UNIT 4: INTRODUCTION TO COMPUTER FORENSICS INVESTIGATIONS & ELECTRONIC EVIDENCE :

Digital Forensics : authenticity, comparison & enhancement

- acquisition & analysis of digital evidence for its admissibility in the court of law. (motive)
- process – identification, preservation, analysis, documentation, presentation.
- Locard's principle – whenever 2 bodies come in contact an exchange of materials occurs between them. Expectations – recovery, searching, volatile
- Branches – Computer, Mobile, N/w, Forensic Data Analysis, Database, Email, Malware, memory, wireless n/w, Disks. Objectives – evidence, motive, tampering, acquisition, impact report, CoC
- Digital Evidence – latent, borders, altered, time sensitive
- Handling DE – recognize, siege, document, collect, label, pack, transport
- Important Documents and Electronic Evidence – List A (establish identity & employment auth), List B (establish identity), List C (establish employment auth)

Adv – integrity, evidence, info, track, money + time, prove Disadv – tampering, storing, knowledge, convincing, standards

Introduction to Evidence Acquisition :

- EBA – Identification → Collection → Preservation → Examination → Analysis → Presentation
- Identification – seizure, acquiring, analysis (FTK, Autopsy, Sleuth kit)
- Acquisition – photo, live data, n/w traffic, volatile / non-volatile
  - ↳ Challenges – guidelines, tech, big data, anti-forensic tech, tools, damage, volatile, lost, integrity
- Preservation – current state, power, login, install, connect, modify
- Examination – extracting, analyzing, copy, (Autopsy, bulkext, FTK, Encase, Magnet, CAINE)
- Analysis – what, how, who, controlled env.
- Presentation – clear, concise, forms / reports / photos / charts

Evidence Acquisition Process :

- Write Blockers – read only access to storage devices, chain of custody, soft / hard → chip, → workstation
  - ↳ Pros – reliant on single OS (not), easy, visual, interfaces, accepted, direct
  - ↳ Cons – kit, hardware, restricted, ext adapter, difficult, dependence
- Imaging Techniques – FTK Imager.
- Evidence Integrity – forensic soundness, MD5/SHA-1.
- SOP – acquisition & preservation.

MBR

Bootstrap code | Partition Table 1 2 3 4 | Boot signature

Introduction to Data Recovery & Carving :

- Data Recovery – lost or deleted data, software & hardware, Disk Drill / Recuva.
- Data Carving – reassembling files from raw data fragments when no file system metadata is available.
- Comparison – metadata, filesystem contents, memory, tools.

→ SOPs in DF – preinvestigation, decision on law, identification, collection, reporting, final

→ Chain of custody – documenting the handling of evidence, CCF

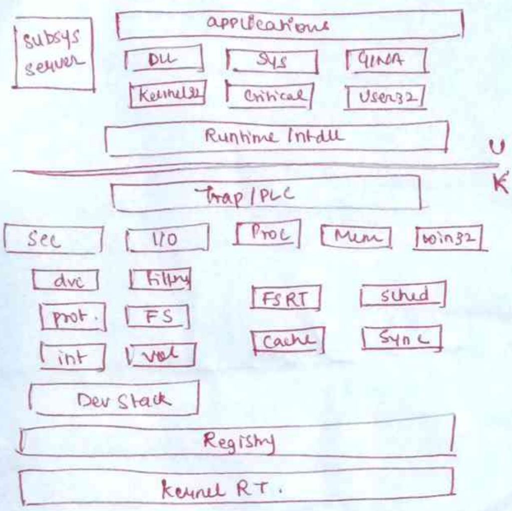
→ Windows OS boot process – POST, boot loader, Hardware, Kernel, logon

NTDLR BOOTMGR GRUB

UNIT V - FORENSIC ANALYSIS

MP4	14 66
PSD	38 42 50 53
GIF	47 49
ZIP	50 4B
IMG	50 49
JPG	FF D8
EXE/DLL	4D 5A

1) Windows Architecture – wmic os get architecture



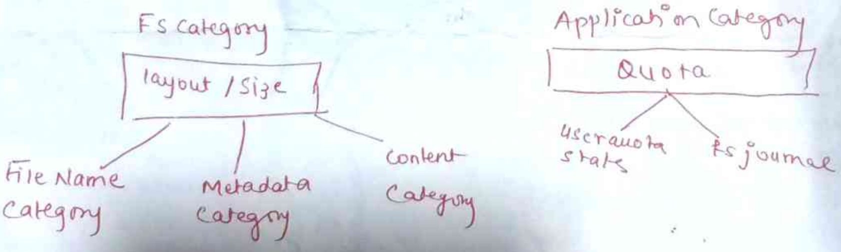
- Hardware Abstraction layer
- Kernel
- Executive Services
- Protected Subsystem
- Environment

2) Linux OS Architecture
→ hardware → Kernel → Sys Lib → Sys Utils
→ Desktop env → Applications

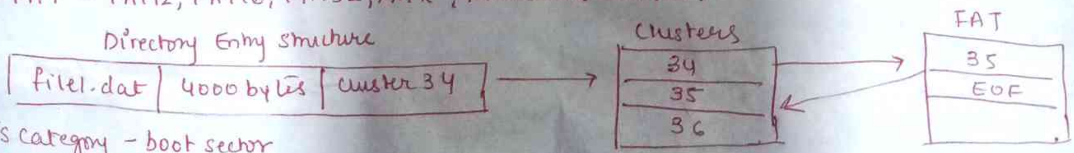
3) MAC OS Architecture
→ Kernel & Device Drivers → Core OS → Core Serv → Media → Application
→ Darwin OS – BSD Unix

2) Filesystems – DiskPart, EaseUS, AOEMI, Disk Management
hierarchy of files & directories, structural & user data, how data is stored & retrieved, ISO 9660 fs → optical disks ; func - storage mgmt, file naming, dir/folders, metada, access rules & priv ; files → groups (dir) ; files on a storage device is kept in sectors, groups of sector = block ; size, position, sector, attributes, ~~Fatr~~ file name, dir hierarchy

Reference model :



→ Aspects : Space mgmt, Filenames, Directories, Metadata
→ FAT – FAT12, FAT16, FAT32, FATX, Mic DOS & win9x, flash cards & thumb drives,



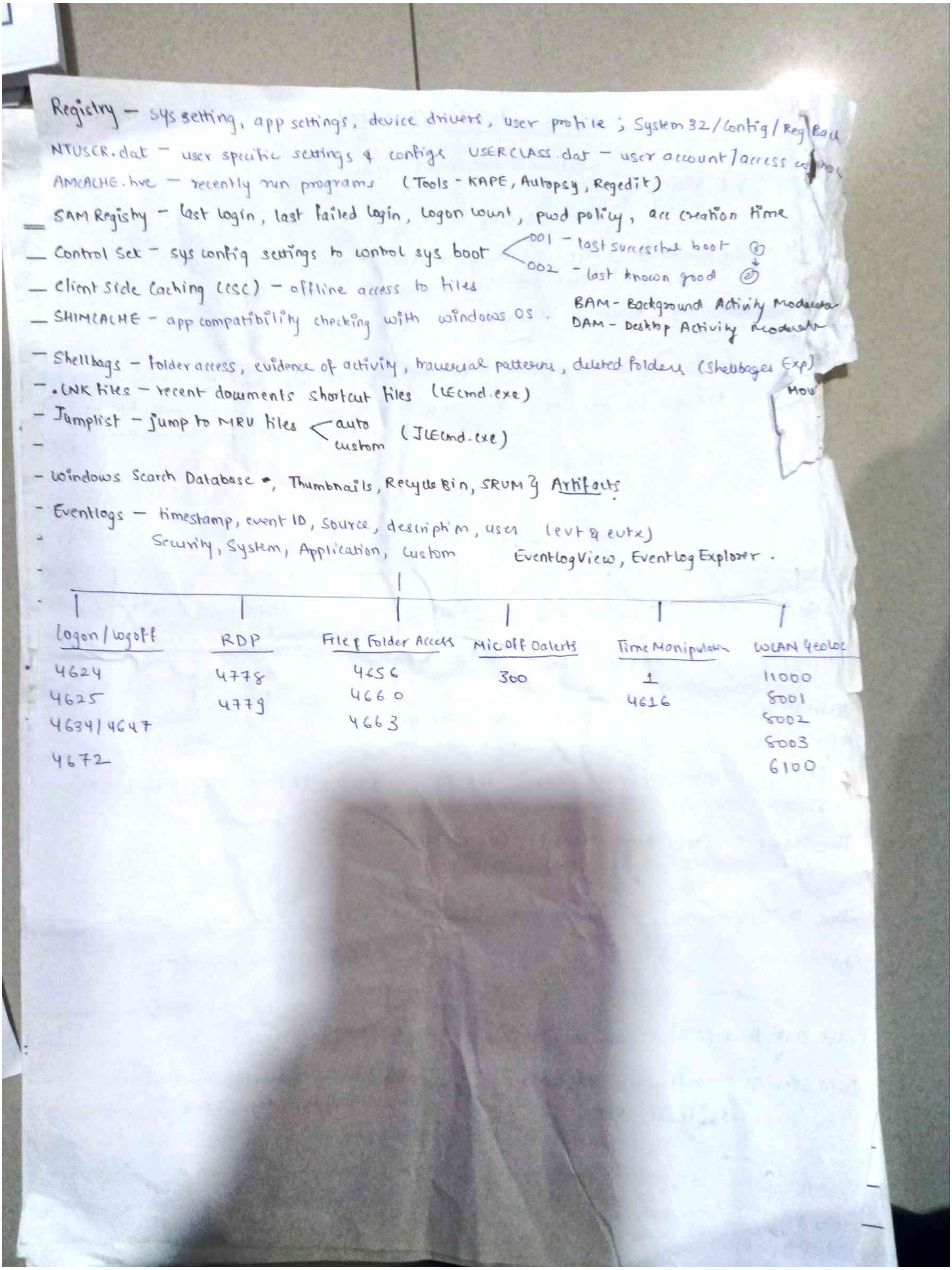
Fs category – boot sector

→ NTFS – win NT, reliability, security, large storage, scalability, MFT ♡ (1024 bytes), MFT Entry – 1KB, 42 bytes, ~~28 [illegible]~~
$MFT – on disk location of MFT . "FILE" "BAD" flag,
→ UNIX – /(root), inode ls -i
→ EXT2/EXT3 – Remy card, fast

Boot	B4 0	B41	B42	B4N

↳ Super block, Group desc, Data block bitmap, inode bitmap, inode table, data blocks.

→ NFS – allows remote hosts to mount fs over a n/w, TCP, UDP, rpc.nfsd, OS diff
→ HFS – 1985, Apple, 2TB ; 24B ; 255 char, B-Tree
→ File Type – file format, file extensions
↳ name ↳ content/struct
→ File Signature – verify contents, header, Hxd Editor



Registry – sys setting, app settings, device drivers, user profile ; System 32/Config/Reg Back

NTUSER.dat – user specific settings & configs USERCLASS.dat – user account/access config

AMCACHE.hve – recently run programs (Tools - KAPE, Autopsy, Regedit)

= SAM Registry – last login, last failed login, logon count, pwd policy, acc creation time

– Control Set – sys config settings to control sys boot < 001 – last successful boot ① ↓ 002 – last known good ②

– Client Side Caching (CSC) – offline access to files

– SHIMCACHE – app compatibility checking with windows OS.

BAM – Background Activity Moderator
DAM – Desktop Activity moderator

– Shellbags – folder access, evidence of activity, traversal patterns, deleted folders (Shellbages Exp)

– .LNK files – recent documents shortcut files (LEcmd.exe)

– Jumplist – jump to MRU files < auto / custom (JLEcmd.exe)

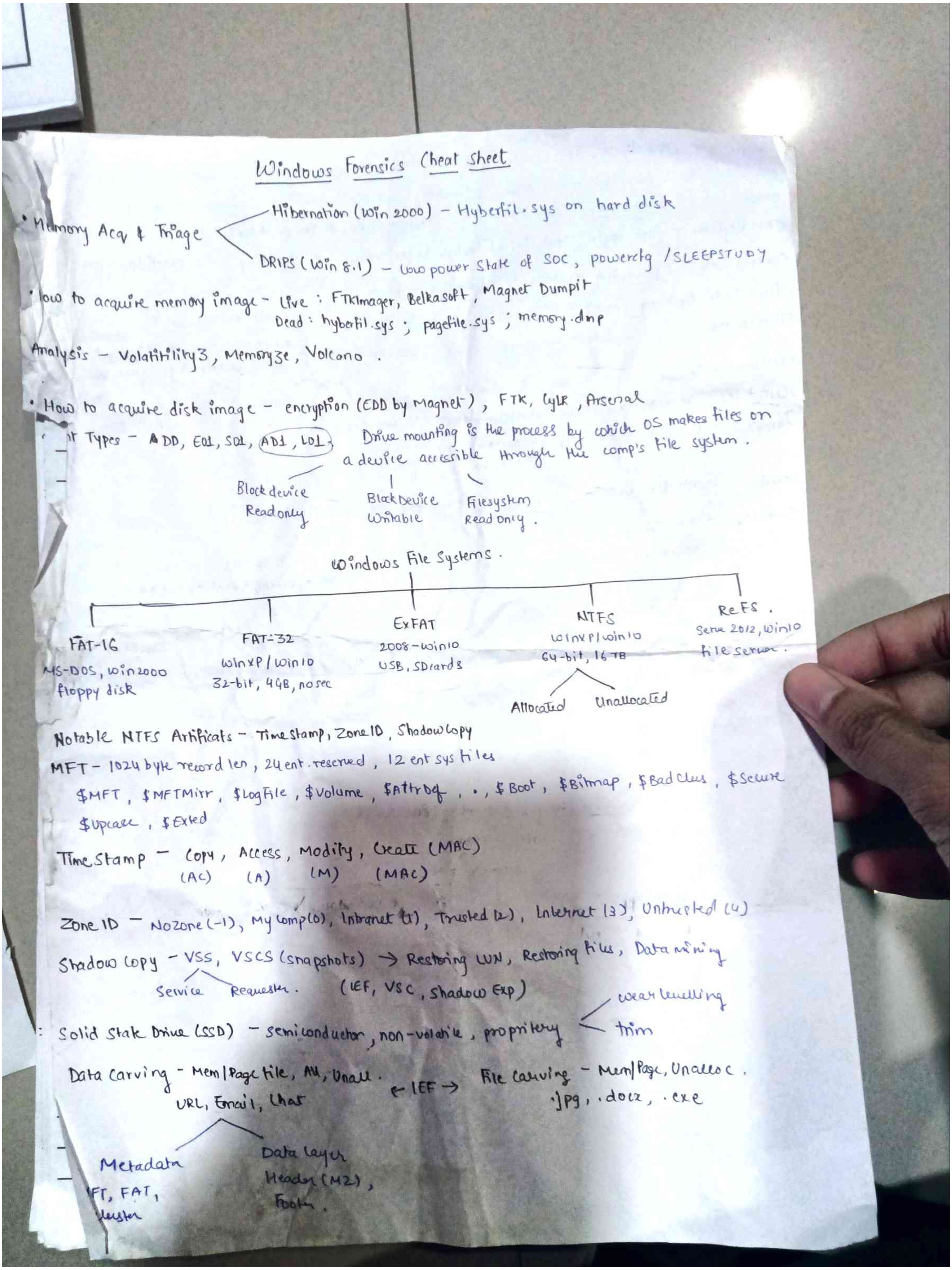
Mov

–

– Windows Search Database •, Thumbnails, Recycle Bin, SRUM } Artifacts.

– Eventlogs – timestamp, event ID, source, description, user (evt & evtx)
Security, System, Application, Custom   EventlogView, Eventlog Explorer.

Logon/logoff	RDP	File & Folder Access	Mic Off & alerts	Time Manipulation	WLAN Geoloc
4624	4778	4656	300	1	11000
4625	4779	4660		4616	8001
4634/4647		4663			8002
					8003
4672					6100



Windows Forensics Cheat sheet

- Memory Acq & Triage
  - Hibernation (Win 2000) - Hyberfil.sys on hard disk
  - DRIPS (Win 8.1) - Low power State of SOC, powercfg /SLEEPSTUDY
- How to acquire memory image - Live : FTKImager, Belkasoft, Magnet Dumpit
  Dead : hyberfil.sys ; pagefile.sys ; memory.dmp

Analysis - Volatility3, Memoryze, Volcano .

- How to acquire disk image - encryption (EDD by Magnet), FTK, CyLR , Arsenal

it Types - DD, E01, S01, AD1 , L01 - Block device Readonly

Drive mounting is the process by which OS makes files on a device accessible through the comp's File system.

Black Device Writable

Filesystem Read Only .

Windows File Systems .

FAT-16
MS-DOS, Win2000
floppy disk

FAT-32
WinXP / Win10
32-bit, 4GB, no sec

ExFAT
2008-Win10
USB, SDcards

NTFS
WinXP/Win10
64-bit, 16 TB
Allocated
Unallocated

ReFS .
Serve 2012, Win10
file server.

Notable NTFS Artificats - TimeStamp, ZoneID, ShadowCopy

MFT - 1024 byte record len , 24 ent. reserved , 12 ent sys files
$MFT , $MFTMirr , $LogFile , $Volume , $AttrDef , . , $Boot , $Bitmap , $BadClus , $Secure
$Upcase , $Exted

TimeStamp - Copy , Access , Modify , Create (MAC)
(AC) (A) (M) (MAC)

Zone ID - NoZone (-1), My Comp(0), Intranet (1), Trusted (2), Internet (3), Untrusted (4)

Shadow Copy - VSS, VSCS (snapshots) → Restoring WN, Restoring files, Data mining
Service Requester . (IEF, VSC , Shadow Exp)

: Solid State Drive (SSD) - semiconductor, non-volatile, propritery
- wear levelling
- trim

Data Carving - Mem/Page file, All, Unall .
URL, Email, Chat
Metadata
FT, FAT,
luster
Data layer
Header (M2),
Footer .

← IEF →

File carving - Mem/Page, Unalloc .
.jpg , .docx , .exe

Topic .... Date ....

UNIT V CONTINUED

→ windows Artifact Analysis – boot proc (CMOS configuration), tampering (malware)

→ Internet Artifacts – browsers (cookies, C:\Users\UserName\AppData\Roaming\Microsoft\windows\cookies – index.dat 256-byte records) (history (128 byte) (web cache 128) (emails – .PST, .OST)

→ OS Artifacts – swap file, recent, recyclebin, temp, restore, hiberfil.sys, Fav

→ FileSystem Artifacts – FAT, NTFS, Ext2, Ext3, Ext4, NFS, HFS, CDFS

→ Registry artifacts – regedit, hives (HKLM, HKU), key Pane, value Pane, HKCR HKCU, HKLM, HKU, HKCC, LastWrite (key ✓ value x), Keytime.exe, autoruns, MRU Lists, userAssist Key (ROT13), SSIDs (Static#). My Network Place, Computer Description Key, USB

low-level settings

→ Application Artifacts – application event log, log files, dynamic analysis

→ Log Analysis – stream of msgs in time seq, file/n/w stream, debugging, compatability, induce system for full domain

→ windows logs – event log, Event Viewer $\overset{\text{evtx}}{}$, C:\Windows\System32\winevt\logs App events (error, warning, info), Security (audit S/F), setup, System, Forwarded, log Parser (SQL)

→ Unix logs – syslog, /etc/syslogd, /var/log, System log Viewer

→ N/w log Analysis – packet captures (pcap), libpcap winPcap, Microsoft N/w monitor, wireshark, Tcpdump, logman, Registry

→ File System Analysis – essential fs data, non-essential fs data.

User Application configurations & Preferences

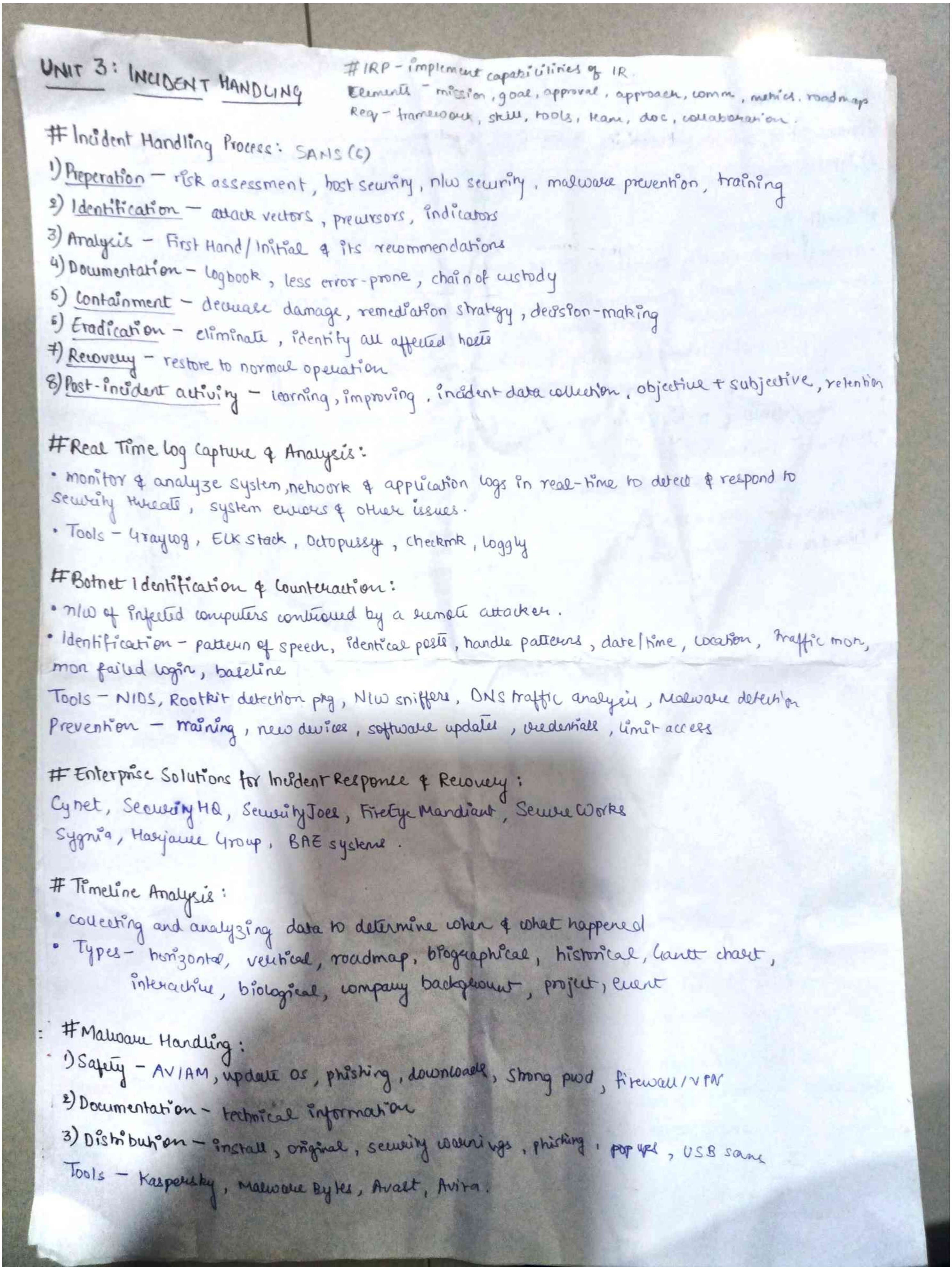
Attached devices – Device Manager

Shared location – File Explorer > Network

Installed Apps – HKLM\Software\Microsoft\Windows\Current Version\Uninstall

.evt – old .evtx – new

Teacher's Sign



UNIT 3: INCIDENT HANDLING

#IRP - implement capabilities of IR
Elements - mission, goal, approval, approach, comm, metrics, roadmap
Req - framework, skill, tools, team, doc, collaboration.

#Incident Handling Process: SANS (6)

1) Preperation - risk assessment, host security, n/w security, malware prevention, training
2) Identification - attack vectors, precursors, indicators
3) Analysis - First Hand/Initial & its recommendations
4) Documentation - Logbook, less error-prone, chain of custody
5) Containment - decrease damage, remediation strategy, decision-making
6) Eradication - eliminate, identify all affected hosts
7) Recovery - restore to normal operation
8) Post-incident activity - learning, improving, incident data collection, objective + subjective, retention

#Real Time log Capture & Analysis:

- monitor & analyze system, network & application logs in real-time to detect & respond to security threats, system errors & other issues.
- Tools - Graylog, ELK stack, Octopussy, Checkmk, loggly

#Botnet Identification & Counteraction:

- n/w of infected computers controlled by a remote attacker.
- Identification - pattern of speech, identical posts, handle patterns, date/time, location, traffic mon, mon failed login, baseline

Tools - NIDS, Rootkit detection prg, N/w sniffers, DNS traffic analysis, Malware detection

Prevention - training, new devices, software updates, credentials, limit access

#Enterprise Solutions for Incident Response & Recovery:

Cynet, SecurityHQ, SecurityJoes, FireEye Mandiant, SecureWorks
Sygnia, Harjauee Group, BAE systems.

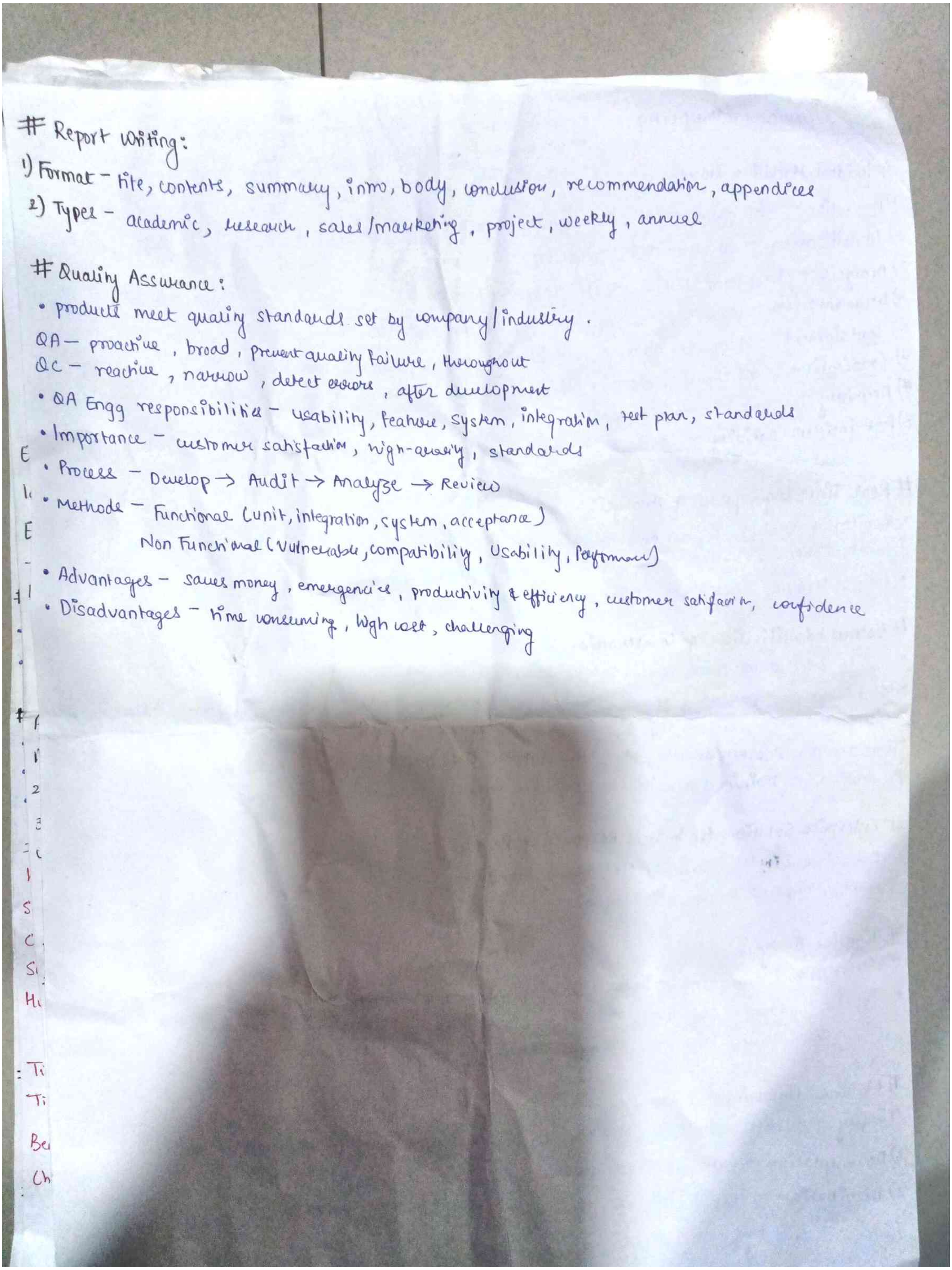
#Timeline Analysis:

- collecting and analyzing data to determine when & what happened
- Types - horizontal, vertical, roadmap, biographical, historical, Gantt chart, interactive, biological, company background, project, event

#Malware Handling:

1) Safety - AV/AM, update OS, phishing, downloads, Strong pwd, firewall/VPN
2) Documentation - technical information
3) Distribution - install, original, security warnings, phishing, pop ups, USB scans

Tools - Kaspersky, Malware Bytes, Avast, Avira.



Report writing:

1) Format - tite, contents, summary, intro, body, conclusion, recommendation, appendices
2) Types - academic, research, sales/marketing, project, weekly, annual

Quality Assurance:

- products meet quality standards set by company/industry.

QA - proactive, broad, prevent quality failure, throughout
QC - reactive, narrow, detect errors, after development

- QA Engg responsibilities - usability, feature, system, integration, test plan, standards
- Importance - customer satisfaction, high-quality, standards
- Process - Develop → Audit → Analyze → Review
- Methods - Functional (unit, integration, system, acceptance)
  Non Functional (vulnerable, compatibility, Usability, Performance)
- Advantages - saves money, emergencies, productivity & efficiency, customer satisfaction, confidence
- Disadvantages - time consuming, high cost, challenging

Incident Prioritization - never be handled on first come first serve basis

Functional Impact

None, low, medium, High

Informational Impact

None, privacy breach, prop. breach, integrity loss

Recoverability

Regular, Supplemented, Extended, Not Recoverable

Incident Notification - policies; who/what; communication channels (email, web, phone, VoIP, paper, in person).

Evidence Gathering & Handling - system of interest; chain of events; snapshots

Identifying attacking hosts - IP, OSINT, Databases, comm channels

Evidence Retention - Prosecution; Data Retention; cost

——— x ———

Data - set of characters; raw info

- Highly confidential
- Sensitive
- Internal Use Only
- Publicly Available

Data - CIA

People - AAA

Access control - selective restriction of access to some kind of resource.

1) DAC - user; permissions; CRUD

2) MAC - admin; security policy; compliance; central authority

3) RBAC - permissions → roles; roles → users; edit/modify/delete users

4) MLS - user → trust level; item → confidentiality level

Signs of an incident -

1) Precursors - abt to happen; rare; web server log entries, new exploit, threat

2) Indicators - already happend; common; IDS alerts, filname unusual

Incident Category

- High
- Medium
- Low

Defⁿ: Events, Adverse Events, Comp Sec Incidents, Security Incidents; Information Security Incidents

Identify/Report an Incident

- Event Mgmt (CI)
- web (ticketing)
- Phone (FCR)
- Email

Malware - virus, backdoor, downloader, launcher, rootkit, spyware, adware, scareware, spamware ransomware, key-logger, botnet.

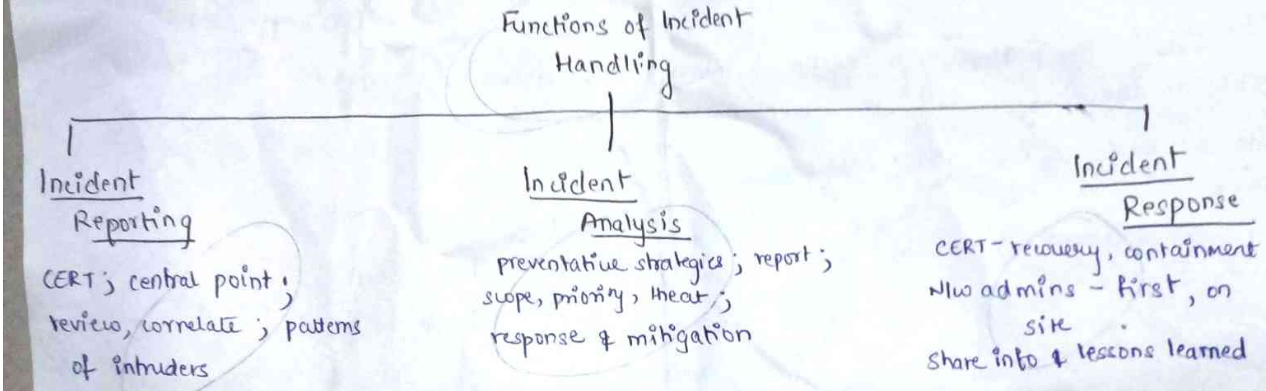
Hy

oals of Incident Response (x8) - Confirm; reduce impact; what; business continuity; prosecute
Keep mgmt informed; prevent future attacks; improve security & IR.

ncident Response Plan (IRP) - need - data compromise, unique req.
formal, focussed & co-ordinated approach to incident response.
roadmap for implementing the IR capability.

Elements of IRP (x8) - Mission; Strategies & goals; Senior mgmt approval; org approach; communication;
metrics; roadmap; how the prog. fits?

Requirements of IRP (x6) - framework; skilled resource; team; tools; documentation; collaboration



Functions of Incident Handling

Incident Reporting
CERT; central point; review, correlate; patterns of intruders

Incident Analysis
preventative strategies; report; scope, priority, threat; response & mitigation

Incident Response
CERT - recovery, containment
N/w admins - first, on site.
Share info & lessons learned

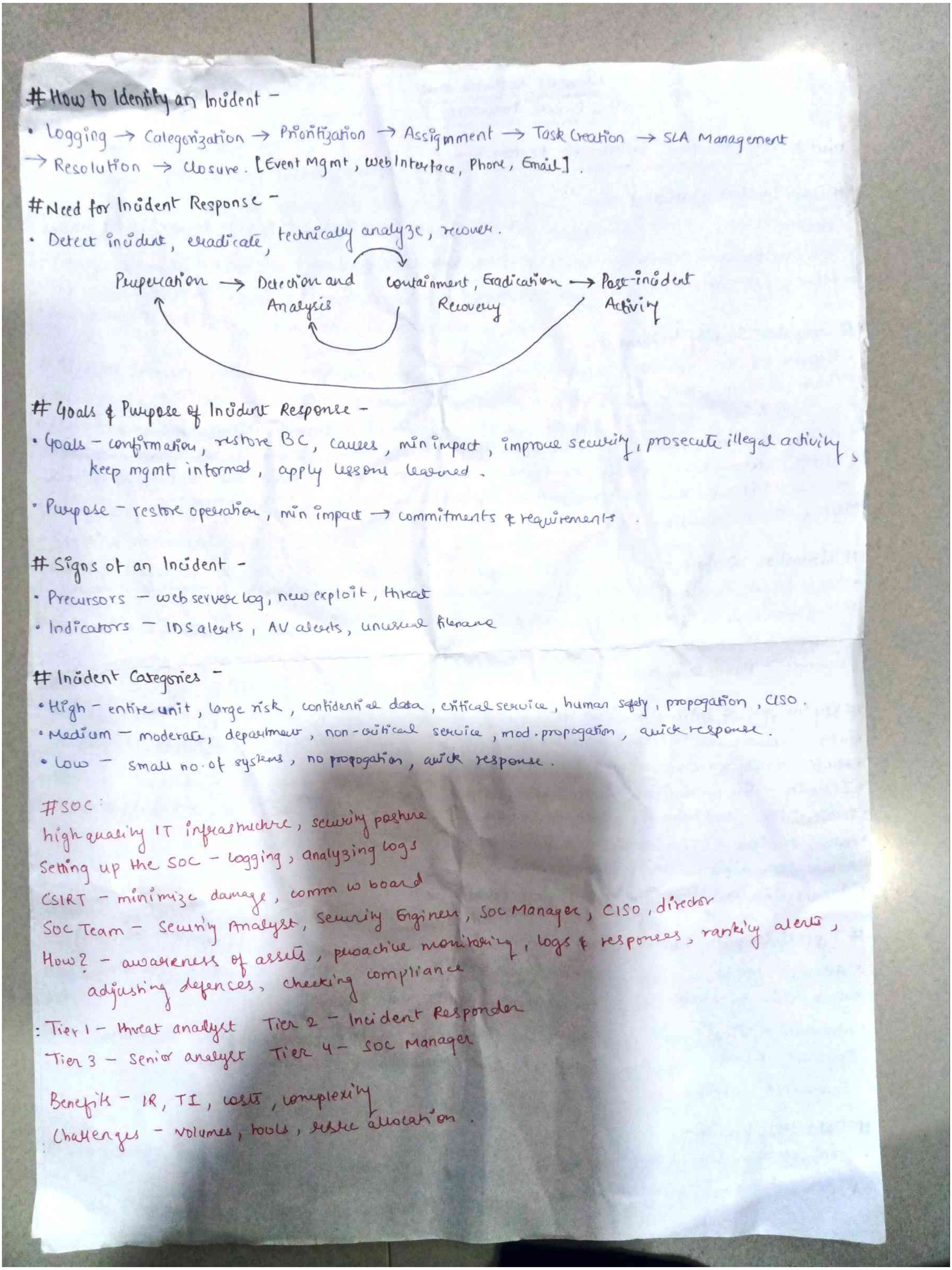
SANS Institute - SysAdmin Audit N/w Security; for-profit; US; 1989; cybersec training & certification; 6 steps to handlie incidents.

Steps of Incident Handling:

1. Preperation - prevention; risk assessment; host sec; n/w sec; malware prev; training
2. Identification - attack vectors; prec & ind - alerts, logs, public info, people
3. Containment - decrease damage; time; decision-making
4. Eradication - eliminate; identify infected hosts
5. Recovery - restore to normal; confirm; backup, clean files, patches, pwd, perimeter security
6. Lessons learned - learning & improving; meeting; objective & subjective; incident data

Incident Analysis - accurate precursors?; false positives; legitimacy
First Hand / Initial - profile; normalcy; log retention; even corr; clock syn.
knowledge base of info, search engines, packet sniffers, data filtering, help

Incident Documentation - logbook; start to end; error prone; time stamped
status; summary; indicators; other incidents; actions; chain of custody
impact assessment; contact info; evidence; comments; next steps



#How to Identify an Incident -

- Logging → Categorization → Prioritization → Assignment → Task Creation → SLA Management → Resolution → Closure. [Event Mgmt, WebInterface, Phone, Email].

#Need for Incident Response -

- Detect incident, eradicate, technically analyze, recover.

Pruperation → Detection and Analysis ⇄ Containment, Eradication Recovery → Post-incident Activity

#Goals & Purpose of Incident Response -

- Goals - confirmation, restore BC, causes, min impact, improve security, prosecute illegal activity, keep mgmt informed, apply lessons learned.
- Purpose - restore operation, min impact → commitments & requirements.

#Signs of an Incident -

- Precursors - web server log, new exploit, threat
- Indicators - IDS alerts, AV alerts, unusual filename

#Incident Categories -

- High - entire unit, large risk, confidential data, critical service, human safety, propogation, CISO.
- Medium - moderate, department, non-critical service, mod. propogation, quick response.
- Low - small no. of systems, no propogation, quick response.

#SOC:

high quality IT infrastructure, security posture

Setting up the SOC - logging, analyzing logs

CSIRT - minimize damage, comm w board

SOC Team - Security Analyst, Security Engineer, SOC Manager, CISO, director

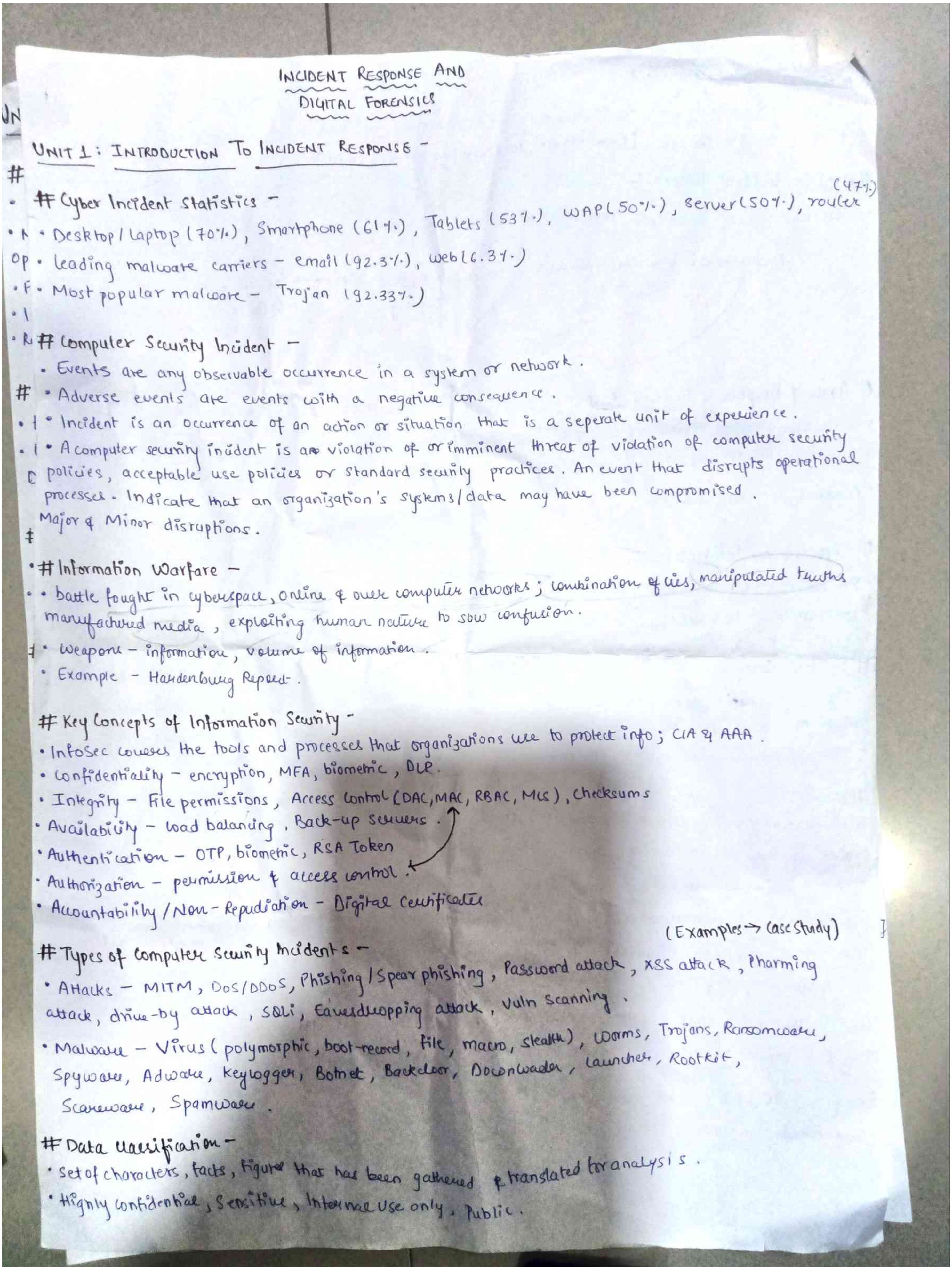
How? - awareness of assets, proactive monitoring, logs & responses, ranking alerts, adjusting defences, checking compliance

: Tier 1 - threat analyst Tier 2 - Incident Responder

Tier 3 - Senior analyst Tier 4 - SOC Manager

Benefits - IR, TI, costs, complexity

Challenges - volumes, tools, resource allocation.



INCIDENT RESPONSE AND
DIGITAL FORENSICS

UNIT 1: INTRODUCTION TO INCIDENT RESPONSE -

Cyber Incident Statistics -

- Desktop / Laptop (70%), Smartphone (61%), Tablets (53%), WAP (50%), Server (50%), router (47%)
- leading malware carriers - email (92.3%), web (6.3%)
- Most popular malware - Trojan (92.33%)

Computer Security Incident -

- Events are any observable occurrence in a system or network.
- Adverse events are events with a negative consequence.
- Incident is an occurrence of an action or situation that is a seperate unit of experience.
- A computer security incident is an violation of or imminent threat of violation of computer security policies, acceptable use policies or standard security practices. An event that disrupts operational processes. Indicate that an organization's systems/data may have been compromised. Major & Minor disruptions.

Information Warfare -

- battle fought in cyberspace, online & over computer networks; combination of lies, manipulated truths manufactured media, exploiting human nature to sow confusion.
- Weapons - information, volume of information.
- Example - Hardenburg Report.

Key Concepts of Information Security -

- InfoSec covers the tools and processes that organizations use to protect info; CIA & AAA.
- confidentiality - encryption, MFA, biometric, DLP.
- Integrity - File permissions, Access Control (DAC, MAC, RBAC, MLS), Checksums
- Availability - load balancing, Back-up servers.
- Authentication - OTP, biometric, RSA Token
- Authorization - permission & access control.
- Accountability / Non-Repudiation - Digital certificates

(Examples → case Study)

Types of computer security incidents -

- Attacks - MITM, DoS/DDoS, Phishing / Spear phishing, Password attack, XSS attack, Pharming attack, drive-by attack, SQLi, Eavesdropping attack, vuln scanning.
- Malware - Virus (polymorphic, boot-record, file, macro, stealth), Worms, Trojans, Ransomware, Spyware, Adware, Keylogger, Botnet, Backdoor, Downloader, Launcher, Rootkit, Scareware, Spamware.

Data classification -

- Set of characters, facts, figures that has been gathered & translated for analysis.
- Highly confidential, Sensitive, Internal Use only, Public.

UNIT 2: INCIDENT MANAGEMENT –

Incident Prioritization –

→ matrix (H, M, L)

- critical point in incident handling; never handle on first come first serve; impact & urgency
- Need – focus resources on high-priority; improve response time; align with business objectives; optimize resource allocation; ensure consistency.
- Functional Impact – None, Low, Medium, High
- Information Impact – None, Privacy breach, Proprietary breach, Integrity loss.
- Recoverability – Regular, Supplemented, Extended, Not Recoverable.

Disaster Recovery Technologies –

- tools designed to help organizations recover critical IT systems & data after a disruptive event.
- Data backup & recovery, replication, virtualization, cloud-based data recovery, high availability, Disaster recovery testing, rebuilding, replacing, patches, n/w perimeter security.

Impact of Virtualization on IR & Incident Handling –

- Creating virtualized copies of critical systems & data to deploy during disaster.
- Rapid provisioning, Isolation, Snapshots, Centralized Mgmt, Agility.

Estimating Cost of an Incident –

- Steps – Scope → direct cost → indirect cost → total cost → future cost → IR Plan update
- Cost to Business – cost code, direct & indirect cost
- Cost of Incident Mgmt – Throughput (T), Team Composition, Time Spent (P), Capital Exp. (C), Salary (Y), Overhead cost (H), Sum of all staff's cost (S)

Staff Cost Calculation = $B = (Y/100) * P \qquad S = B_1 + B_2 + \dots + B_n$

Cost Per Incident (CPI) = $\dfrac{(S + (S * H/100) + C)}{T}$

Incident Reporting –

- take appropriate measures to prevent similar incidents from happening in the future.
- steps – Incident reporting procedures; train employees; std reporting form; ensure confidentiality; evaluate incidents; lessons learned; keep records.

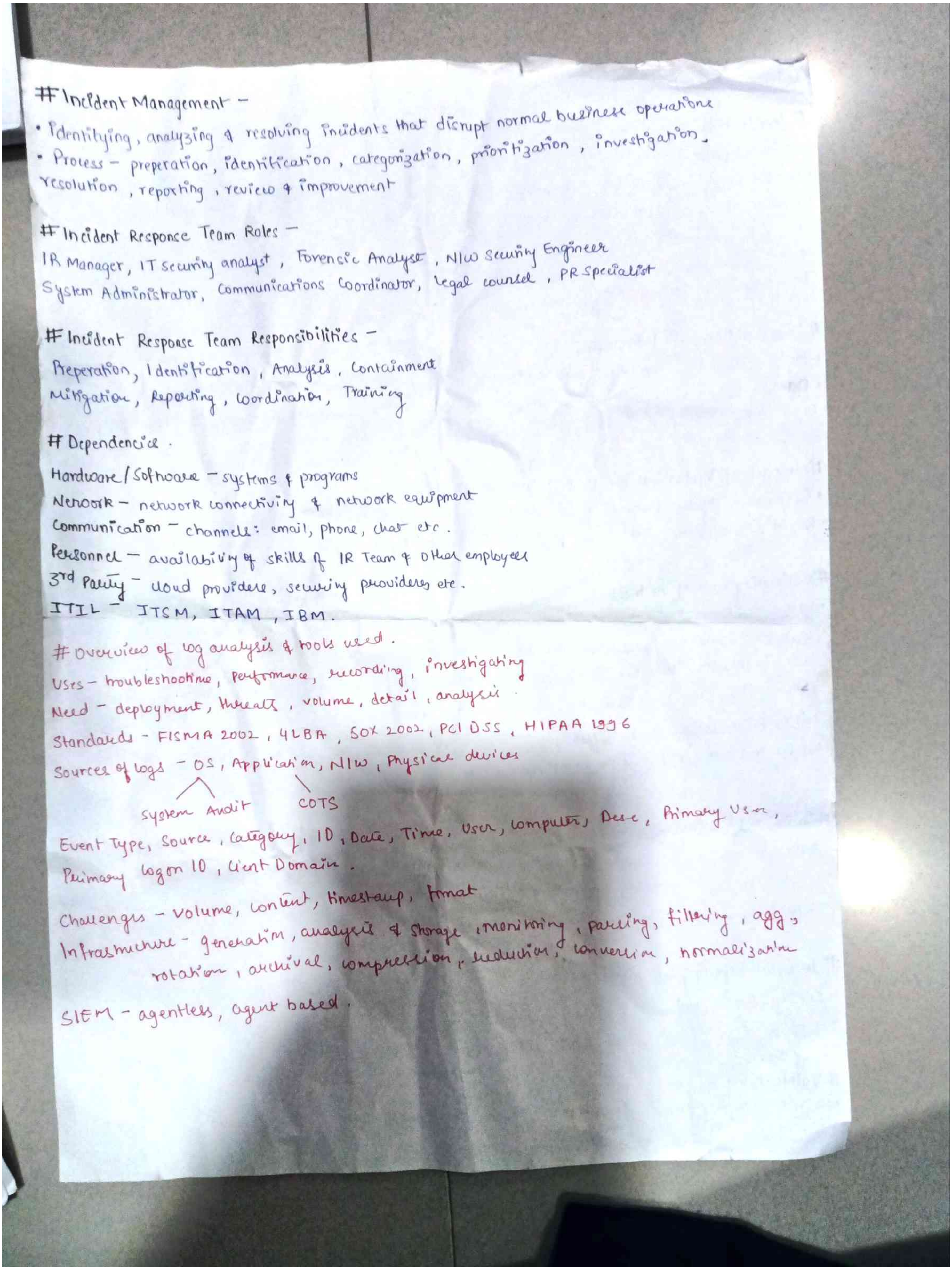
Incident Reporting Organizations –

- CERT, SANS, CISA
- NHTSA, CPSC, FDA, OSHA, FAA, NTSB, EPA, FEMA, USCG

Vulnerability Resources –

NVD, CVE, OWASP, NIST, Security Focus, Vulnerability lab

Secunia Research, ZDI, Microsoft Security Updates.



Incident Management -

- Identifying, analyzing & resolving incidents that disrupt normal business operations
- Process - preperation, identification, categorization, prioritization, investigation, resolution, reporting, review & improvement

Incident Responce Team Roles -

IR Manager, IT security analyst, Forensic Analyst, N/w Security Engineer
System Administrator, Communications Coordinator, legal counsel, PR Specialist

Incident Response Team Responsibilities -

Preperation, Identification, Analysis, Containment
Mitigation, Reporting, Coordination, Training

Dependencies.

Hardware / Software - systems & programs
Nework - network connectivity & network equipment
Communication - channels: email, phone, chat etc.
Personnel - availability of skills of IR Team & other employees
3rd Party - cloud providers, security providers etc.
ITIL - ITSM, ITAM, IBM.

overview of log analysis & tools used.

Uses - troubleshooting, performance, recording, investigating
Need - deployment, threats, volume, detail, analysis.
Standards - FISMA 2002, 4LBA, SOX 2002, PCI DSS, HIPAA 1996
Sources of logs - OS, Application, N/w, Physical devices
System Audit COTS
Event Type, Source, Category, ID, Date, Time, User, computer, Desc, Primary User, Primary logon ID, Client Domain.

Challenges - volume, content, timestamp, format
Infrastructure - generation, analysis & storage, monitoring, parsing, filtering, agg., rotation, archival, compression, reduction, conversion, normalization

SIEM - agentless, agent based.