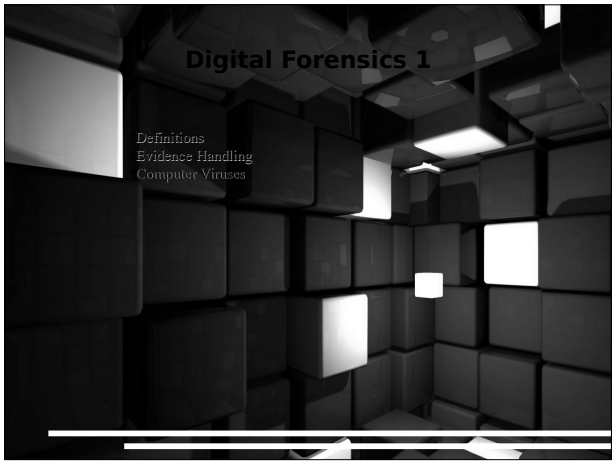
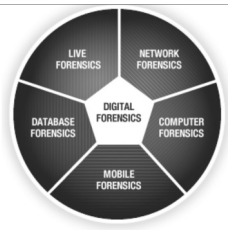



*Digital Forensics*




**DEFINITION:**
The high-level process of digital forensics includes the acquisition of data from a source, analysis of the data and extraction of evidence, and preservation and presentation of the Evidence. (Brian Carrier,International Journal of Digital Evidence, V.1 n4,2003)

*Digital Forensics*


**DEFINITION:**
US-CERT defines computer forensics as the discipline that combines
elements of law and computer science to collect and analyze data from computer systems,
networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

*Digital Forensics*

**Live Forensics** refers to what may be lost when a suspect system is powered down, and it attempts to collect that data while the systems is still operational, with minimal impact to the integrity of data while collecting evidence.

*Digital Forensics*

**Database Forensics** refers to the forensic study of databases and their related metadata. This may also include timestamps applying to the update time of a row in a relational table, or the identification of transactions indicating a fraud.

*Digital Forensics*

**Mobile Forensics** refers to the recovery and analysis of sound digital evidence from mobile devices.
**Network Forensics** is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.

*Digital Forensics*

**Computer Forensics** refers the branch of digital forensics pertaining to legal evidence found on computers and digital storage media.

*Evidence Handling*

Procedures for evidence handling are evolving (SANS Institute Digital Forensics and Incident Response Blog). There is a shift towards simply "pulling the plug" towards the acquisition of "live" evidence from a suspect computer.

*Evidence Handling*

Reasons –
Apps can be installed on removable media & virtualised in RAM without a trace on the hard disk.
Undetectable Rootkits (to OS) hide within process and when using local binary tools — you must analyze memory with trusted binaries

*Evidence Handling*

Reasons –

Fully RAM resident Malware with no trace of existence on the hard disk
Use of hidden encrypted files or partitions - areas of the hard drive to hide evidence
Web browsers offering the ability to cover one's tracks — user activity log files are created but deleted when the browser is closed

*Evidence Handling*

Reasons –

Web 2.0 landscape changes: web-based email, blogs, wikis, twitter,... extending storage of user actions / communications beyond the traditional hard disk found on the users machine.

*Live Forensics: Order of Volatility of digital evidence*

1. CPU, cache and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary/Virtual file system (swap space)
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

1.Photograph Computer and Scene
2.If Computer is off, do not turn it on
3.If Computer is on, photograph the screen
4.Collect live data: start with RAM image (Live Response, FastDump Pro locally or remotely via F-Response) and then collect other live data "as required" such as network connection state, logged on users, currently executing processes etc.

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

5.Check if encryption (eg full disk encryption with PGP Disk) is used, with tools like Zero-View), collect "logical image" of Hdd using dd.exe, Helix - locally or remotely via F-Response
6.Unplug power cord from the back of the tower - If the computer is a laptop you will probably have to remove the battery
7.Diagram and label all cords

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

8.Document all device model numbers and serial numbers
9.Disconnect all cords and devices
10.Check for Host Protected Area then image hard drives using a write blocker, Helix or a hardware imager

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

HPA was introduced in ATA-4 standard
It was used for large hdd's so older bioses would work
Used by some manufacturers eg Dell, LG, IBM to hide utilities/system restore software/preloaded OS. Stolen laptops get reformatted but the HPA is untouched
Used by some rootkits to avoid anti-rootkit/anti-viruses
Used by some NSA exploits for app persistance

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

HPA – detectable when booting Linux (dmesg).. hdb: Host Protected Area detected.

Hdparm can also detect it. Other tools can detect and manipulate eg HPARemove, HDAT2, setmax, Feature Tool, MHDD

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

11.Package all components (using anti-static evidence bags)
12.Seize all additional storage media (create respective images and place original devices in anti-static evidence bags)

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

13. Keep all media away from magnets, radio transmitters and other potentially damaging elements
14. Collect instruction manuals, documentation and notes
15. Document all steps used in the seizure

*Accepted Best Practices by SANS Institute in Preservation of Live Evidence*

Other points: Network connections, Routes and Clouds..

*Malware Code Types (src:Security in Computing ed.4)*

| Code Type | Characteristics |
|---|---|
| Virus | Attaches itself to program and propagates copies of itself to other programs |
| Trojan horse | Contains unexpected, additional functionality |
| Logic bomb | Triggers action when condition occurs |
| Time bomb | Triggers action when specified time occurs |
| Trapdoor | Allows unauthorized access to functionality |
| Worm | Propagates copies of itself through a network |
| Rabbit | Replicates itself without limit to exhaust resources |

*Computer Viruses*

- Computer viruses were invented in 1984 by the academic Fred Cohen.
- The first widespread infection (Brain virus) occurred in the USA, 1986, causing media sensation.
- Some people incorrectly thought they occurred accidentally.

*Viruses*

- An expert programmer (Peter Norton) once claimed they did not exist! (Before they became widespread)
- Unlike earlier viruses, a number of new viruses are destructive.
- The number of viruses doubles every 9 months. In 1982 the number was 1500. In late 1996 this amount grew to over 9100. Worms, once rare, have become widespread due to Microsoft mail program vulnerabilities

*Viruses*

In 2001, more than 60,000 different viruses exist yet a small number counted for most infections
In 2008, over a million viruses existed.

## *Viruses*

- In 2014, more than 150,000 are in circulation every day and more than 148,000 computers are compromised every day.
- One virus to be aware of is **CryptoLocker** which comes disguised as an email attachment. Usage of **CryptoProtect** and **EMET** (Microsoft) is recommended

## *EMET*

- What is the Enhanced Mitigation Experience Toolkit?
- The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. (making exploitation difficult)

## *EMET*

- It is designed to harden Windows systems even before new and undiscovered threats against the operating system and third-party software are formally addressed by security updates and antimalware software. (More info: Krebsonsecurity blog)

## *EMET*

- Security mitigation technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities.
- It is not a guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform.

## *EMET*

- Brought back in Win10's exploit mitigations, starting from Win10 Fall Creators Update
- Windows Defender Exploit Guard

## *Win Defender Exploit Guard*

### *Application Guard for Edge*

- Runs Edge under a VM (similar to Sandboxie)

### *Windows Defender Advanced Threat Protection (ATP)*

- Cloud-based heuristic malware detection
- Since Creators update – detects memory manipulation, script-based attacks and keylogging
- Reporting and tracking being improved
- Available also on Windows server (2016 and 2012 R2) + in future on non-Win platforms

### *Viruses*

Viruses are either Resident (can stay active after host program ends) or Non-Resident (Transient)

### *Logic Bombs*

A logic bomb is a conditional statement that causes some program code to execute when a condition is satisfied. The condition can be a time condition, the presence or absence of data such as a name etc. E.g. a maliciously modified spreadsheet that zeroed a particular cell on Mondays between 9 and 10pm. The result would be confusing to trace.

### *Logic Bombs*

They are frequently found in more sophisticated cases of computer crime. E.g. a programmer maintaining a payroll package programmed some instructions which checked that his name was in the payroll file. If it was not (in case he was fired) files would be deleted and other damage would happen.

### *Logic Bombs*

After he was fired, the logic bomb triggered the destruction. Only upon reinstatement by his employer did he agree to point out the logic bomb. He was not prosecuted.

### *Logic Bombs*

- At IBM, on 11th April 1980 all IBM 4341s ceased to operate. The bomb was placed by a disgruntled employee.
- Logic bombs are often found in viruses where the payload causing the side-effects is triggered when a certain condition is met. Eg. the Cascade virus produces its side effects only between 1st October 1988 and 31st December 1988. This type of delay allows a virus to spread unnoticed, showing its side-effects after it has reproduced extensively.

### *How Viruses Attach*

- Printed virus code does nothing
- For a virus to do its malicious job, it must be activated
- Programs may be executed in many ways
- A SETUP program may call dozens or more of programs on the distribution media, or on your PC or memory. If one of these are infected, the virus code could be infected

### *How Viruses Attach*

- Payload – An action performed by a virus when it spreads. This might be damage or even nothing.
- Attachment to Email: Virus writer tries to convince recipient to open the attachment. As soon as it is opened, the virus is activated.

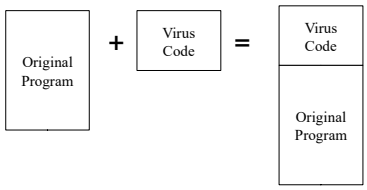
### *How Viruses Attach*

- **Ease of use:** Some modern email handlers "*help*" the victim by automatically opening attachments. Dangerous code-exes, other files including word docs, pdf/graphics/photo images (can contain code which can be executed by an editor)

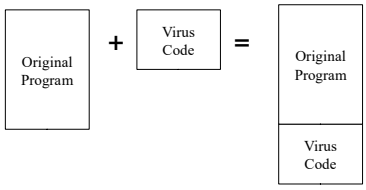
### *Appended Viruses*

- A program virus attaches itself to a program.
- The virus activates whenever the program runs
- Easy to program

### *Prepended Viruses*



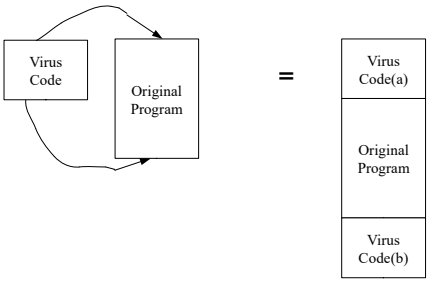
### *Appended Viruses*




### *Prepended Viruses*

- Inserts a copy of itself into executable file before the first executable instruction. Then all virus instructions are run first, followed by a jump to the first program instruction.
- Simple and Effective
- Virus author does not need to know about the host program
- Most viruses

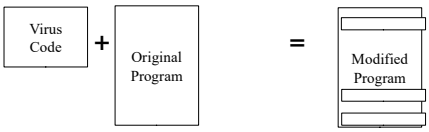
### *Viruses Surrounding a Program*




### *Viruses Surrounding a Program*

- It runs the original host program but has control BEFORE and AFTER it's execution.
- Eg virus writer wants to prevent detection. By disk storage, its presence will be given away by its filename or size (affecting disk space). Thus a virus might infect the ls program. By regaining control after the listing program was generated the list, but before it is printed, the virus could delete its entry or modify the file size or space counts (camouflage).

### *Virus Integration/Replacement in a Program*




### *Virus Integration/Replacement in a Program*

- A virus can replace part of the original program code with its own replacement.
- Requires understanding of the target host's exact structure.
- Entire target can be replaced, mimicking effect of target or ignoring its effect and performing only the virus effect

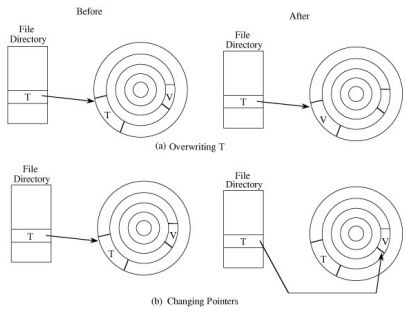
### *Document Virus*

- One of the most popular virus types
- Some Document types can include code (macros, formulas, formatting controls, links, system calls, file accesses, variables, procedures,..)
- An author can perform malicious actions
- User sees just the data by default

### *Virus Control*

- The Virus (V) has to be invoked instead of the Target (T)
- Virus has to assume identity of T (I am T) or to push T out of the way and substitute T (Call me instead of T); or blatantly say 'Invoke me (you fool)'
- Virus can **overwrite** T in storage or **change pointers** in file table so that virus will be located instead of T whenever T is accessed

### *Virus Control (src:Security in Computing ed.4)*




### *Malware Author's Ideal*

- Virus Hard to detect
- Not easily removed or deactivated
- Infection spreads widely
- Can reinfect its home program or other programs
- Easy to create
- Machine independent and OS independent

### *Malware Author's Ideal*

- Multiple Execution used to be needed for spreading.. (no longer today)
- Majority is One-Time-Execution eg opening of email

### *Boot Sector Viruses*

- A fairly popular case is the Boot Sector or MBR (Master Boot Record) Virus
- At boot-time control goes to firmware determining which hardware components are present. A hardware platform runs many potential OSes thus this is invoked dynamically perhaps even by user choice. OS is software stored on disk.

### *UEFI – Unified Extensible Firmware Interface*

- UEFI too uses an MBR but without executing the MBR boot code (exception legacy BIOS mode). Today's BIOS is really UEFI firmware.

### *Boot Sector Viruses*

- BOOTSTRAPPING (BOOTING): A copy is done from storage to memory and control is transferred to it.
- Firmware does its control transfer, reading a fixed number of bytes from a fixed location on the disk (BOOT SECTOR) to a fixed memory location and then transferring control (jumping) to it.
- Bootstrap loader will read into memory the rest of the OS from disk.

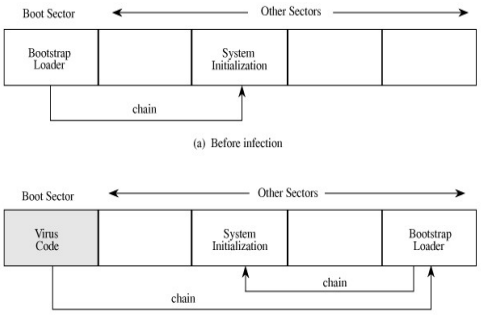
### *Boot Sector Viruses*

- To run a different OS, the user inserts a new disk with the new OS and bootstrap loader.
- This scheme is used on PC's, workstations and large mainframes
- Boot sector on a PC is slightly less than 512 bytes

### *Boot Sector Viruses*

- To allow for larger loaders, hardware designers support "**chaining**" in which each block of the bootstrap contains the location of the next block. This process also makes virus installation simpler. It simply has to break the chain at any point and install a pointer to its code.

### *Boot Sector Viruses (src:Security in Computing 4th ed)*




### *Boot Sector Viruses*

- By executing early in the process, it may evade detection, or complicate it. Files in the boot area may be hidden from users by the OS, making it not easily noticeable by users
- One countermeasure in use today is to boot a Linux OS with an antivirus on a USB stick or CD/DVD

### *Case Study of a Hacker Break*

- Source: http://krebsonsecurity.com/2013/11/hackers-take-limo-service-firm-for-a-ride/
- Hackers broke in a US company that brokers limousine reservations, exposing personal and financial information on 850000 customers including CEOs, lawmakers and A-List celebrities
- Same attacker may have been involved in stealing of info from PR Newswire and source data from Adobe

### *Case Study of a Hacker Break*

- File archive name reads "CorporateCarOnline", matching a company in Kirkwood,Missouri which provides software management solutions for the limousine and transportation industry
- Data included credit card numbers (inc.American Express),names and addresses
- CorporateCarOnline.com declined to comment but confirmed to the chief security officer at Hold Security inc that the data was stolen from its systems

### *Case Study of a Hacker Break*

- The compromise occurred due to a vulnerability in ColdFusion (a web app platform), a favourite target of hackers
- Celebrities with stolen records included LeBron James, Aaron Rodgers and Tom Hanks (his record: Chicago Midway, June 19, 2013; "VVIP. No cell/radio use with passenger/prepaid. 1500 W. Taylor Street Chicago, Rosebud, Dinner Reser @8pm)
(Image src:Wikipedia)

### *Case Study of a Hacker Break*

- Some of the lawmakers included Sen. Mark Udall and former senator Tom Daschle.
- Top executives included Donald Trump (Wynn Hotel, Las Vegas, Feb. 12, 2007: "Must be new car, clean, and front seat must be clear.")
- Information included future dates and locations of travel for many important people – very useful for nation-level attackers

### *Case Study of a Hacker Break*


FP National Security

Now the Chinese Are Hacking Us Through Our Limos

- Consider this story in Foreign Policy magazine
- Kevin Mandia (CEO of Mandiant) was a victim of a targetted cyberattack that attempted to foist upon him a booby-trapped PDF copy of a recent limo invoice, send "from an [advanced hacking] group in China" (quote from Mandia)

### *Case Study of a Hacker Break*

- The stolen limo database may have been involved in this attack. His record was in the database
- The database also included details on misbehaviour and all sorts of naughtiness by clients..

Image src:Orlando Limo Service

### *Virus Signatures*

- The completely invisible virus does not exist. It must leave tracks
- Code must be left somewhere and it must be placed in memory to run
- Characteristics yield a pattern – a **signature**.
- A **scanner** can look for it, searching memory and long-term storage for virus patterns

### *Virus Signatures*

Eg. Code Red's pattern from Apache logs:

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```

### *Virus Signatures*

- After recognition, a scanner can take actions such as blocking the virus, informing the user, remove the virus (cleaning, or quarantine)
- Scanners have to be kept up-to-date
- Scanners can detect suspicious patterns (eg JMP … at start)
- A particular virus will in most cases always be located at the same position relative to its attached file. Eg. Always at the top or always at the bottom of the file

### *Medium of Delivery*

- Email and Documents with code
- Files
- Boot Sectors
- Peer to Peer sharing protocols
- Remote exploitation of vulnerabilities
- Multiple methods

### *Virus Prevention*

- Only way is not to receive an executable from an infected source
- .exe used to be an indication of an executable
- Today documents may have code eg documents, spreadsheets, presentations, media files can contain scripts or code and harbor viruses
- A .doc file is expected to be a document but the true document type is hidden in a field at the start of the file! This “helps” users who rename a .ppt file to an incorrect suffix.. so this can be exploited

### *Virus Prevention*

- Code has been hidden in read-only docs and in pictures. This may not be easily detected eg a file with a photo and every $16^{th}$ is part of a command string... this would be more difficult to detect
- To be 100% we need to disconnect...
- Governments keep disconnected network communities...
- BadBios (Nov. 2013) claimed to infect through 'radiation' –  has not been confirmed by anyone obviously

### *Safe Electronic Contact Procedures*

(It is not feasible to disconnect 100% from the outside world, as use of Internet grows)

- Use only commercially obtained software or any software which you can trust the source 100% - where vendors are reliable and well established.
- Test new software on an isolated computer. Alternatively in a VM, or using Sandboxie. Test with an up-to-date scanner.
- Open attachments known to be “safe”. An unknown source is not “safe”... Also a known source with a peculiar message should not be trusted

### *Safe Electronic Contact Procedures*

- Make a recoverable system image and store it safely. Use it to reboot securely. Prepare it before infection as afterwards it is too late.
- Make and retain backup copies of executable system files. Use inexpensive media CD/DVD's... You want to start with a clean system.
- Use virus detectors. Update them daily. Windows Defender is not enough. Look at Virus Bulletin tests.