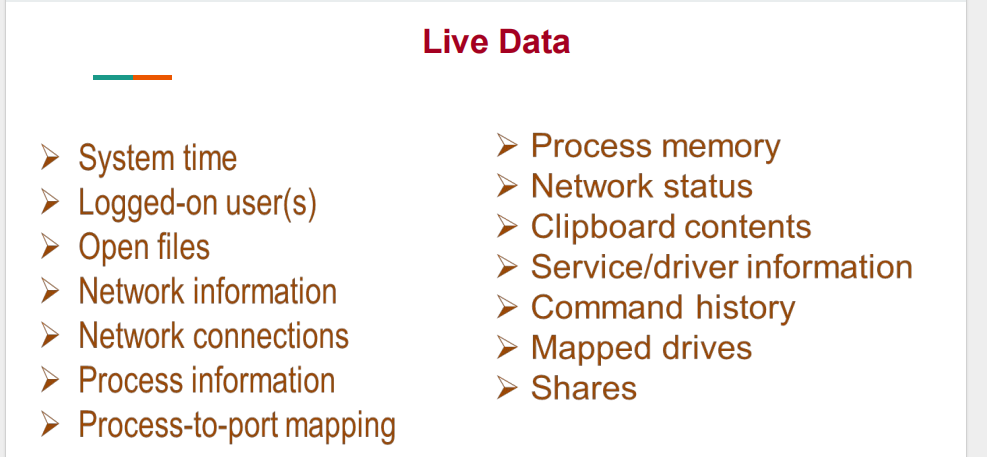
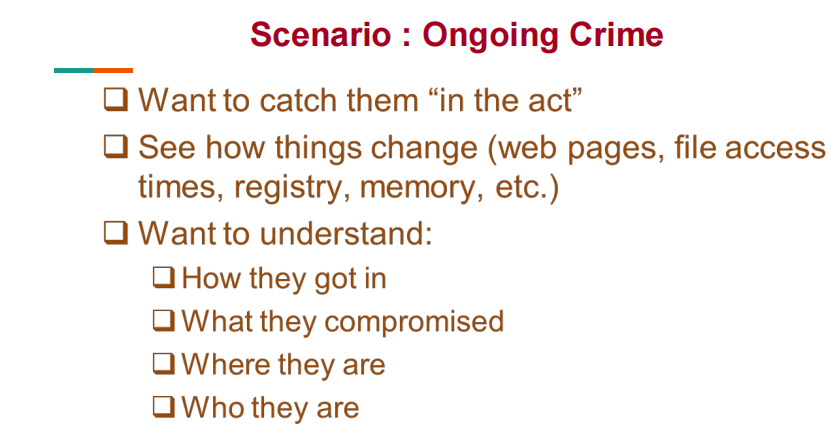
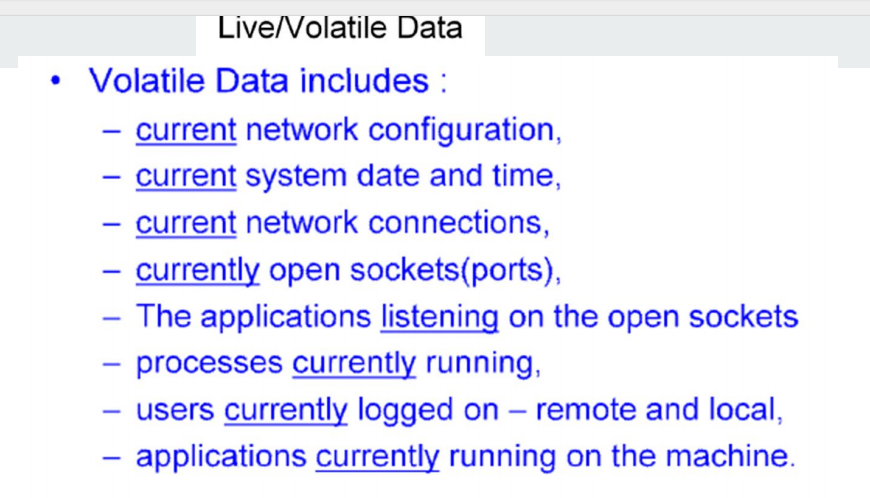
browser stores a lot of sensitive information about the

user and its surfing habit.

I think it as a great chance for me to gain an academic advantage which involves offerings of such a prestigious institute's program.

Issue the date and time commands again (repeat step 2) to record the time and date

that you completed the live data collection. This ensures that you have a record of

when you were on the system, so that if anything is changed on the system outside

this timeframe, you will know that you are not responsible for the alterati

▼ Run the date and time commands to sandwich your response between starting and ending times.

These commands record the current system time

Store the data to remote media such as floppy disks, USB drives, or tape drives.

Use netcat (or cryptcat) to transfer the retrieved data to a forensic workstation over the network.The next option asks if you would like to protect the image file with a password. We

never set this option. It does not truly protect the data from unauthorized access, because it is trivial to circumvent

honesty towards investigation

being fair

not hiding evidence: upholding

lawful

not being reckless

privacy of crime commiter or safety of public

honour property rights, copyright

credits to everyone deserving

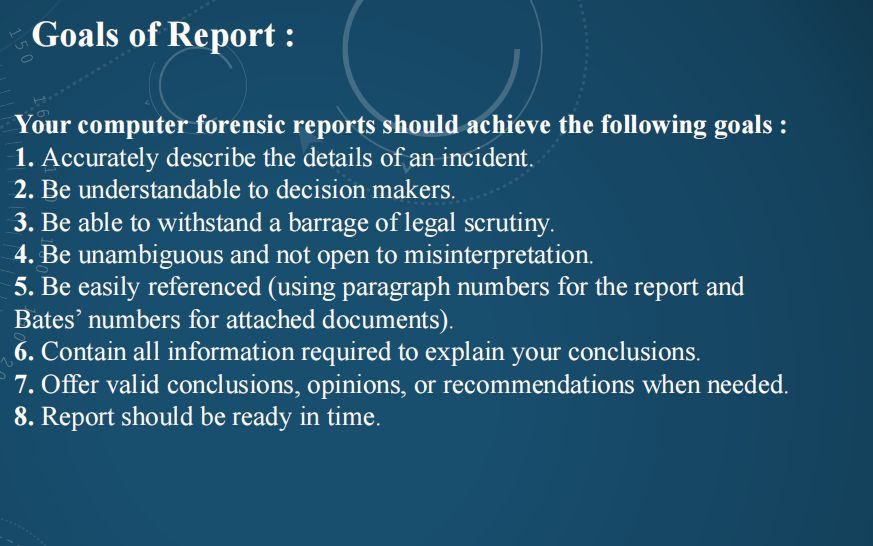
respect privacy

reveal clients secrets

have an opinion

create evidence when sure of killer vs staying truthful

minimize risk or effect to rest



**INVESTIGATIVE REPORT: std organized template format followed:**

Ok so this was the issue reported, TIMELY ASAP DOCUMENTATION + MICRO MACRO DETAILS: **EXECUTIVE SUMMARY… Case descp**

Decide what aim is before analysis? To investigate and find evidence: **OBJECTIVE and resp strategy**

**Examination:**

**COMPUTER EVIDENCE ANALYZED**

I found so and so on this PC/system/node : use common identifiers

I used so and so harddrive. Here is its metadata, md5sum, location etc.

We found all this from crime scene: **RELEVANT FINDINGS**

**Eg. Code that was used to inject sql, make it an attachment. don’t interrupt ur report with random code in between**

We found this evidence to support: **SUPPORTING DETAILS**

Tips and outstanding tasks, that could be done if more time or help received: **LEADS**

Conclusion

Lesson learned

Have coworkers or nontech peeps proof read ur report.

artifacts : An artifact is a remnant or trace left behind on the computer which helps to identify the source of malicious traffic and attack conducted onto the system

* Browsing activity
* Downloads
* History
* Saved Password
* websites visited
* Bookmarks
* Extensions
* Cache
* autocomplete login data
* Sessions
* tmp folders created by applications
* Cookies that are stored by the browser is another way to get to the web history of the user, Use a third-party software to open them and view history
* access to the hidden index.dat file for logs
* history.hst files
* If using multiple logins devices, use google activity

Exceptions: history paused, selectively deleted, guest mode

If by any chance, the suspect pc had restoration points, deleted files can be recovered.

**C:\Users\91985\AppData\Local\Google\Chrome\User Data\System Profile**

* The SPF policy framework is an **authentication scheme. Sender Policy Framework**
* SPF defines a process for the domain owners to identify which **IP addresses** are authorized to forward email for their domains, thus creates a spf dns record for source emailers
* Each participating domain declares attributes that uniquely describe their mail, including authorized senders. This description is represented in an SPF record, which is published in DNS records..
* SPF blocks spammers and other attackers from sending email

SPF and other authentication-based measures are designed to redress a vulnerability

in SMTP

2 types of possible query results:

pass, which means that the message meets the domain's definition for legitimate

messages;

fail, which means that a message does not meet that requirement; and further

stipulations for mail that don't fit either category, such as messages from domains

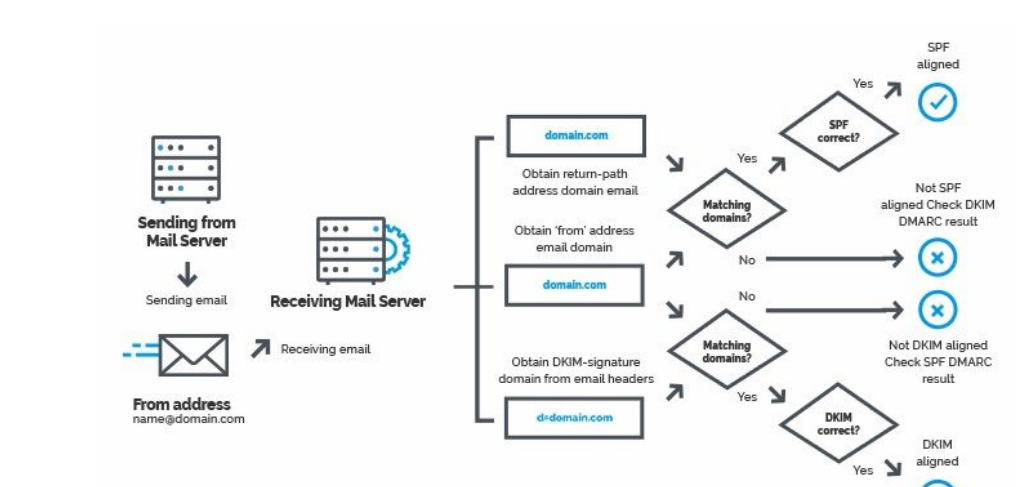
that do not publish SPF data.

* Receiving email servers that get email from an email service under SPF must check the **TXT records** when they perform a query for DNS lookup on the inbound email.

*Pass:* which means that the message meets the domain's definition for legitimate messages

*fail*

* If source mail is found in the dns records. Authenticated, else mark as spam since the sender is trying to appear as from a legitimate organization

**Domain-based Message Authentication (DMARC) protocol**

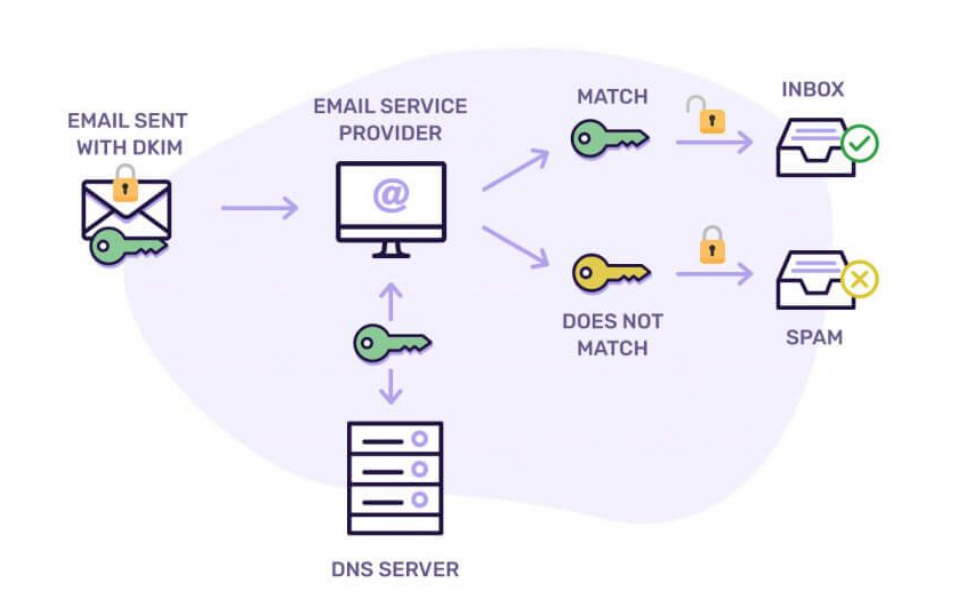
SPF is not the only email authentication strategy used against spammers.

Domainkeys Identified Mail (DKIM) and the Domain-based Message Authentication (DMARC)

protocols both work with SPF to enhance email security.

DKIM defines a protocol for claiming responsibility cryptographically for email messages sent

from a domain.



* Device acquired: DON’T BOOT FROM IT
* Look for hidden files or locked ones
* Restoration recovery points in suspect pc
* create img using FTKimager, dd, dcfldd: open wo mount using aut
* Recover deleted using foremost scalpel CARVING
* RECYCLE BIN FORENSICS cmd line and

Delete vs shift + delete

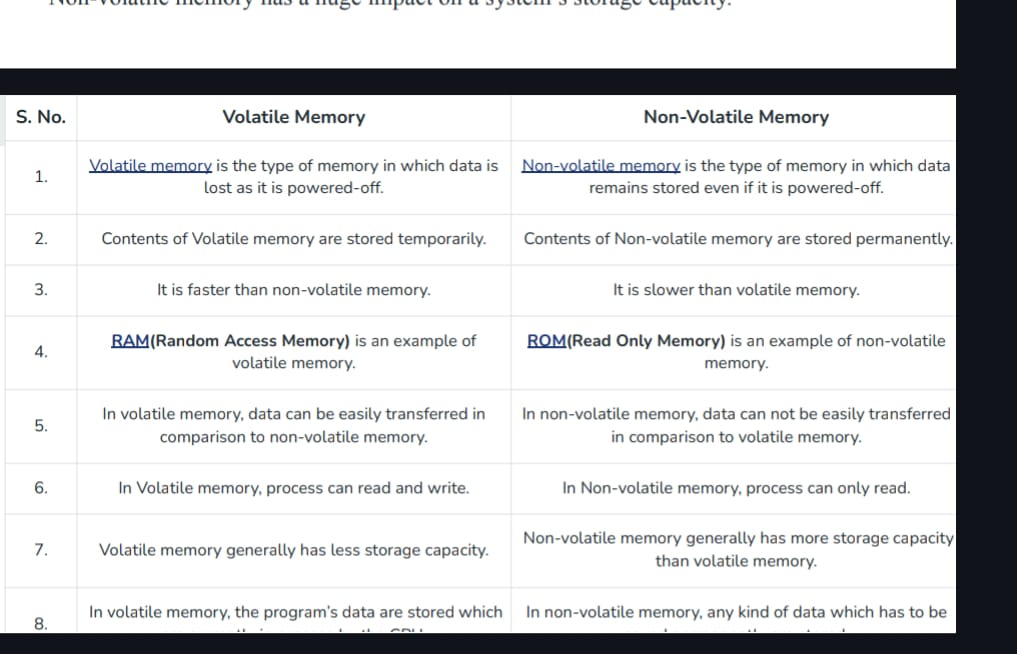
**$I** contains meta data of the deleted file and **$R** contains actual deleted file

$I PARSER can be used to recover the metadata

* Pcap files: network miner wireshark, unauth logins attempts/ unusual traffic
* RAM FORENSICS pagefile.sys: VIRTUAL MEM : volatality3 cmd line, volix for gui

Live data:

* current nw config
* current nw connections
* open sockets/ports/sessions
* applications open rn: open files, task manager
* cmd prompt history of cmds recently run
* ids, router, firewall logs
* all users logged in
* clipboard contents
* open registry keys
* malware (using which suspect pc was hacked): trojan horses/backdoor
* Hidden hard drive partitions:
* USB DEVICE FORENSICS: WINDOWS REGISTRY EDITOR & usbdeview
* NETWORK FORENSICS: wifi pswd hacking using fluxion
* MOBILE DEVICE: sim data: calls, msgs/ emails, sd card contents
* EMAIL FORENSICS
* BROWSER FORENSICS



The advanced static method in malware analysis involves a deeper and more comprehensive examination of the malware binary without executing it. It goes beyond basic static analysis techniques to uncover intricate details about the malware's functionality, behavior, and inner workings. Here are some key aspects of advanced static analysis:

1. \*Code Analysis:\* Advanced static analysis involves a detailed examination of the malware's code structure, logic, and algorithms. This includes:

- Decompiling or disassembling the binary to understand its assembly instructions and high-level constructs.

- Identifying control flow structures, loops, conditionals, and function calls to analyze the malware's execution flow.

- Analyzing code obfuscation techniques used by the malware to evade detection and analysis, such as code encryption, packing, and anti-debugging measures.

2. \*Malware Artifacts:\* Advanced static analysis aims to identify and extract various artifacts embedded within the malware binary, including:

- Strings: Extracting hardcoded strings, URLs, API function names, registry keys, and other indicators of malicious behavior.

- Configuration Data: Identifying configuration parameters, command and control (C2) server addresses, encryption keys, and other critical data used by the malware.

- Resource Files: Extracting embedded resources such as images, icons, configuration files, and executables that may be used by the malware during execution.

3. \*Behavioral Analysis Features:\* Advanced static analysis may include features typically associated with dynamic analysis, such as:

- Emulating API calls and system interactions to understand how the malware interacts with the underlying operating system.

- Identifying potential network communication patterns, encryption algorithms, and data encoding methods used by the malware.

- Extracting potential indicators of compromise (IoCs) and generating YARA rules or signatures to detect similar malware samples.

4. \*Reconstruction and Visualization:\* Advanced static analysis techniques may involve reconstructing the malware's execution flow and visualizing its behavior using tools such as:

- Control flow graphs (CFGs) and function call graphs (FCGs) to visualize the relationships between different code segments and functions.

- Dependency graphs to visualize the dependencies between various components and resources within the malware binary.

- Data flow analysis to track the flow of data and variables within the malware code.

By leveraging advanced static analysis techniques, malware analysts can gain deeper insights into the functionality, behavior, and architecture of malware samples, enabling more effective detection, classification, and mitigation of cyber threats.

"Advanced dynamic analysis" refers to an in-depth and sophisticated approach to analyzing malware behavior and characteristics through dynamic execution in controlled environments. While basic dynamic analysis focuses on observing malware behavior during execution, advanced dynamic analysis delves deeper into understanding complex malware functionalities, evasive techniques, and interactions with the target system. Here are some key aspects of advanced dynamic analysis:

1. \*Environment Emulation:\* Advanced dynamic analysis often involves creating highly specialized and customized environments, known as sandboxes, to execute malware samples. These sandboxes replicate the target system's environment, including operating system version, installed software, network configurations, and user behaviors. Emulating diverse environments allows analysts to observe how malware behaves under different conditions and identify evasion techniques targeting specific configurations.

2. \*Code Instrumentation:\* Advanced dynamic analysis may involve instrumenting the malware binary or the execution environment to gather detailed runtime information. This can include hooking system calls, intercepting API functions, and monitoring memory allocations and modifications. By instrumenting the code, analysts can gain insight into the malware's internal operations, such as file system modifications, network communications, and process interactions.

3. \*Behavioral Analysis:\* While basic dynamic analysis focuses on observing observable behaviors, advanced dynamic analysis employs advanced techniques to extract more granular behavioral information. This includes monitoring interprocess communication, analyzing timing and sequence of events, and detecting stealthy or polymorphic behaviors. Behavioral analysis aims to uncover complex malware functionalities, such as code injection, privilege escalation, and anti-analysis mechanisms.

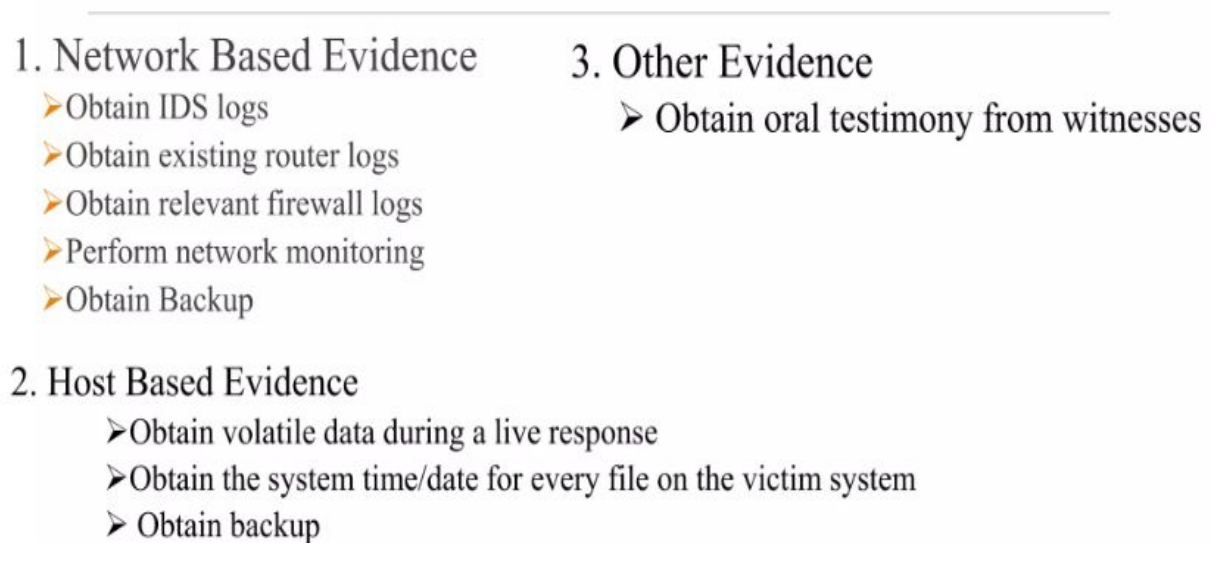
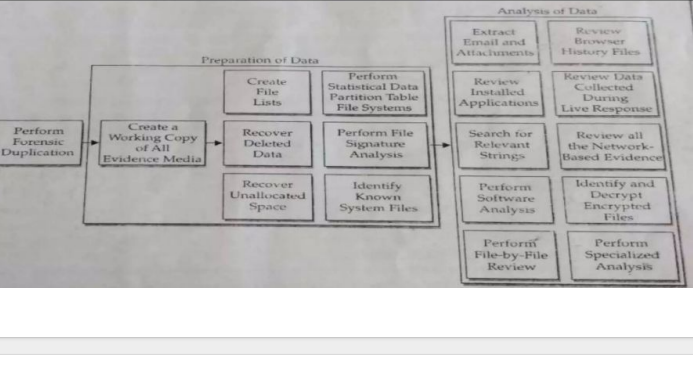
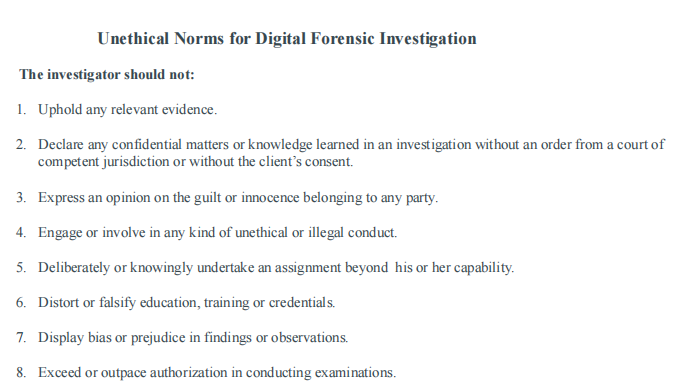
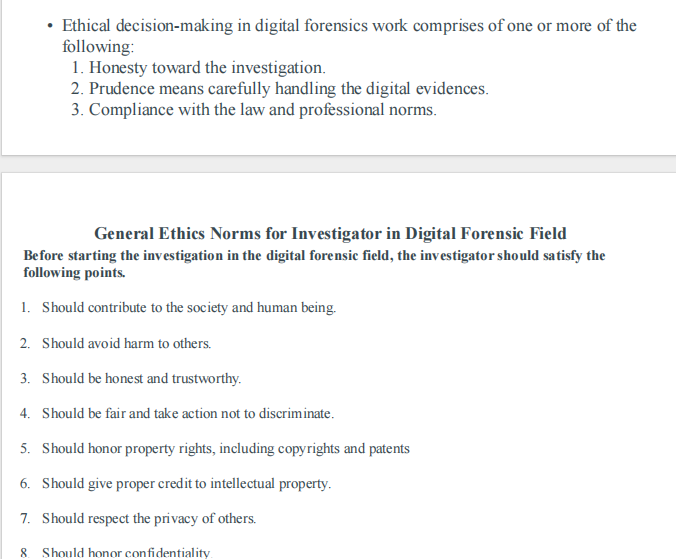
4. \*Malware Interaction:\* Advanced dynamic analysis may involve actively interacting with the malware sample during execution to trigger specific behaviors or responses. This can include sending simulated user input, modifying environmental variables, or injecting code into running processes. By actively interacting with the malware, analysts can uncover hidden functionalities, trigger dormant behaviors, and evaluate the resilience of evasion techniques.

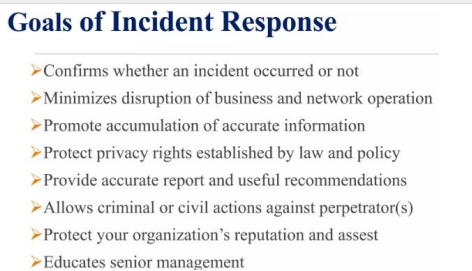
5. \*Dynamic Data Analysis:\* In addition to observing runtime behaviors, advanced dynamic analysis focuses on analyzing data generated or manipulated by the malware during execution. This can include monitoring memory content, analyzing network traffic payloads, and decrypting encrypted data. Dynamic data analysis helps analysts understand how malware communicates, exfiltrates data, and interacts with external entities.

6. \*Automated Analysis:\* To handle the large volume of malware samples encountered in modern cybersecurity operations, advanced dynamic analysis often incorporates automation and machine learning techniques. Automated analysis platforms can execute malware samples at scale, extract behavioral indicators, and generate actionable intelligence for threat detection and response.

By leveraging advanced dynamic analysis techniques, cybersecurity professionals can gain deeper insights into malware threats, improve detection capabilities, and enhance the resilience of defense mechanisms against evolving cyber attacks.

-------------------------1st mod





● Identification: purpose, resources, tools

● Preservation: & acquisition

● Analysis: examine

● Documentation

● Presentation: conclude report summarize

1. Computer Forensics

2. Network Forensics

3. Mobile Devices Forensics: sim, gps

4. Database Forensics

● pre incid prep: implement host nw sec, employ ids, acl, hw sw old documen arrange

● incident detection: ids, failed login attempts, unfam exes, gaps in logs, slow sys, sys crash

start docum

● Initial response checklists

● formulate response strategy: review acl (access control list)

● Incident Declaration

● Assembling the Computer Security Incident Response Team

● find Host-based evidence, Network-based evidence

● resolution, recovery, measures

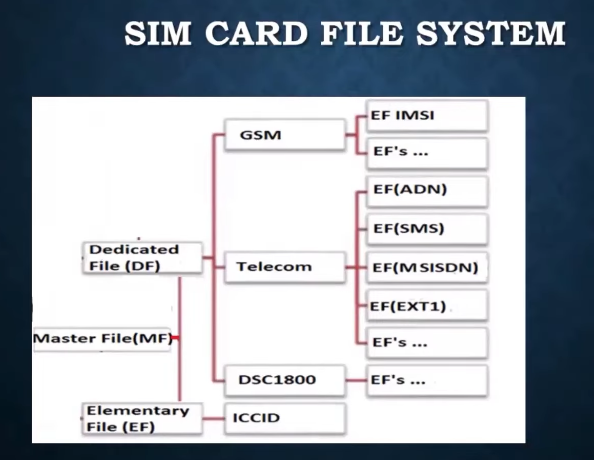
csirt: tech, cs, legal, bus manager, hr, workers

SIM CARD FORENSICS:

Subscriber identity module: micro mini nano

SIM card forensics can reveal valuable information such as contacts, call logs (incoming and outgoing calls with timestamps), text messages (both sent and received), and sometimes location data if the SIM card is equipped with GPS capabilities.

* ****Extraction Methods****: Forensic investigators use specialized tools and techniques to extract data from SIM cards. This can include using SIM card readers, which connect the SIM card to a computer for analysis, or through mobile device forensic tools that can extract data directly from the phone's memory.



sim= icc

integrated ckt card: mc based access module

clk vcc gnd reset pins on sim

components: eeprom, cpu and os, ram, rom

electronically erasable programmable

level of access:

always: no restriction

never

card holder verification 1

card holder verification 2

administrative

sensitive data in sim:

icc id

imsi (intl mobile subscriber identity) and msi number

spn subs provider name

mobile country code

mobile nw code

dialing number

last dial number

sms short msg service

lang pref

card holder verfication chv 1&2

ciphering key

emergency call code

mf= master file... root

df= dedicated file. sub directory of master

only 1 ef of mf holds icc ic

df dcs 1800, df dsm has nw related info

df telecom has service info

msgs to phone and from phone are encrypted

pin: personal id number

GPS FORENSICS:

when someone has a gps device

they enter in either their current locn or the locn they want to go to

info to be recovered:

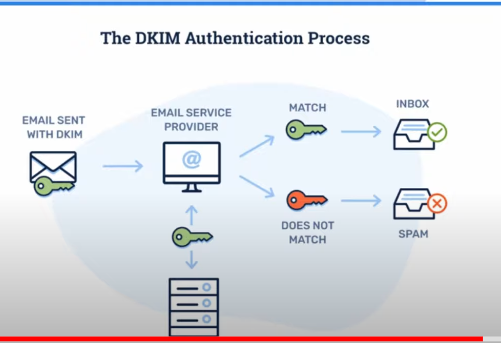
it records the list of coordinates the portable gps has visited.

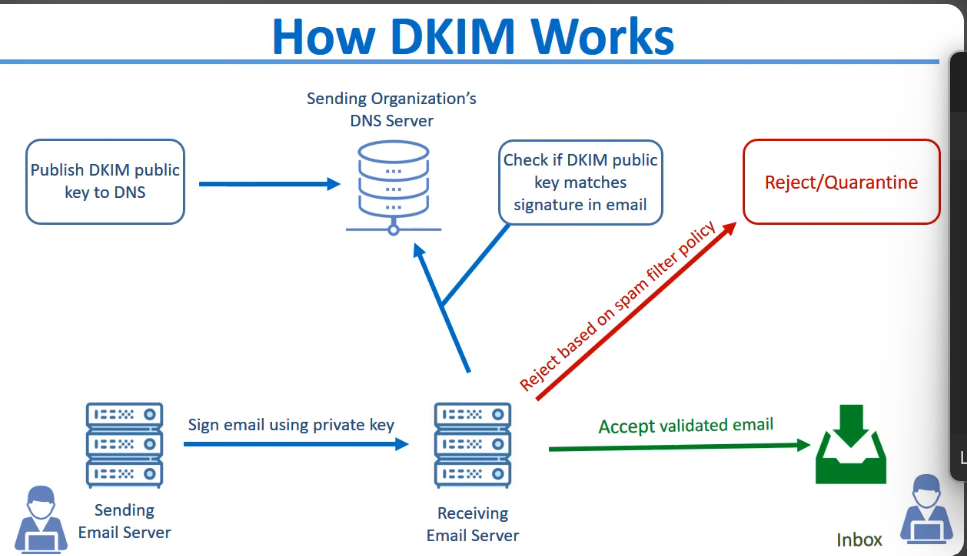
route history

timestamps when locns were recorded

(tracking suspects' movements), missing persons cases

DKIM





publish dkim public keys to dns while spf publishes spf records to dns

dkim is basically to tell if the mail has been tampered with (the body contents, the mail header or the from address)

mail aya

check domain

search that domain in dns

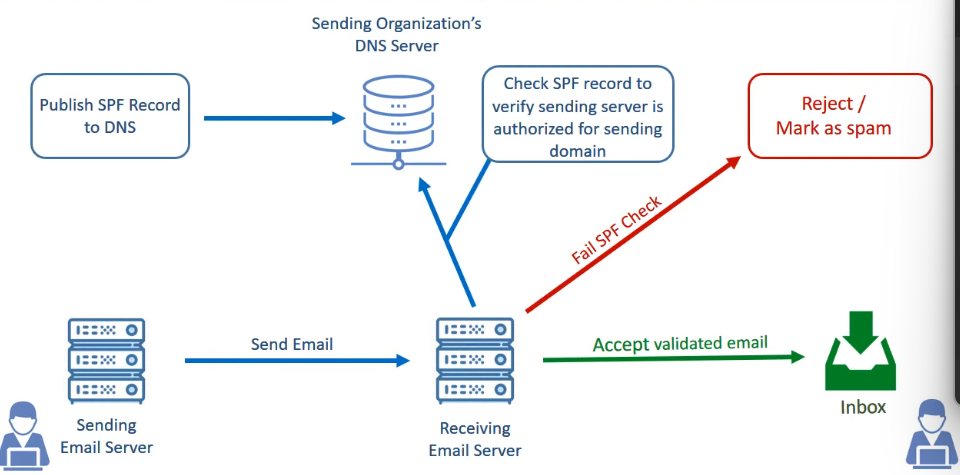
find its pub key in record

email is signed with a private key

using the private and public key it is seen if the msg decrypted = original msg sent

SPF

spf records are dns txt records that specify which ip addresses or servers are allowed to send mails to a particular domain.



to prevent email spoofing and email authenticity:

spf specifies specific servers who are authorized to send emails for a domain. it creates these spf records and send em to dns

whenever a receiver gets an email, it runs this spf check on it. checking spf records to verify the sender is authorized for sending.

like how anyone outside the ves organization can be disallowed to send a mail to a @ves.ac.in id

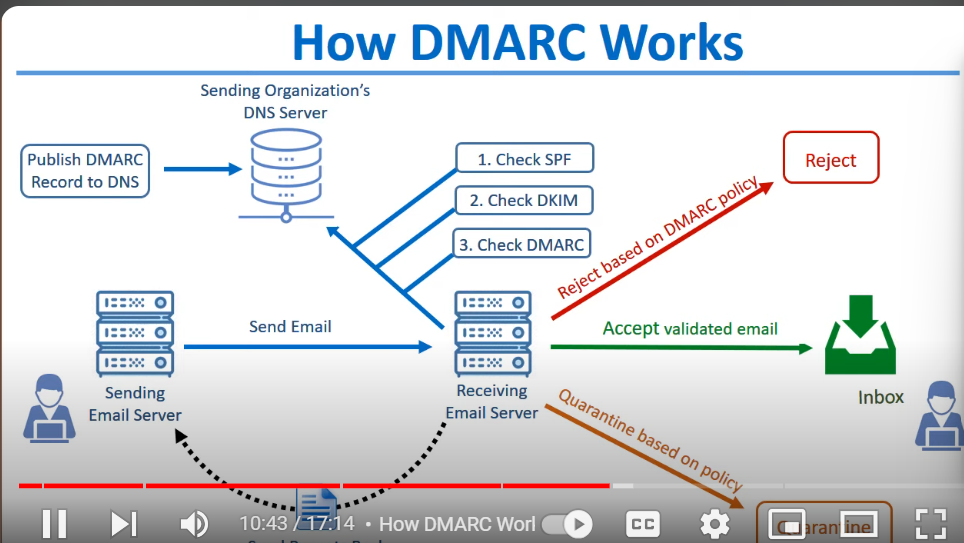
if a mail fails spf check, it is rejected and marked as spam

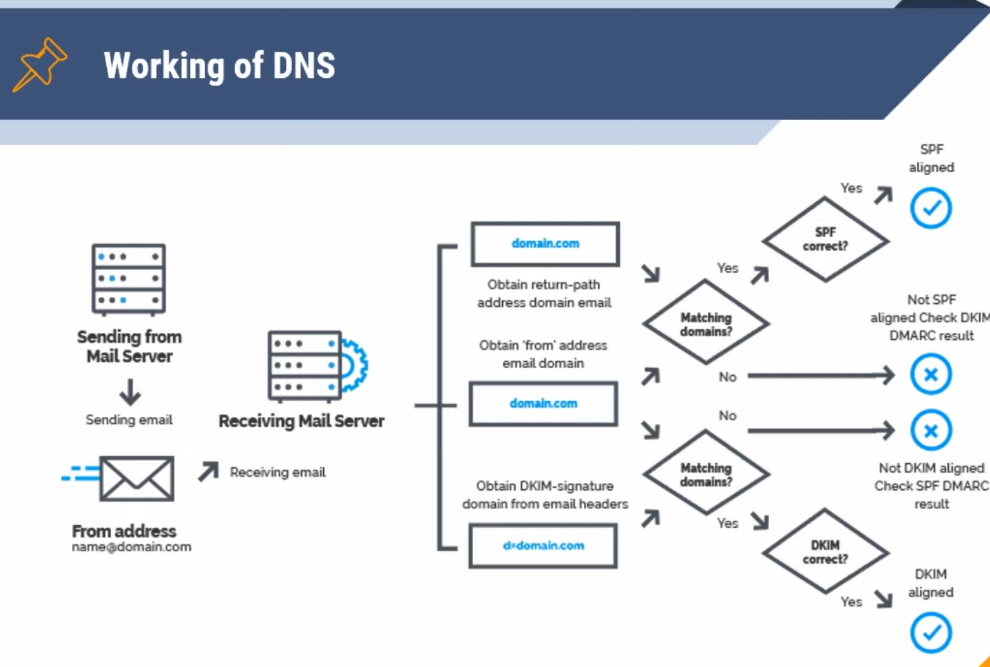
when aceepted as a valid email, it is received in inbox

DMARC

dmarc is not an email authentication protocol

checks if dkim and spf align





return address and from address match: aligned

Quarantining an email typically refers to the process of isolating a suspicious or potentially harmful email message from the rest of the email system to prevent it from causing harm. When an email is quarantined, it is usually moved to a separate location or folder where it can be further analyzed or safely deleted without risking the security of the entire email system. This is often done by email security systems or spam filters to protect users from phishing attempts, malware, or other malicious content.

A copy is made onto forensically sterile media.

Vital information resource under seize: VIRUS

black hat hacker = cracker

What volatile data can be obtained from investigation of routers?

browser stores a lot of sensitive information about the

user and its surfing habit.

steganography:

hiding a msg into a bigger file like a pic or sound file

take precautions to not nullify the evidences credibiltiy

Sure, here are some headings for different types of cybercrimes:

1. \*\*Financial Cybercrimes:\*\*

- Online fraud

- Identity theft

- Phishing scams

- Credit card fraud

- Money laundering

2. \*\*Cyber Espionage:\*\*

- Corporate espionage

- State-sponsored hacking

- Intellectual property theft

- Cyber spying

3. \*\*Cyber Warfare:\*\*

- DDoS attacks (Distributed Denial of Service)

- Malware attacks on critical infrastructure

- Cyber terrorism

- Information warfare

4. \*\*Cyber Bullying and Harassment:\*\*

- Online harassment

- Cyber stalking

- Revenge porn

- Doxxing (revealing personal information online)

5. \*\*Cyber Extortion:\*\*

- Ransomware attacks

- Data breaches with demands for payment

- Threats of releasing sensitive information

6. \*\*Cyber Vandalism:\*\*

- Defacement of websites

- Destruction or alteration of data

- Hacking for the sake of causing damage

7. \*\*Cyber Fraud:\*\*

- Investment fraud

- Auction fraud

- Online shopping fraud

- Employment scams

8. \*\*Cyber Terrorism:\*\*

- Attacks on critical infrastructure (power grids, transportation systems)

- Dissemination of propaganda

- Coordinated attacks on government systems

9. \*\*Cyber Piracy:\*\*

- Copyright infringement

- Illegal downloading or distribution of software, movies, music, etc.

- Unauthorized access to copyrighted material

10. \*\*Online Child Exploitation:\*\*

- Child pornography

- Grooming

- Sextortion

- Child trafficking

These headings cover a wide range of cybercrimes, each with its own set of subcategories and methods.

Briefly explain the process of collecting the volatile data in Windows system

collection process of volatile data in windows

steps for investigating routers

role of Windows registry in collecting forensic evidence.

ntfs vs fat

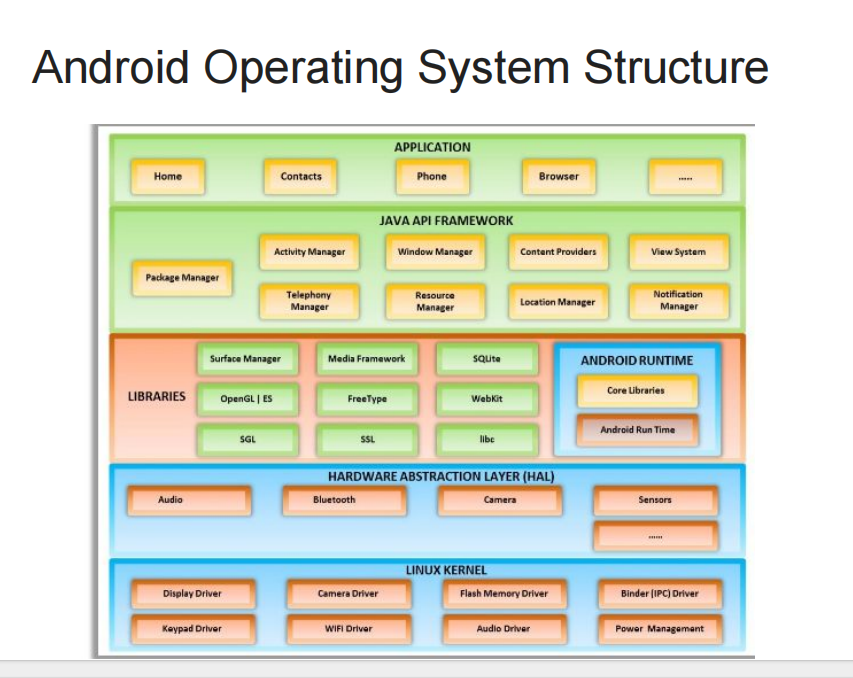
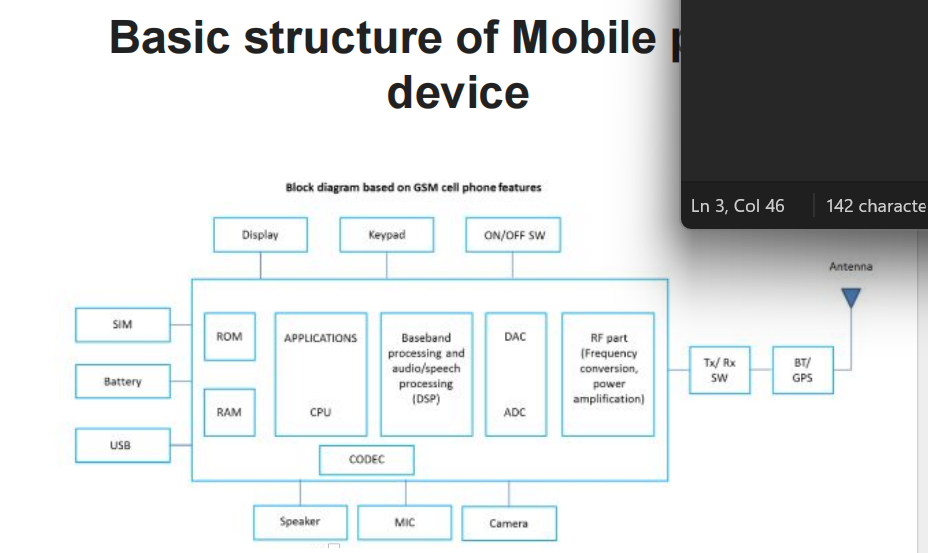
Mod5… mobile forensics

Personal calendars, pswds, voice recordings, banking details

there is no standard hardware architecture for mobile phones.

Newer tech everyday not compatible w old

iPhone may have a different hardware architecture than an Android mobile phone.

Investigators must apply **different tools and techniques** , different os…diff booting processes

Hw and sw knowledge required for investigator

For chipoff and appln

voice and data signals

core processing is different interface stds like lte and gsm

Antenna: An antenna converts the electro-magnetic

radiation to electric signals and vice versa

usb on/off

screen

on screen keyboard

sim card: builtin mem

sd card: external mem REMOVABLE STORAGE DEVICE

ram rom

bt gps rf

sensors eg. motion for gesture control, TEMP HUMID WEATHER, FINGERPRINT (SUURONDINGS) WIFI MODULES : ESP8266, HC05 FOR BT

drivers

adc dac

camera speaker mic antenna

Storage mem

1. sys mem/ sys storage has ur sys appls, app data and cache, inaccs by users
2. Phone storage for users.. downloaded pgms gallery INTERNAL SD ke jaisa but it’s a NON REMOVABLE STORAGE DEVICE

GSM PHONES REQUIRE SIMs

While collecting android mobile data for forensics, it is more difficiult since it can be tampered with by making use of wifi bt modules, which allow some services to be delievered via CC and even remote access perhaps. This is if the phone is still on and connected to a wifi nw.

Hence u put the phone in a FARADAY BAG which doesn’t allow any rf thus discontinuing bt wifi connections

U remove all usb and wired connections.

1. Find where data is stored
2. Extract it
3. Analyze it

Logical image:

Deleted and unused space is not copied. Only current files.

Physical image: all. Bit by bit

USB debugging allows an Android

device to establish communication with a computer/workstation that runs Android

Software Developer Kit (SDK).

The device should be unlocked to allow new or any previous USB connections

If the device is "OFF", then leave it in the turned off state because turning it ON could alter the evidence on the device

If the owner of the device is present at the scene, the law enforcement agents can obtain passcode from the owner. If they deny, the investigators can get a warrant and proceed legally

Mobile devices should be protected from signal interruption, which might lead to data overwriting.

Data acquisition techniques:

1. Chip off

Disassemble the mobile device

Remove NAND flash chips form ckt board

Require hardware knowledge as desoldering has to be done

Could overheat and damage the chips : risk

Sw method can be used when device is BOOTABLE and FUNCTIONAL

1. JTAG (Joint Test Action Group) is a hardware interface used for debugging and testing electronic devices like microprocessors and integrated circuits. It allows direct access to a device's pins for boundary scan testing, firmware debugging, and flash programming, facilitating efficient development and troubleshooting in embedded systems.

In digital forensics, JTAG (Joint Test Action Group) can be utilized to extract data from electronic devices, including smartphones and routers, bypassing locks or encryption

1. Adb android debug bridge

Cmd line tool tool to access mobile for

Pulling data pushing data navigating through file system

(unrooted obv, don’t have admin pswds)

1. Reverse engineer the bootloader and firmware, or the backup files

compare using hash and digital signatures

the current state of bootloader and firmware

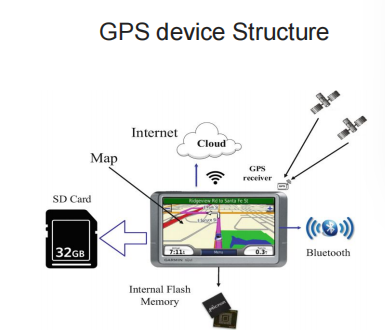
with the state when bootloader that was burned

to check for unath changes

check bootloader if device is damaged or inaccessible thru conventional means.

firmware that facilitates pgming is stored in nvram or flash mem. new code uploads on or apps download will change bootloader. it brings initial state of sys back. like factory reset

GPS makes it possible to precisely identify locations on the earth by measuring distance from the satellites.

Ground control stations play roles of monitoring, controlling and

maintaining satellite orbit to make sure that the deviation of the satellites from the orbit as well as GPS timing are within the tolerance level

GFX is a light-weight XML file format hat contains GPS data.

Promotes easy exchg

Convertible to diff formats

Gfx has the coords mentioning:

1. \*\*Route:\*\* Kalyan to Chembur

go to kalyan stn via auto

Get to pf 2

Board a csmt train

Deboard at kurla

Kurla auto to chembur

2. \*\*Track:\*\* The actual path taken by the train from Kalyan to Chembur.

1. \*\*Waypoint:\*\* Specific locations or landmarks along the railway route, such as Dombivli, Thane, Vashi, etc.

types of threats targeting mobile devices:

▪ Web and Network-based Attacks: malicious websites

cookie data steal malware installed or adware

mic: sound energy to electrical energy

speaker: electrical audio signals to sound energy . has a volume adjustable ckt to amplify volume

amplification, attenuation

make disk partitions: cmd line tool: diskpart

list disk

select disk 1

list partition

create partition primary size=500

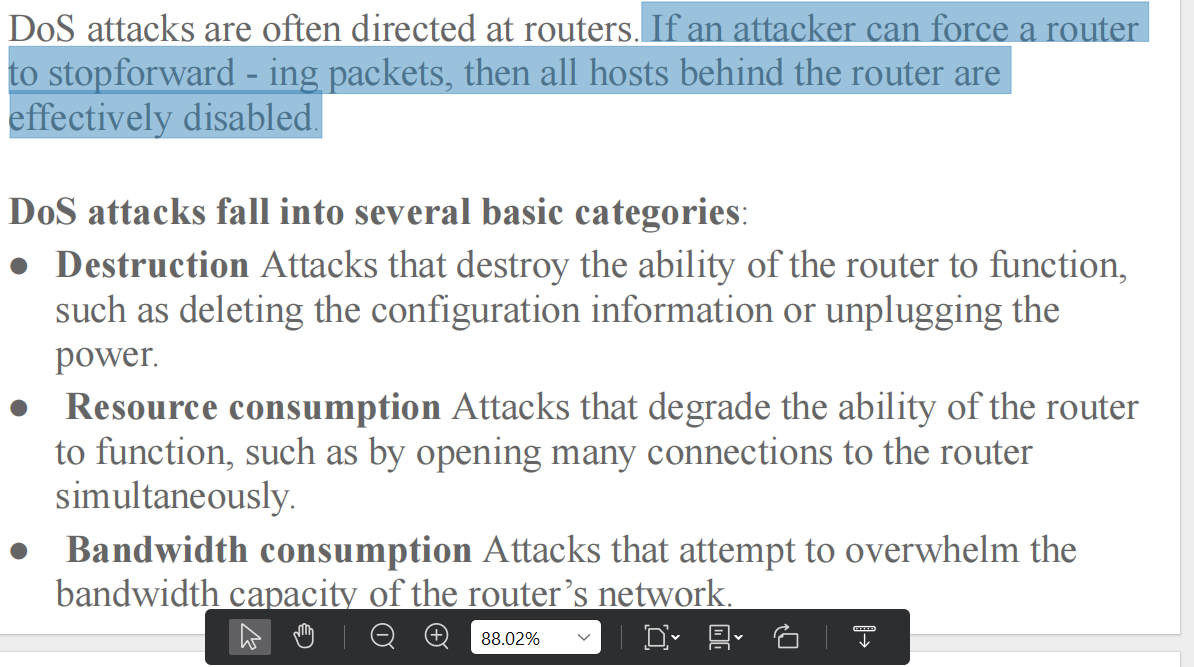
create partition primary

select partition 2

assign letter E

shrinking and merging volumes to make storage size for big image files

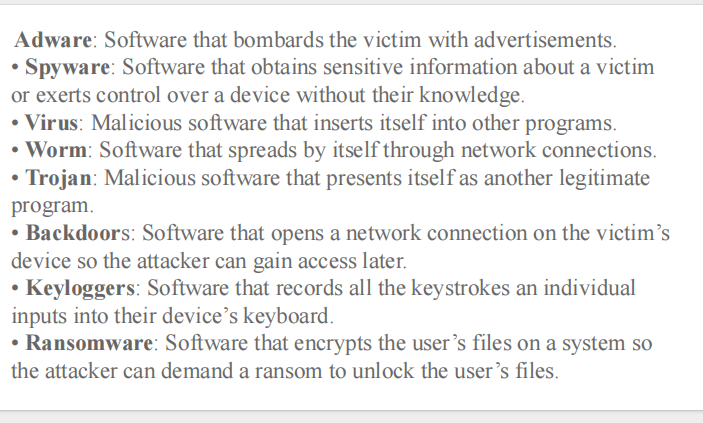
mounting the imgs as drives



Acl: wrt protocol, sender recv ip, domain,

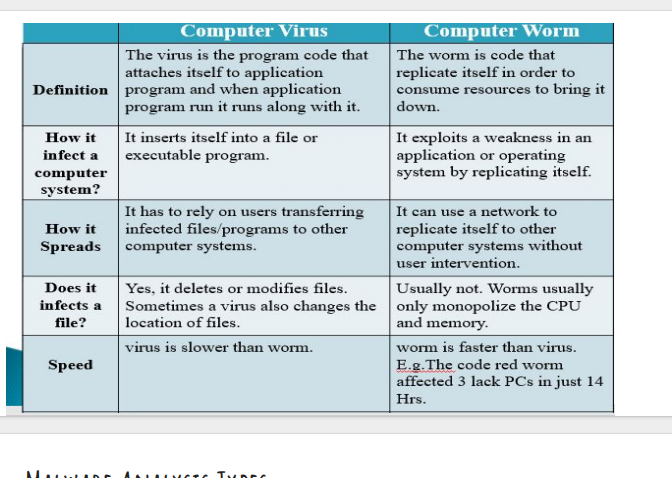
Upgrade sw

Close listening services



Response to malware:

Identify, communicate, block, restore, recover, reexamine



1. \*\*Basic Static Analysis\*\*:

- \*\*Scanning using Antivirus\*\*: Using a reputable antivirus software like Avast or Malwarebytes to scan the malware file for known signatures.

- \*\*Hashing\*\*: Calculating the hash value (e.g., MD5, SHA-256) of the malware file to uniquely identify it and check against known malware databases.

- \*\*Detection of Packed or Obfuscated Code\*\*: Identifying if the malware file is packed or obfuscated using tools like PEiD or Exeinfo.

2. \*\*Advanced Static Analysis\*\*:

- \*\*Analysis of Strings\*\*: Examining ASCII and Unicode strings embedded within the malware file to identify keywords, URLs, or encryption keys.

- \*\*Analysis of Linked Libraries and Functions\*\*: Investigating imported and exported functions, as well as linked libraries, to understand the behavior and capabilities of the malware.

- \*\*IDA Disassembler\*\*: Using IDA Pro or Ghidra to disassemble and analyze the assembly code of the malware for deeper insights.

3. \*\*Basic Dynamic Analysis\*\*:

- \*\*Building a Virtual Machine\*\*: Setting up a virtual machine environment (e.g., VMware, VirtualBox) to isolate and analyze the malware safely.

- \*\*Malware Sandbox\*\*: Running the malware in a controlled environment provided by a malware sandbox like Cuckoo Sandbox or Hybrid Analysis.

- \*\*Process Monitoring\*\*: Observing the behavior of the malware process, including file system modifications, registry changes, network connections, and process creation.

4. \*\*Advanced Dynamic Analysis\*\*:

- \*\*Debugging\*\*: Using a debugger like OllyDbg or WinDbg to dynamically analyze the behavior of the malware, set breakpoints, and step through the code.

- \*\*Registry Analysis\*\*: Examining changes made to the Windows registry by the malware, including additions, modifications, or deletions of registry keys and values.

- \*\*Analysis on a Windows System\*\*: Conducting dynamic analysis directly on a Windows system to observe the malware's interaction with the operating system and other processes.

5. \*\*Malware Analysis Report\*\*:

- \*\*Characteristics of Malware\*\*: Summarizing findings from both static and dynamic analysis, including information on file hashes, detected behaviors, network activity, and potential impact on systems.

- \*\*Behavioral Analysis\*\*: Describing observed behaviors of the malware during analysis, such as file encryption, data exfiltration, or attempts to establish command and control communication.

- \*\*Recommendations\*\*: Providing recommendations for mitigation and remediation based on the analysis findings, including antivirus signatures, network rules, and system hardening measures.

Identify unauthorized user accounts or groups.

● Identify rogue processes and services.

● Look for unusual or hidden files/directories.

● Check for unauthorized access points

task manager

remote logins/ teamviewer / vnc viewer (like using an hdmi to get multiple display screens)

angry ip scanner to get all ip addresses connected to my nw eg. rpi

eg. login to it using putty,

only works if telnet and ssh were enabled during rpi os installation

or directly access files on it using filezilla

rpi can be stored for 1. storage

2. deployment of a cyberattack

3. exploit iot devices

4. digital currency mining Resource Consumption: Consider electricity and network usage;

rpi os can be either cmd line based or gui based

If a criminal intentionally disables SSH access during the installation of the Raspbian operating system, it could potentially hinder remote access to the device.

If a criminal intentionally disables SSH access during the installation of the Raspbian operating system, it could potentially hinder remote access to the device. However, this does not necessarily prevent forensic analysis or access to the SD card's contents

if the malicious code files are automatically removed or demounted upon connection to a victim system, investigators may lose access to crucial evidence that could help identify the nature of the attack, the attacker's methods, and potential accomplices. This loss of evidence can hinder the investigation and make it challenging to attribute the attack to specific individuals or groups.

Concealed Malware Distribution: By posing as a connector, the Raspberry Pi can execute malicious code when connected to another device, without triggering auto-mounting and antivirus scans. riminals can use the Raspberry Pi as a staging platform to prepare and launch further attacks, disabling auto-mounting reduces the likelihood of leaving forensic traces on the victim device, Disabling auto-mounting can prevent the device from appearing in registry entries or triggering USB forensics tools, making it more challenging for investigators to detect its presence and activities on the victim system

thus even testing of the suspect device can be harmful.Without access to the malicious code files, forensic analysts may be unable to conduct a detailed examination of the code's functionality, behavior, and origin. This limits their ability to understand the scope of the attack, assess its potential impact, and develop effective countermeasures to prevent future incidents.

sometimes the files are write and read protected

however sometimes thonny can access and upload files to microcontroller boards because it communicates with the microcontroller using specific protocols and interfaces

=---------------=

evidence can be found at

registry, slack space, ram, free or unallocated space (prev deleted stuff), logs

swapfiles (recently closed)

appln level files: browser history

temporary files created by applns: eg. proteus backup files timely

or workspace files for logging

check the printer spool

check if suspect pc has gmail or outlook mail history

Unfortunately, not all USB device types will leave traces in Windows registry

owner/ user of pc/ identification info.. autopsy tells pc name

proof against user.. pics vids

proof he wasnt alone

proof he tried to erase evidence (delete files, new os) recover it

proof that he was tryna run away

usbs? sdcards

The longer a machine is off, the more data becomes lost.

zero day attacks

..................

routers have little data storage capabilities

routing tables, listening services pswds rn, will be lost if reboot or power off

The routing table contains the blueprint of how the router

forwards packets. If an attacker can manipulate the routing table, the attacker can change

where packets are sent.

direct compromize, u access thru ssh, smtp, telnet console or web or modem and gain admin access.

remove static routes in RT, reboot router

If an attacker can force a router

to stopforward - ing packets, then all hosts behind the router are

effectively disabled.

can be integrated with all google services: sign in with google wo having to put in pswd hence pswd synch

auto complete data

multiple device logins

tools: db browser to open .sqlitle files

os forensics

restoration points for recovery (checkpoints): only if enabled

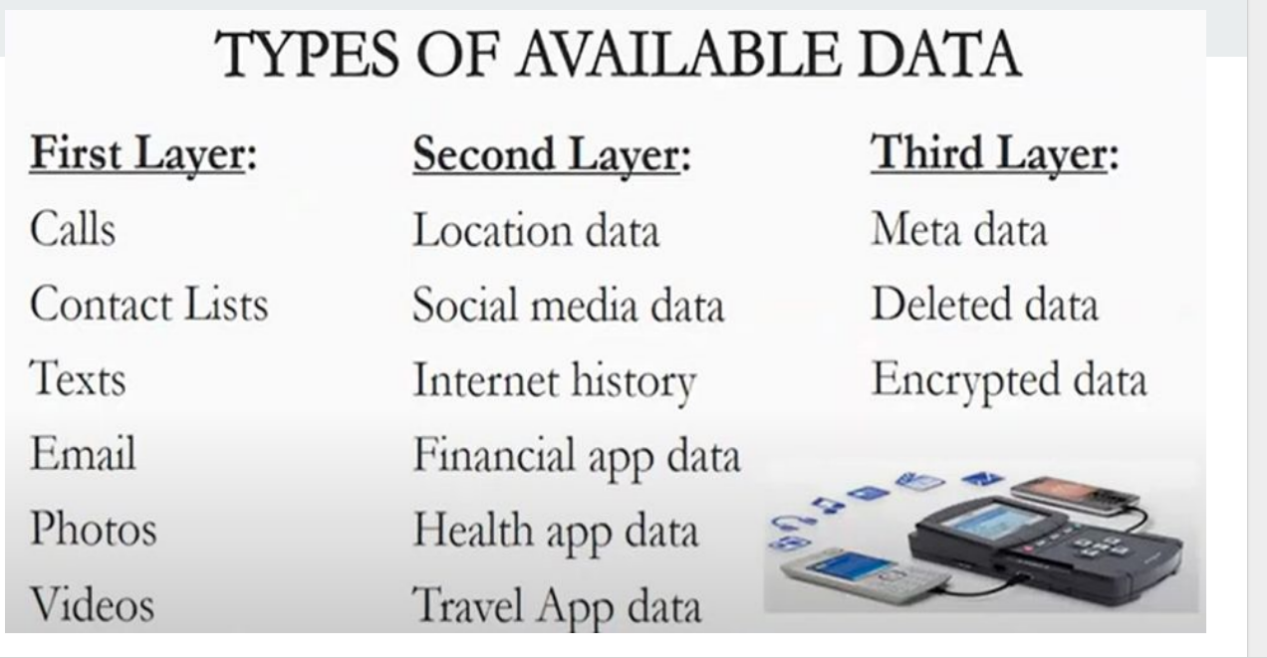
deleted browsing history is still in logs

which is index.dat hidden file

or a 3rd party file recovery sw: recuva

dns records on ipconfig/displaydns

google activity section.... with timestamps

1. \*\*Basic Static Analysis\*\*:

- \*\*Scanning using Antivirus\*\*: Using a reputable antivirus software like Avast or Malwarebytes to scan the malware file for known signatures.

- \*\*Hashing\*\*: Calculating the hash value (e.g., MD5, SHA-256) of the malware file to uniquely identify it and check against known malware databases.

- \*\*Detection of Packed or Obfuscated Code\*\*: Identifying if the malware file is packed or obfuscated using tools like PEiD or Exeinfo.

2. \*\*Advanced Static Analysis\*\*:

- \*\*Analysis of Strings\*\*: Examining ASCII and Unicode strings embedded within the malware file to identify keywords, URLs, or encryption keys.

- \*\*Analysis of Linked Libraries and Functions\*\*: Investigating imported and exported functions, as well as linked libraries, to understand the behavior and capabilities of the malware.

- \*\*IDA Disassembler\*\*: Using IDA Pro or Ghidra to disassemble and analyze the assembly code of the malware for deeper insights.

3. \*\*Basic Dynamic Analysis\*\*:

- \*\*Building a Virtual Machine\*\*: Setting up a virtual machine environment (e.g., VMware, VirtualBox) to isolate and analyze the malware safely.

- \*\*Malware Sandbox\*\*: Running the malware in a controlled environment provided by a malware sandbox like Cuckoo Sandbox or Hybrid Analysis.

- \*\*Process Monitoring\*\*: Observing the behavior of the malware process, including file system modifications, registry changes, network connections, and process creation.

4. \*\*Advanced Dynamic Analysis\*\*:

- \*\*Debugging\*\*: Using a debugger like OllyDbg or WinDbg to dynamically analyze the behavior of the malware, set breakpoints, and step through the code.

- \*\*Registry Analysis\*\*: Examining changes made to the Windows registry by the malware, including additions, modifications, or deletions of registry keys and values.

- \*\*Analysis on a Windows System\*\*: Conducting dynamic analysis directly on a Windows system to observe the malware's interaction with the operating system and other processes.

5. \*\*Malware Analysis Report\*\*:

- \*\*Characteristics of Malware\*\*: Summarizing findings from both static and dynamic analysis, including information on file hashes, detected behaviors, network activity, and potential impact on systems.

- \*\*Behavioral Analysis\*\*: Describing observed behaviors of the malware during analysis, such as file encryption, data exfiltration, or attempts to establish command and control communication.

- \*\*Recommendations\*\*: Providing recommendations for mitigation and remediation based on the analysis findings, including antivirus signatures, network rules, and system hardening measures.