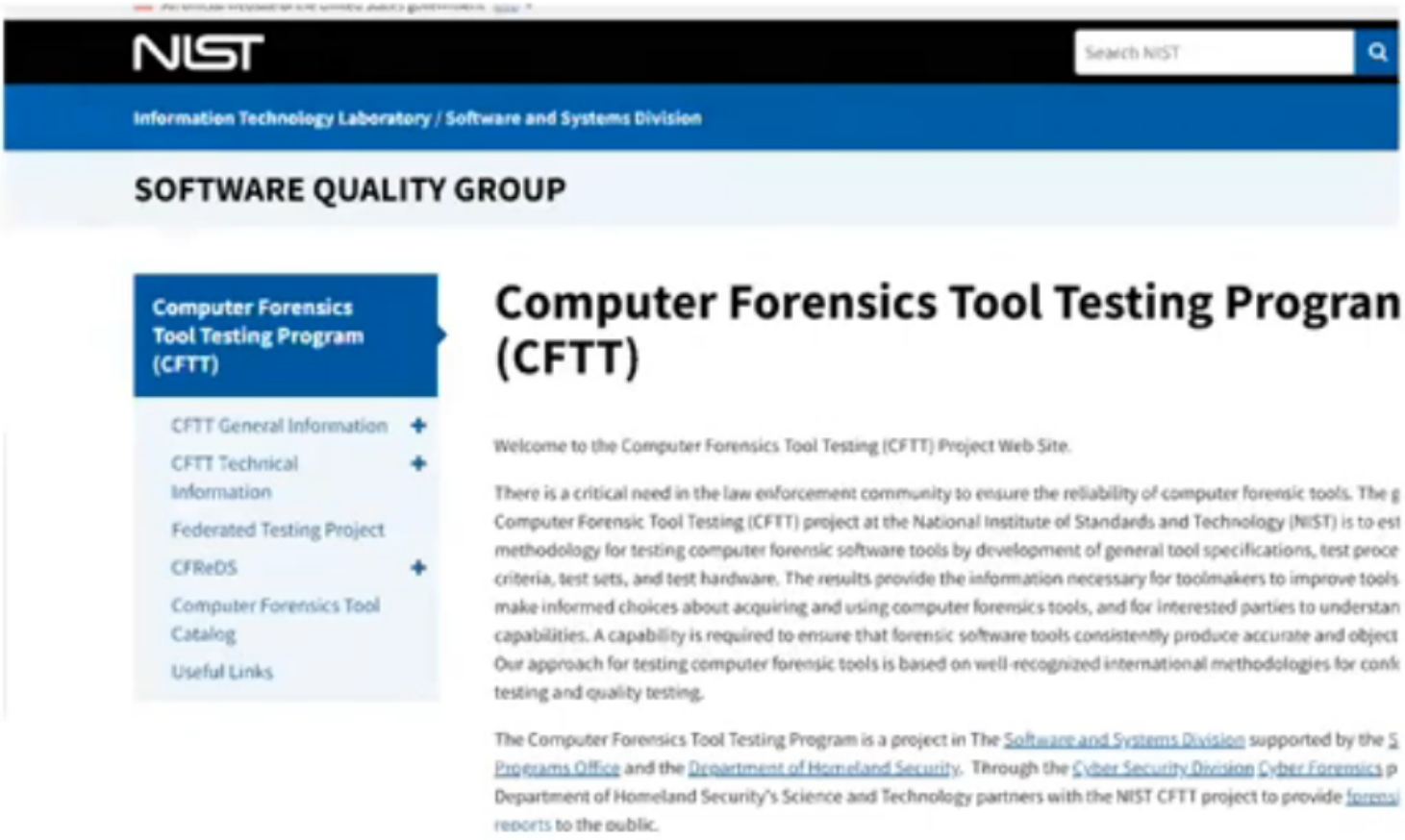
• Create a software library containing older versions of forensics utilities, OSs, and other programs - you always will need legacy tools for some of the cases.

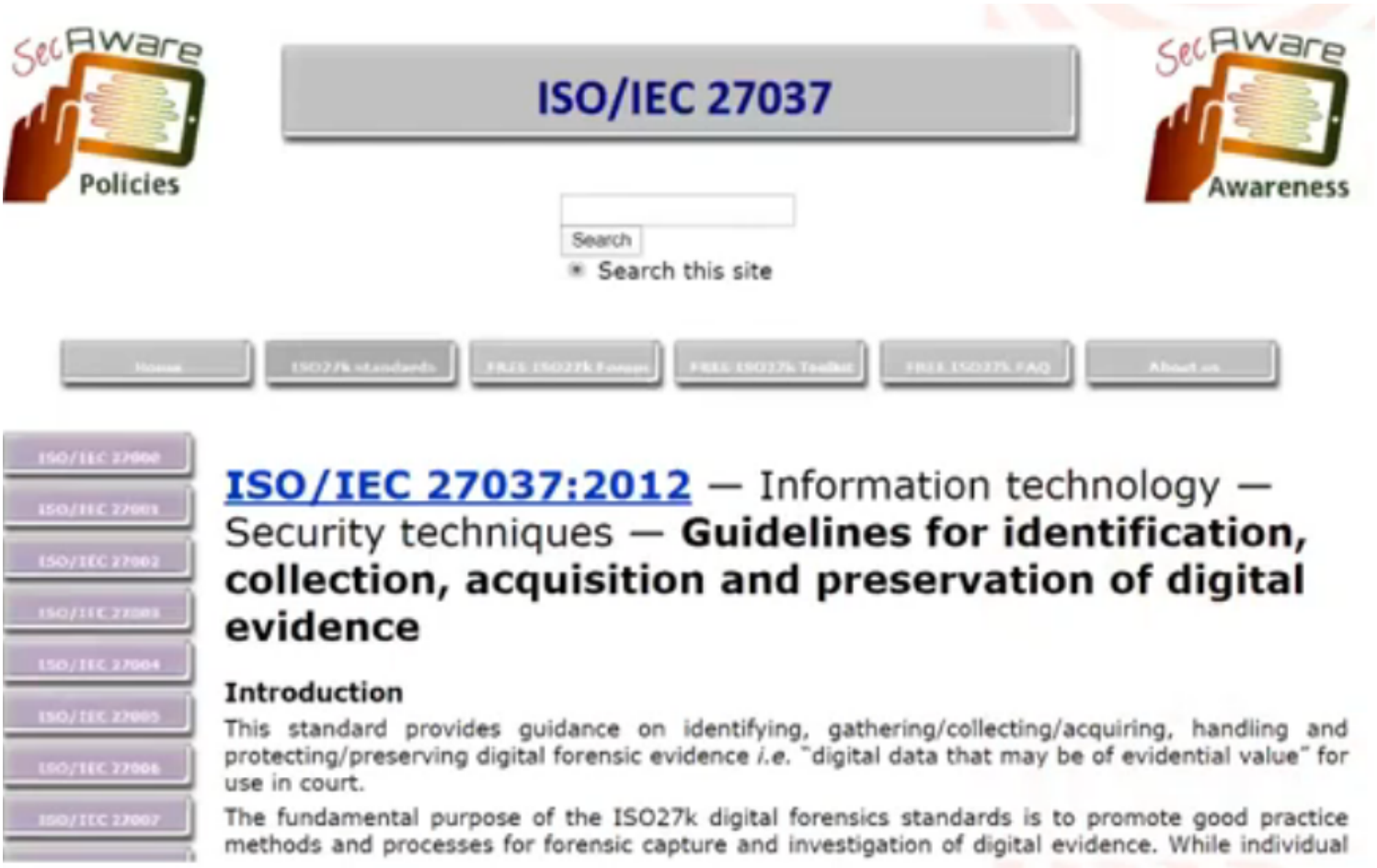
DFT Testing & Standards

DFT Testing & Standards

• Follow guidelines setup by NIST's Computer Forensics Tool Testing (CFTT) program
- LInk:- https://www.nist.gov

• ISO/IEC 27037:2012 standard - Guidelines for identifications, Collection, acquisition and preservation of digital evidence.





Tasks Performed by DF Tools

Tasks Performed by DF Tools

- FIve major task categories a DFT is expected to perform
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting

DF Software Tools

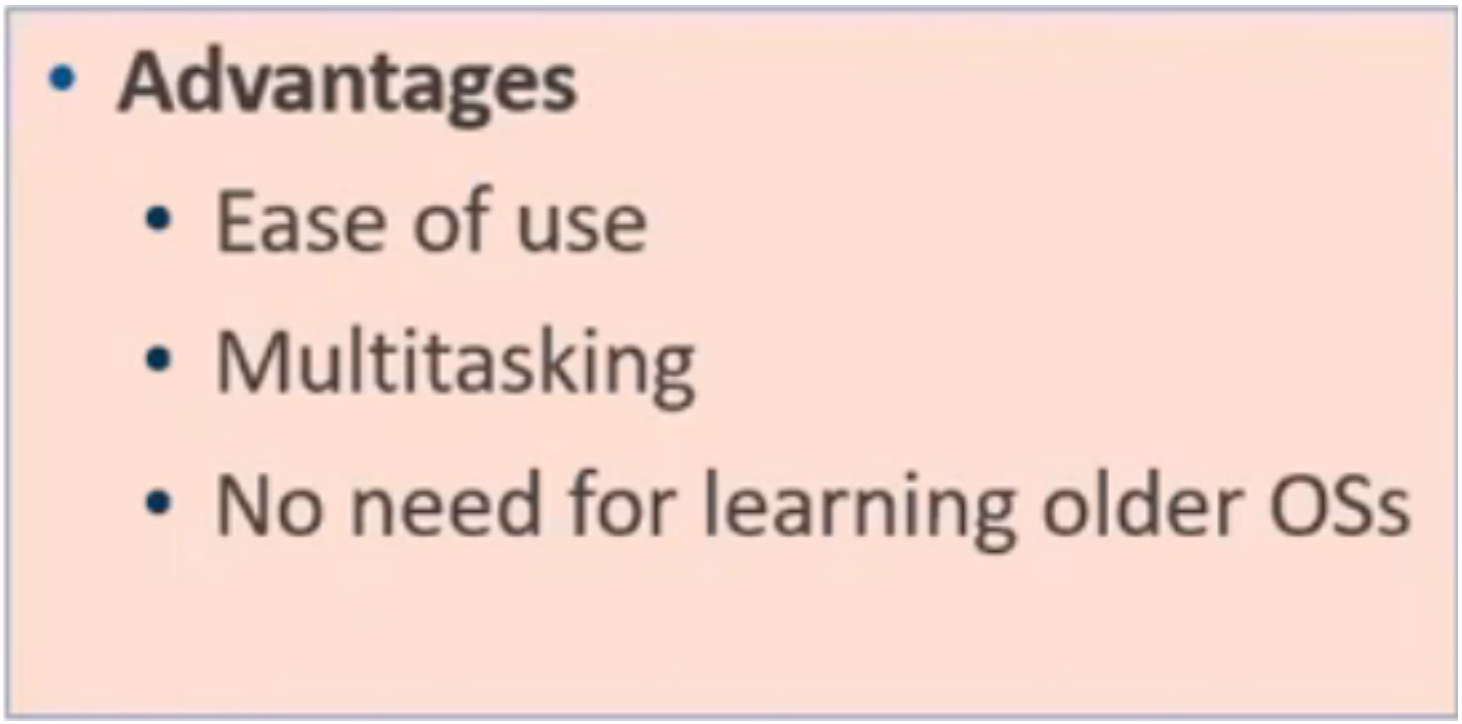
DF Software Tools

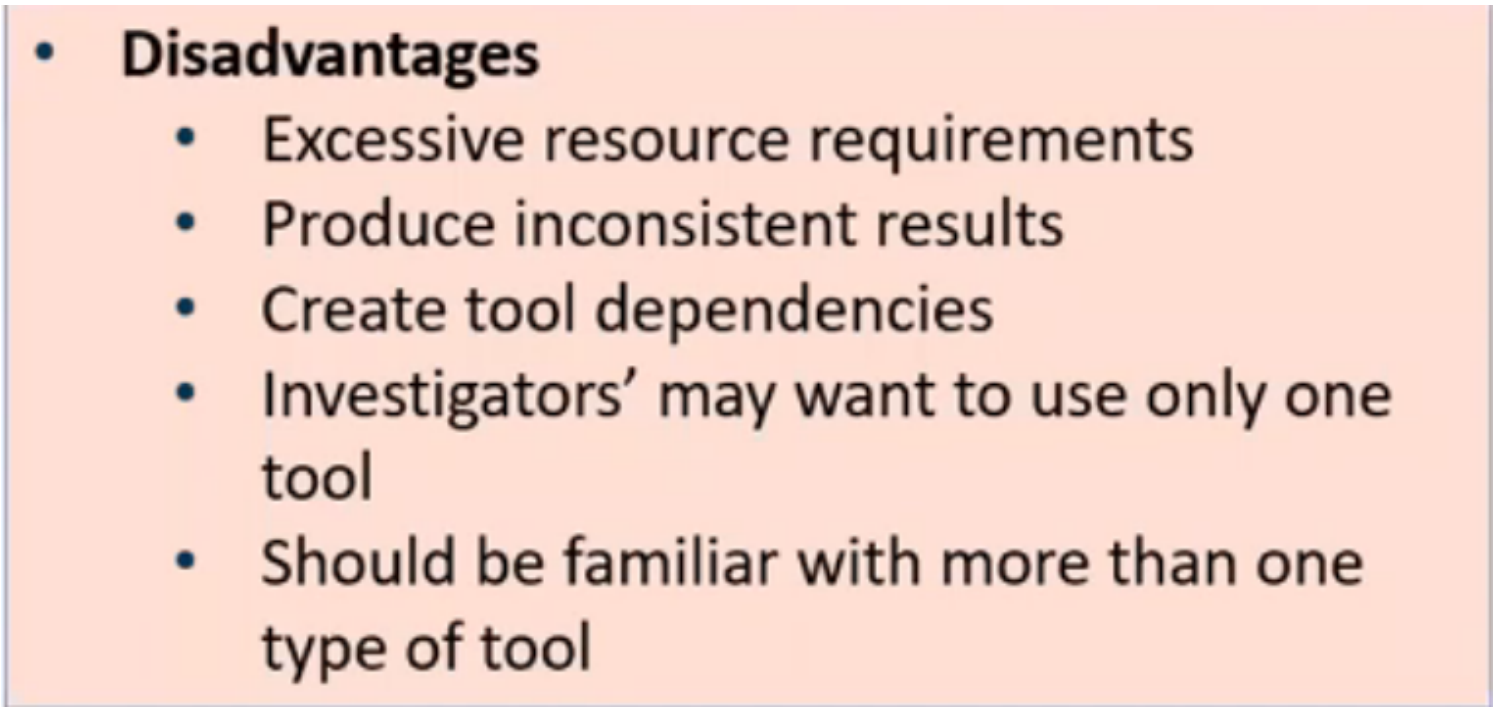
- Software forensics tools are classified into command line applications and GUI applications
- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems
- Norton DiskEdit
  - One of the first MS-DOS tools used for computer investigations
- Command line tools require few system resources
  - Designed to run in minimal configurations

GUI Forensics Tools

GUI Forensics Tools

• GUI forensics tools can simplify digital forensics investigations
• Have also simplified traning for beginning examiners
• Most of them are put together as suites of tools





DF Hardware tools

DF Hardware Tools

• Hardware DFTs range from simple, single purpose components to complete computer systems and servers.
• Technology changes rapidly, so keep updating your DFT hardware by visiting vendor's web site and checking for product updates.
• Hardware eventually fails
    ■ Schedule equpment replacements periodically
• When planning your budget consider:
    ■ Amount of time you expect the forensic workstation to be running
    ■ Failures
    ■ Consultant and vendor fees
    ■ Anticipate equipment replacements

Forensic Workstations

Forensic Workstations

• Carefully consider what you need
• Categories
    ■ Stationary workstation
    ■ Portable workstations
    ■ Lightweight workstations
• Balance what you need and what your system can handle
    ■ Remember that RAM and storage need updating as technology advance

- Law enforcement labs
  - Need many options
  - Use several PC configurations
- Keep a hardware library in addition to your software library
- Private corporation labs
  - Handle only system types used in the organization

- Building a forensic workstation is not as difficult as it sounds

Advantages	Disadvantages
• Customized to your needs • Save money	• Hard to find support for problems • Can become expensive if careless

- Also need to identify what you intend to analyze
- Some vendors offer workstations designed for digital forensics
- Having vendor support can save you time and frustration when you have problems.
- Can mix and match components to get the capabilities you need for your forensic workstation.

Recommendations for a Forensic Workstation

Recommendations for a Forensic Workstation

- Determine where data acquisitions will take place
- With the newer Firewire and USB write-blocking devices
  - ✓ You can acquire data easily with Digital Intelligence FireChief and a laptop computer
- For compact options consider something like:
  - ✓ WiebeTech Forensic DriveDock
  - ✓ Logicube Talon

- As with any technology, what your forensics workstation includes is often a matter of preference. Whatever vendor you choose, make sure the devices you select perform the functions you expect to need as an investigator.

- Recommendations when choosing stationary or lightweight workstation:
  - ✓ Full tower to allow for expansion devices
  - ✓ As much memory and processor power as budget allows
  - ✓ Different sizes of hard drives
  - ✓ 400-watt or better power supply with battery backup
  - ✓ External FireWire and USB ports
  - ✓ Assortment of drive adapter bridges
  - ✓ Ergonomic keyboard and mouse
  - ✓ A good video card with at least a 17-inch monitor
  - ✓ High-end video card and dual monitors
- If you have a limited budget, one option for outfitting your lab is to use high-end game PCs

Using Validation Protocols

Using Validation Protocols

- Always verify your results by performing the same tasks with other similar forensics tools
- Use at least two tools
  - ✓ Retrieving and examination
  - ✓ Verification
- Understand how forensics tools work
- One way to compare results and verify a new tool is by using a disk editor
  - ✓ Such as Hex Workshop or WinHex

Using Validation Protocols (2 of 3)

- Disk editors do not have a flashy interface, however they:
  - ✓ Are reliable tools
  - ✓ Can access raw data
- Digital Forensics Examination Protocol
  - ✓ Perform the investigation with a GUI tool
  - ✓ Verify your results with a disk editor
  - ✓ Compare hash values obtained with both tools

Using Validation Protocols (3 of 3)

- Digital Forensics Tool Upgrade Protocol
  - ✓ Test
    - New releases
    - OS patches and upgrades
  - ✓ If you find a problem, report it to forensics tool vendor
    - Do not use the forensics tool until the problem has been fixed
  - ✓ Use a test hard disk for validation purposes
  - ✓ Check the Web for new editions, updates, patches, and validation tests for your tools