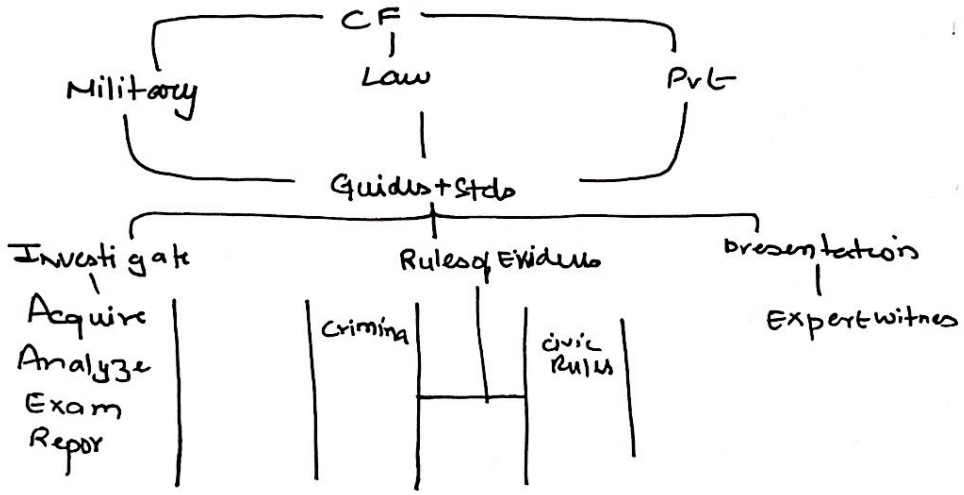
Basics of Cyber Forensics

→ For the preservation, identific, extract, doc & interpret of computer media for evidence or court.

→ used to supplement investigations.



Digital forensic science

" The use of scientifically derive & proven methods to preserve, collect, validate, id ~~and~~ verify, interpret, document & present digital evidence doing from source for the purpose of facilitating or furthering process of forensic investigate (under criminal nature). or to anticipate unauthorized actions".

	1st	Sno	Envt
Law	Prosecute		After
Military	continuity	Procedu	RTS
Bussines	Aval	Procedu	RTS

cf
- Network
- Small scall devices
- Storage
- Cloud.

Cyberforensic

↳ the scientific way to examine & analyze data to use as ~~evidence~~ evidence later.

Requirements

1 Hardware
- Familiarity with all devices
- understanding of HDD
- " of MoBo & chipsets
- power & memory use

2 BIOS
- How bios works.
- Setting & limits of bios.

3 OS
- DOS
- UNIX
- LINUX

4 S/W
- familiarity with s/w packages.

5) Tools
- familiarity with tools.

Handling Evidence

Admissibility -

→ Legal rules which determine is something can be used.
→ obtained in a manner that keeps authenticity & validity

- No evidence must be damages, destroyed or compromised by the CF.
  - Prevent introduction of viruses.
  - The Extracted info is handled properly & stored.
  - Maintain chain of custody
  - Limit amount of business operation effect
  - Respect client-attorney info.

Initiating an investigation

Don't work randomly on the fs

1. Establish evidence custodian & start a journel with date & time + info
2. designate suspected machines as off limit & including backups, change.
3. Collect Email, DNS & Network logs.
4. Capture exhaustive TCP & UDP portinfo.
5. Contact all relevant authorities.

Response

1. Identify / designate / become evidence custodian.
2. Review existing journal ~~note~~
3. Start & maint the journel.
4. Install the monitoring tools.
5. make a copy of disk without rebooting or affecting running processes.
6. Network info
7. Proces & files in use
8. config info
9. Reciept & sign date

Data

volitile

- Network info
- Active Proces
- Logged on users
- open files

Non volitile

- info that is presistent
- access by disk mapping
- make a back up copy.

CF Activities

I S I E P A

1. Secure data
2. Identify suspect
3. examine suspect
4. present findings
5. Apply laws.

Acquire ; Authenticate ; Analyze

Crime Scenes

" When a crime is committed, something is always left behind "

Digital evidence

↳ Digital data that establish occurrence of crime.

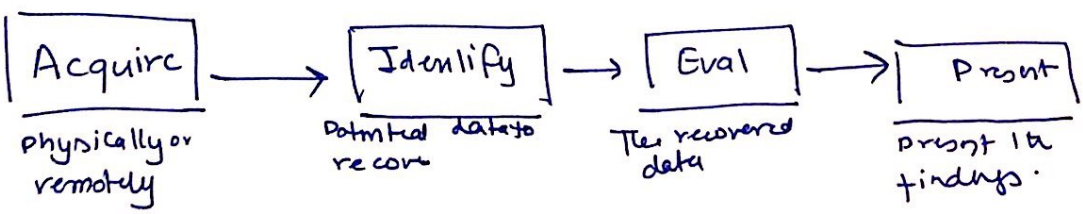
Digital Crime Scene

↳ Electronic evnt where digital evidence can exist.

Principles

↳ evidence is Volitile
↳ any mod is irreversible
↳ Acceptance is based on best evidence principle
↳ Printouts, stats.
↳ Chain of custody is crucial.

1) when dealing with evidence all general principles apply
2) upon seizing data make sure its not changed again.
3) only trained people should access the OG data.
4) All activities should be fully documented.
5) An individual is responsible for all actions while the data is in their production.
6) All agencies responsible for buying, storing & Info must comply.



① Identification

→ ID potential containers of evidence
eg smol devices, nontraditional media, multiple crime scenes.

→ Keep context of invest in mind.

→ Do not operate in a vaccuum.

→ Don't forget non electronic media.

② Collection

→ minimize contamination.

→ collect or seize

→ make forensic images.

→ Document what you collect.

→ Imagine
  → make 2 copies / don't work on OG.
  → copies ≈ OG but not copy = OG

→ The evidence can be duplicated without degradation

→ use write blockers. [HW. SW.

→ Copy with bitstream ie bit-by-bit copying data.

→ residual data is key.

→ make checksums.

③ Examination

- High level look over sys
- verify integrity
- Recover deleted files
- Determine k/w list
- Determine timeline
- Examine directory tree.
- do k/w search.
- Look for the obvious.

ISSUES

- Lack to certify tools
- Lack of STD
- Lack of certification for pros
- Lack of understanding by Judicious
- Lack of curriculum
- Rapid changes in tech.
- Immature Discipline.

Evidnce Guideline

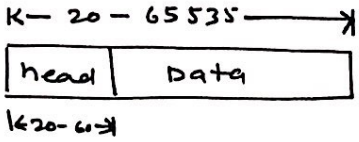
1. shutdown sys (consider volitile data)
2. Document H/w of system
3. Transport to safe location
4. Make Bitstream copies.
5. Authenticate all divices
6. Document Sys Date & time.
7. Make list of H/w
8. Eval swap
9. Eval stack
10. Eval unalloc space.
11. ~~Eval~~ Search Files, stac for keywords.
12. Document nams, Dates.
13. ID anomalies
14. Evaluate Functionality.
15. Document Finding
16. Return evrything used.

IP header Analysis

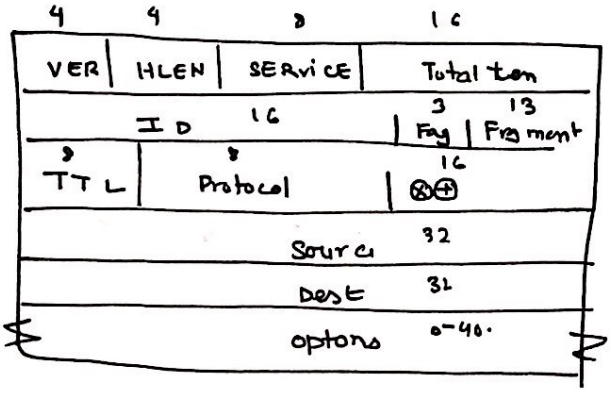
- IP is the transmission mech of TCP/IP @ Network.

Datagram

- Packets @ Network layer.
  - variable lenght
  - 20–60 byte header
  - In 4 byte sections.



IP HEADER



Servia : 6 | 2 — codepoint | X

XXX 000 precedence

X XXX ## Differentiated.

0 → Inet
11 → local
01 → Temp.

Total len gives total len of data gram not of header.

data < 46 byte then add padding.

Q1) 01000010 first 8 bit is acc/rg

VER = 0100 = 4 ✓

HLEN = 0010 = 2×4 = 8 ✗ corrupted

Q2 HLEN = 1000 = 8×4 = 32 = HLEN ⇒ 12 by

Q3. HLEN = 5_{16} Total len = 0028_{16}

Header = 20 byte.

Total = 40 ⇒ 20 byte of data

Q4 45 00 00 28 00 01 00 00 01 02

get No of hops

⇒ TTL = 8 bytes = 16 hex chars

= 01 = only one hop.

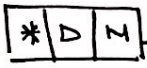
Fragmentation

- goes through diff networks
- each router decap & encap to another.
  - recieved = frame'work of arriva.
  - sent = frame work of sending.

MTU: Max transmission unit.

- only the datagram is fragmented.

Flags :



→ More frags exist.

↳ Do not frag

Q5 M = 0

it is the last frag but we cannot say if it was a part of frags

Q6 : M=1

→ Frag ? : yes ; Location ? No

Q7 : M=1 ; offset = 0

⇒ First of the frags

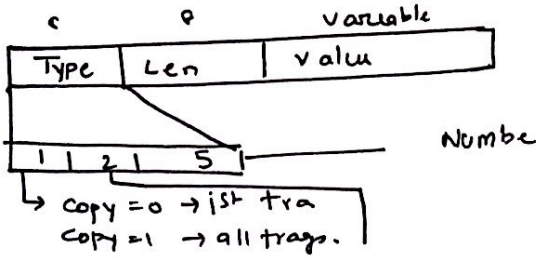
8 : offset = 100 ; HLEN = 5 ; total = 700

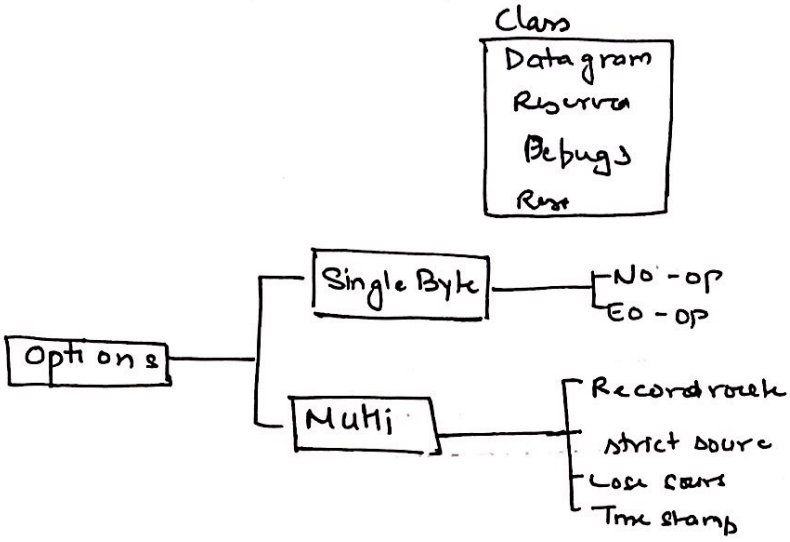
First = 800 total = 8100 hlen = 20

⇒ ~~of the~~ ⇒ first: 800 last = 879.

Options

↳ Not needed but can be used for testing & debugging.





Check sums

↳ Error detection method.

↳ done at sender value add & sent.

↳ only covers the ~~data~~ header not the data.

Android Malware Detection

- Mobile OS's made OS's more popular
- Types of OS's increased each having security holes
- security holes made attackers interested + No AV.
- New tasks needed.

Android Malware

- Mostly made on a Java backbone
- Run on the Android Runtime Engine (4.4 + up)
+ Apps are kept as APK files.
+ App is first compiled and then archived to APK will all parts.
+ APK = Zip(Bytecodes, resources, certificates, manifests)
+ On installing its copied to
  - → System apps : /system/app and
  - → user : /data/apps.

Forensics

↳ Apk has 3 main parts : Signatures, Bytecode, resources.

- Signature: # of the APK to check integrity.
  - experts can collect signatures to speed up id process.
- ByteCode : The executable part @ classes.dex in the APK
  - has the compiled classes as bytecodes.
  - Bytecode → instructions @ Android Runtime VM
  - ARVM is Register based
  - Apk can also have a catalog lib.
- Resources : The non executable part
  - UI
  - Manifest.XML : contains permission info for the apps
    : some apps use these.
    : Analyzing this is the most important step.

Malware Detection

- using hash.
- collect hash from a database i.e playstore.
- If the two hashes don't agree, the app may be a malware.
- Also can be done be checking for suspicious permission req.
  ↳ many people ignore it.

Anti forensics + Counter Measures

1 Obfuscation

- Save a function in a way to maintain its utility making the code hard to analyze & understand.
- Expert makes decompilation before the obfuscating
- ApkTool gets the .dex bytecode
- Dex 2 Jar and JD-GUI are used to decompile to Java.
- Edit the Java code, delete empty classes, correct errors, rename etc.

2 String Encryption

- Encrypt the string of MW.
- Eg XOR, Base64, AES, DES
- They not only check system props but also IMSI.

Malware Analysis

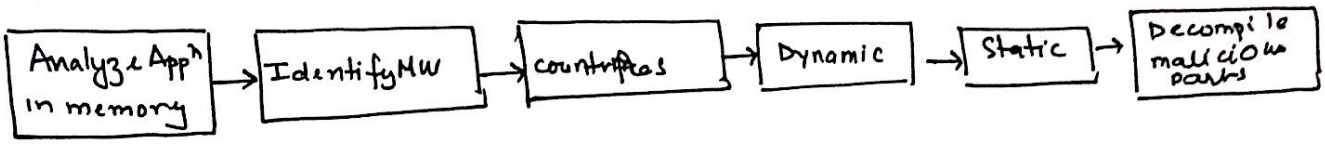
Static, Dynamic, Post-podium.

- Malicious Activity
  - Dynamic: Expert deals with behaviour features & interactions with system, collected data, network connection.

Study Dynam:
- Study the program as it runs
  - Debuggers
  - Funct call tracers
  - Emulators.

→ Dynamic can be done quickly

→ WYSIWYG



Static: No code execution

tools : Disassemblers.
: Decompilers.
: Sourcode analyzers.

- Reveals behavior under uncrucial cases.
- Examine parts that usually don't execute
- It is impossible to fully predict the behaviour.
- The main task it to find the malicious code.

1) ApkTool
2) DexJJAR & JD-GUI.

- **APK Tool**
  - ↳ allows disassembly of malware.
    - → The Android Manifest : permission info
    - → res catalog : The XML files to describe app templates & required image files.
    - → Smali Catalog : smali files the operational code (Notepad++).

Post Mortem

- ↳ Study by looking at the behavior.
- ↳ Analyzed data includes.
  - Local / Remote Loggers.
  - Changes to file contents.
  - Deleted files.
  - Data @ Swap space.
  - Data still lingering in RAM.
  - Information recorded outside the system.

The cyber world

- **Cyber space**
  - Envt wher people, s/w & devices interact
  - Maintained by WHOM
  - Includes : comps, Net s, s/w, HDD etc.
  - A virtual medium that active 24x7x365.

Cyber Security-

- Tech - procedures to safe guard resources from unlawful admittance.
- ISO 27001 IS Mgnt std.
- **Policy-**
  - An authority framework that defines & guides the activities of security
  - provids the outline to effectively protect info.
  - Manages the entire field of ICT users.

Cyber Crimes

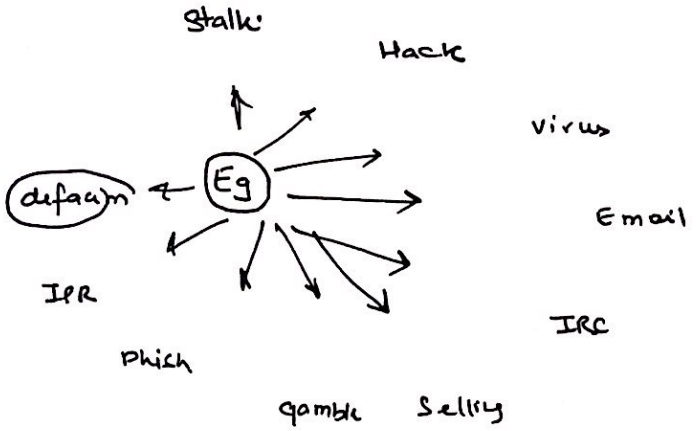
- crime @ complered.

" a criminal activity where a comp/Net is used as a tool or target of a crime ".

As a tool: The individual is the target then comp is a tool
→ stalking, theft.

As a target: done by select people with knowledge by doing series of attacks in a planned manners eg
→ defacement, cyber terrorism.

cyber crime —
- Person — harassment, stalking
- Property - IPR Theft, Validating
- govt/firm - terrorism, piracy
- Society - gambling, selling kinderjoys in USA



Unauthorized access

- any access without permission
- Hack/cracking: gaining unauthorized access.

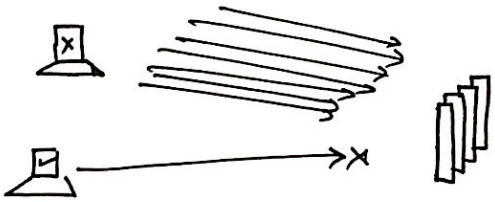
IT Act 2000 : 200K fine + 3 years

Why? : Personal gain

Viruses worms

- self replicating & propagating.
- Piggy backs.

DoS



Email

- Spoof: fraud email with intent to cheat
- Spam: Bulk mail
- Bombing: Sending huge volume of mail eg > inbox overflow.

Sale : Meth, ARIS, Rhinos.

Phishing : Disguise : 100.

IPR : Piracy, copy Right Inf, trade mark voilation.
Eg Satyam Infway : Squatting.

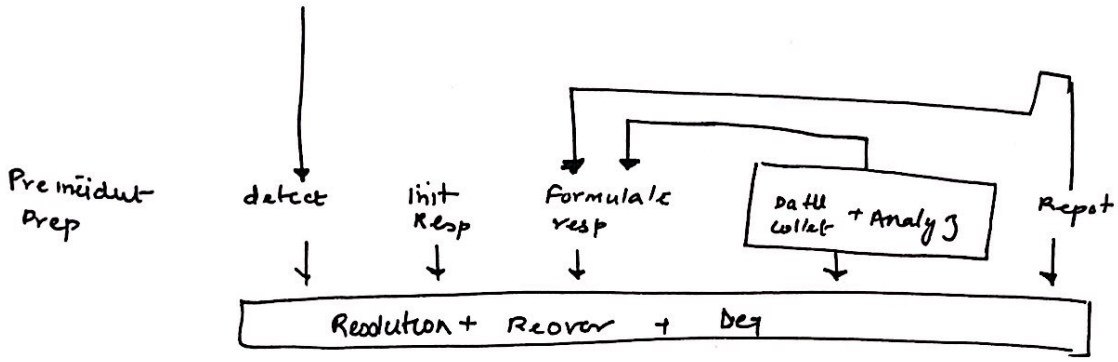
Defacment : self explanitory.

Stalking and vandalism : self explanitory

Live data Collection

– Windows Environment

Incident response



Goals

- obtain enough data to determine response
- consider totality of info.

Two Goals

- confirm the incident occured
- Retrive system data. (volitile)

Creating a response Toolkit

- Plan to obtain all info without affecting any thing
- Collected the required files on a CD.
  - ↳ quick respon,
  - ↳ Pro.
  - ↳ succ.

Eg tools: cmd.exe, NTRK, net stat, crypt cat, Fport.

- GUI : Not recommend due to the background activities they do
- CLI : Yep.

Preparing

Label the Toolkit media

check for dependencies

create Toolkit checksum

write protect any floppys.

Storing the Info obtained

- The powered on system.
- The envt is untrusted.

1. To a HDD.
2. To a notebook.
3. To removable data.
4. To remote system.

Eg NetCat
→ creates connection b/w workstation & device.

Integrity - [MD5 sum]

- Protect from modifications
  - do the check sum infront of witness.
- Run trusted commands on NT server
- Send files to work station
- Get MD5
- Do the invest.

Encryption

- Cryptcat (same funct & syntax as netcat)
- eliminates sniffers.
- Eliminate contamination.

Volitile Data

- System date & currently logged in users.
- Time stamps
- running process
- App° listening for sockets
- systems with recent connections.

Organization & Documentation

- work info which can be used as evidence
- Protects the organization.

create tool Hashes
make sure the Hashes are signed & verified by witnesses

Collecting Volitile Data

1. Execute trusted cmd.exe
2. Record systime & date
3. Determine logged users
4. All files get modb, creatn & accessn. — Dir
5. Determine open ports — fport
6. App^{n} associated with ports
7. Running apps — PsList
8. all recent connects — Netstat. — Arp cache → IP : MAC
   Nbtstat gives remote NetBIOS.
9. Document the commands used. doskey /history.

To know abnormal fun'n we need some baseline.

Scripting the resp.

→ can be done to a .bat file.

```
time /t
date /t
psloggedon
dir /t:a /o:a /a/s C:\
netstat -an
fport
psList
nbstat -c
time/t
date/t
doskey /hist
```

In Depth Live Response

- Date & time
- PsLoggedON
- Netstat
- PsList fport
- Setebak / Encore.
- NTRK
- Pwdump 3e
- NTLast

Collecting live data:

- Event logs
- Registry
- system Pass
- Dump RAM.

- getting Event Logs.
  - auditpol : discovers the await policies
  - NTLast : monitor successful & failed logons
  - Dumpel : retrieve remote logs.
- Reviewing Regs
  - Regdump: textfile dump of reg.
  - queries only get the Key value.
- System Passwords
  - pwdump3e: get pw from sam file.
  - Crack with John or similar tool.
    - Rainbow tables.
    - get dump of ram too.

- Decide
  - ↳ Is the duplicate needed?

- UNix Environment
  - └ create Tk
  - └ store info
  - └ obtain volitile info
  - └ collect
  - └ Deliton
  - └ trusted shell
  - └ info gather.

UNIX Quirks: allows deletion of program after it execute
: Versions are neither fwd or bwk compatible.

Creating Tru Kit

- distros need their own kits
- Keep a Tk ready
- only shell trusteds.

Storing Info
- └ Local HDD
- └ nano
- └ netcat (cryptcat.

Best time?
↳ optimum time for response:

Get volitile data ~~befor~~ during

- open socks
- Running Procs
- RAM
- Unlinked files.
  - files marked to delete when the process terminates

Data to collect

- Date & time
- current users logged on.
- Timestamps for the fs.
- running Procs
- open socks
- App^n listening open socks.
- sys with curr / recent connections.

Eg

↓

+ checksum.

Unix File Deletion

→ Unix keeps a file link count.
  - +ve int for no of files using it.

→ count = 0 ⇒ not in used ; delete.

→ when the attach file is deleted
  - Prog is removed from the dir chain
  - LC--
  - del^n time is set

(The LC ≠ 0 till proc ends).

Running Trusted Shell

2 modes · GUI → terminal

2 → Exit X windows, log onto console as root- ans ttyl.

to mount something

```
mount    /dev/fd0    /mnt/floppy
```

Gather info

- System date & time : date
- User : who.
- record file mods, access etc.

ls -alRu / > /Floppy/atime.
alRc /ctim
aln /mtim

Ports

Ports: netstat -an

Procurs: netstat -anp

Process in unix > windows

Procurs : Ps Commands.

Checksums.

- Record checksum of allfiles.
- Script the init responses.

- In Depth

- use dd, cat, netcat & dos to get logs, confics & others.

Rootkits avail

→ LKMs

→ unix kernel is one big beautiful program (Brian you beast).

→ LKMs can be dynamically linked to the kernel.

↳ Rogue LKM can intercept commands & create false.

↳ hide info & make backdoors.

Getting System Logs

@ /Var/adm or /var/log subdir.

use netcat, crypcat dd & dos.

Point of interest : Utmp, wtmp, Lastlog.

Processes accounting @ /etc/syslon.conf.

Finding Sniffers

- Increase the severity
- attacker had root.

/Proc File system

- pseudo fs to interface kernel DS.

/proc => accessing KDS and not files/directories.

each process gets a sub directory in the /proc to its PID.

. The EXE link in Proc allow recovery of deleted but running files.

. By checking the file descripse we can track all files is used by a process.

RAM DUMP

- UV Diff
- Dump /Proc/Kmem to remote.
- Kmem has the Ram but in a non contigious arrangment.

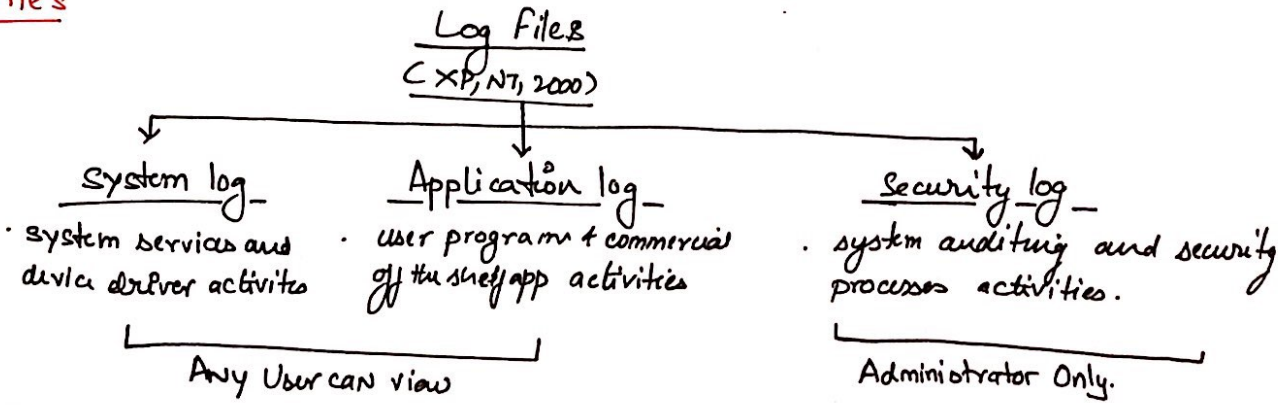
Investigating Windows Environment

- When to start?
  - Initial response is done, further investigation needed
  - Consulted from legal council
  - Duplication of evidence is done

- Where is the Evidence?
  - Volitile data in Kernel Data Structures.
  - Slack Space (can retrieve data of file which were deleted).
  - Free / unallocated space (can retrieve data on deleted files) including damaged or inaccisible clusters.
  - logical file system.
  - The event logs.
  - The registry.

- Steps in Windows Investigation
  1. Retrieve all pertinent logs.
  2. Perform keyword search.
  3. Retrieve relevant files.
  4. Identify unauthorized user accounts or groups.
  5. Identify rogue processes and services.
  6. Look for unusual or hidden files / directories.
  7. Check for unauthorized access points.
  8. Examine jobs run by the scheduler service.
  9. Analyze trust relationship.
  10. Review security identifiers.

- Log Files



Reviewing Logs

1. Determine which users have been accessing.
2. Determine who has been successfully logging in.
3. Determining who has been unsuccessfully trying to log in.
4. Track usage of specific files
5. Track alterations to the audit policy
6. Track changes to user permissions.

Viewing Logs on Windows

- Uses the Event viewer utility to access audit logs.

  Start > programs > Admintools > EventViewer.

- Select log to be viewed

  Eg Log > open > . . . . evt (mention the log type)

- The key decorator on an entry means a successful log
- The Lock decorator on an entry means an unsuccessful log / failure.

ID	Descp
516	Some audit event records discarded.
517	Audit log cleared
528	successful log
529	unsuccessful log / failed.
531	Failed log Locked
538	Successful logoff
576	Assignment and use of rights.

common IDs remember these

- Monitor processes run by an employee / counsel pushed you to have these.

Where to Find Evidence

- Monitor success and failure of detailed tracking
- With detailed tracking turned on, you can monitor every new process created.

  592 → New process created 593 → Process has exited.

- Can track virtually everything i.e any app opened / closed / edited / run.

Offline Investigation

→ Obtain copies of appevent.evt, secevent.evt, sysevent.evt from the forensic duplicates.

[\%systemroot%\System32\Config.]

→ To obtain these use
- → DOS boot disk.
- → Linux with appropriate NTFS drivers.
- → forensic duplicate.

→ If the forensic Computer/Workstation cannot read the logs then:

1. Disable EventLog Service of the workstation
   ControlPanel > Services > Disable EventLog > Reboot.
2. Use the user Manager to change the forensic workstation's audit policy to monitor Nothing at all.
3. Reboot and verify the steps taken are effective.
4. Place the 3 .evt files into default .evt location of workstation either make backup of the og or overwrite them.
5. Start the EventLog service from control panel.
6. State the EventViewer and proceed.

Drawbacks

- Windows does not log successful logons, file accesses etc.
- Only one event can be viewed at a time.
- Only log the source NetBIOS name rather than the IPaddress of remote system.
- Size and Time lenght of each log needs to be set seperatly.
- The description are populated using DLLs which may be corrupted/Not-available if viewed offline.

Keyword Search

- String searches on logical File structures or the physical level to examine the contents of an entire drive.
- Disk search tools do physical level string search, these need to be booted from a boot media.

  Eg> DtSearch, EnCase.

Pick the exact Words that provide useful results
The search should not adequately minimize the focus of the investigation

Reviewing Relevant Files

- Windows system write i/o to so many files at once that almost all actions taken on the system leave some traces of their occurence.
- Files like
  - → Source files
  - → Temp files
  - → cache files
  - → Registry : keeps track of recently used files.
  - → Recycle Bin : keep track of recully deleted files.
- Recognize files by their extensions as well as the true headers.
- Tools : EnCase, Quickview Plus.
- Investigator must be able to identify relevant files.

1. Incident time & time/Date Stamps

- scour network logs / get oral testimony of the time range when the incident occured.
- action days i.e days when the relevent acts took place.
- after identifying these events review time/date stamp encapsulated by them.
- Get a directory listing with file access, modify and creation times using dir.
- Use a tool (FileList) to get the details.

2. Proprietary Email files

- Use appropriate s/w to view suspects emails.

A Netscape Messenger Mail

- maintains mail as plain text files at:

  \Program Files\Netscape\Users\<user>\ Mail.

- Each mailbox has: indexfile (.snm), message text-File
- Mail is organized as INBOX | SENT.
- The content can be viewed using any text reader.

B Microsoft Outlook Mail

- Uses a proprietary format to keep mail.
- uses a *.pst extension, the *.pst file can archive all folders within outlook i.e cal, deleted files, Drafts, inbox, Journel, notes, etc. Everything except the Contacts folder.
- Location: Setting \<user>\Local Setting \ ApplicationData\Microsoft\Outlook
- To investigate, copy the .pst file into the workstation and open with outlook client.

3 Deleted Files and Data

- recovery of lost file which may have been deleted by malicious users.
- Ways:
  1. Undelete tools
  2. Restoring Files in Recycle Bin
  3. Recovering .tmp files
  4. Low Level tools to recover file system.

- **Undelete Tools**
  - Require use of native file system.
  - This is unfavorable as it will overwrite free space which may have valuable info.
  - Tools
    1. File Scavenger: Undeletes as long as the space occupied has not been used.
    2. Norton Utilities Protect: Acts as alt Recycle Bin. has auto delete after some time.

4. Recycle Bin

- Prevents accidental Deletion.
- Only cover recycle bin aware apps like Explorer.
- Cannot recover items deleted from command line.

- Recovering something from recycle bin
  - Find hidden recycle bin directory.
  - These are on the root directory of a partition /a
  - CD into this folder.
  - Use dir /a to view the hidden folder as well as sub folders.

5. Temporary Files

- Files may originate with any ongoing on windows
- have a *.tmp extension.
- These may recover very old items which were deleted like old PPTs or attachments.

6. Backup File Recovery

- NTBACKUP.EXE
  - creates a log file recording
    - date of backup
    - # of files backed up
    - # of files skipped during backup.
    - # of errors encountered.
    - time taken for the backup.
- This can be checked by simply searching for Backup.log and check if it was created by NTBACKUP.

7. Windows Registry

- Central hierarchical database to store information necessary to configure the system for >1 users.
- Replaces AUTOEXEC.BAT, CONFIG.SYS and INI files.
- Can reveal s/w installed in the past, security config, DLL trojans etc.

Use of Registry

- view what s/w has been installed
- To track unauthorized software and steganography tools, LOphtcrack & sniffers.
- To find s/w that were installed and then manually deleted.

Registry Root Keys

- HKCR : HKEY_CLASSES_ROOT.
- HKCU : HKEY_CURRENT_USER.
- HKLN : HKEY_LOCAL_MACHINE.
- HKU : HKEY USERS.
- HKCC : HKEY_CURRENT_CONFIG.

- Tools
  - Registry Reader.
  - Encase.
  - Regedit & Regedit32.
  # Never work on the ouginal.
  # Nakea copy.

Registry root keys are made from major files:
- SAM.
- Security.
- Software.
- System.

\WINNT\System32\Config.

- Offline Registry Investigation
  - Investigation using the forensic duplicate.
    1. Copy the registry root from the source to the forensic workstation
    2. Run Regedit.
    3. Imort these files by selecting Registry.
    4. Import registry files.

8. Web Browser Files

Tools: Internet Explorer History Viewer, Pasco, EnCase.

- Track recently used web pages.
- Browsers maintain cache of the recently viewed pages.

1. NetScape
   - The Netscape.hst file @: \Program Files\Netscape\Users\<user>
   - The Fat.db maintains another longer history file.
2. Internet Explorer
   - Index.dat holds the viewer history.
   - The HTML files are stored in the cache files.

- All of these are binary files.

- Dial Up Networking -

- Determine browsing activities of user by reviewing DUN settings
- Dial-on-demand allows automatic connection by apps.
- The autodial keep a list of IP addresses.
- rasautou-s allow to view autodial database.

Identifying Unauthorized User account or groups.

- use net stat from NTRK to view all domain accounts.
- Examine the security logs using Event viewer

632	NEW ACCOUNT
626	New user ENabled
636	changing acc group
642	user acc changed.

- Check the profiles directory :
  - If user acc exists and directory Not found then No user acc has log on ye
  - If directory is found and the user account is Not listed then the acc No longer exists
- Review SID where the user acc is deleted, it remains in the Registry
  Microsoft\ WindowsNT\ CurrentVersion\ProfileList.

Identifying Rogue Processes and Servics

- Use the most up-to-date virus scanner on wide volume of evidence.
- Tool : Pest Patrol

Looking For unusual or hidden Files/Directories

- To uncover hidden files which may be of some importance.
- NTFS Files streams can be used to hide data behind legitmate files. 4 to store multiple instances of files data in one file entry.
- Explorer cannot indicate presence of additional streams.

Eg> Netcat. (nc.exe) can be hidded as:

cp nc.exe logo.jpg : nc.exe.

The NC.exe within logo.jpg file entry is not reflected by file size but only in the time stamp.

Review Security Identifiers

- User / User groups are identified using SID.
- Each system has its own ID and each user has its own ID as well.
- Computer ID + User ID = SID, SID can unquely ID user accounts.
- SID do not
  - : apply to share security
  - : apply when remote access to a domain is provided.
- SID are like digital footprints that prove that a remote system was used to log on to a machine and access a domain.

Eg S-1-5-21-[10 digit]-[10 digit]-[10 digit]-500.

- 1 → Revision Level → denotes a SID
- 5 → ID authority
- 21-[10 digit]-[10 digit]-[10 digit] → Subauthority value
- 500 → Relative ID.

File auditing and Theft of info.

To identify users who has placed unauthorized files on a server.

1. Use a Network Based sniffer to monitor access to the file server. Or implement host based logs. [if the FS is not NTFS then audit not that easy]
2. Select directory to be monitored and choose the appropriate auditing.

Adding Success-and-Failure of File and Object access we can enable:

- 560 object open.
- 561 Handle Alloc
- 562 Handl closed
- 563 Object open for Delete
- 564 Objet Deleted.

in Windows 2000:

- 565 objet open
- 566 objet operation.

Checking For Unauthorized access points

- Any service which allows for some level of remote access.

  Eg> Terminal, SQL, telNet Daemons, Windows TelNet Server, FTP daemons Webservers, Port 5800 and Port 5631, PPP and PPTP, X servers.

- Tools: Netstat & Fport.

- These use API calls to read the contents of kernels and user space TCP and UDP.

- Remote Control and Access Services

  - Remote Control : PC Anywhere, VNC and Reach Out.
    - Allows absolute control over the system.
    - only one user at a time.

  Tools: Netstat, Fport, PsList.

  - Remote Access : Windows RAS
    - allows for multiple users (upto 256 connections)

  Tools: rasusers to list all the users, Net start to view running service.

Examine Jobs Run by the Scheduler Service

- An attacker can reconnect to the victims system by examining the jobs run by the victim system.

-

```
remote /s "cmd.exe" batman5.
```

This makes it such that no other system cannot connect.

```
remote /c <hostname> batman5.
```

↳ Name of NetBIOS of remote system. → Key phrase to connect.

- Jobs are scheduled using at or soon. At will show any jobs scheduled.

Analyze Trust Relationships

- Windows NT
  - Supports nontransitive / one-way trust.
  - If your NT-PDC trusts another domain, it doesn't need to trust your PDC.
- Windows 2000
  - Provides two-way / transitive trust.
  - Domains located within an active Directory forest require two-way access.