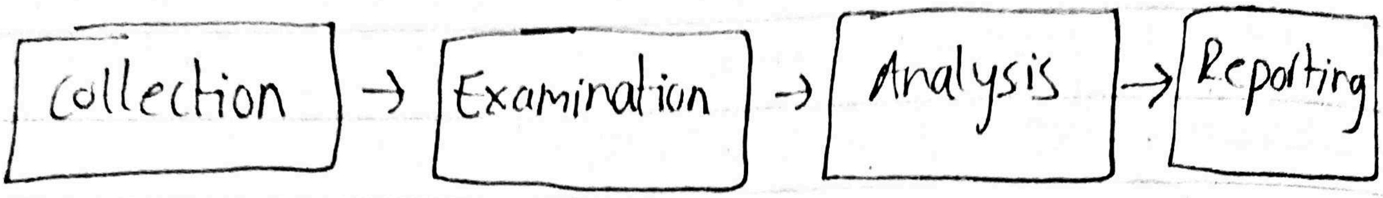
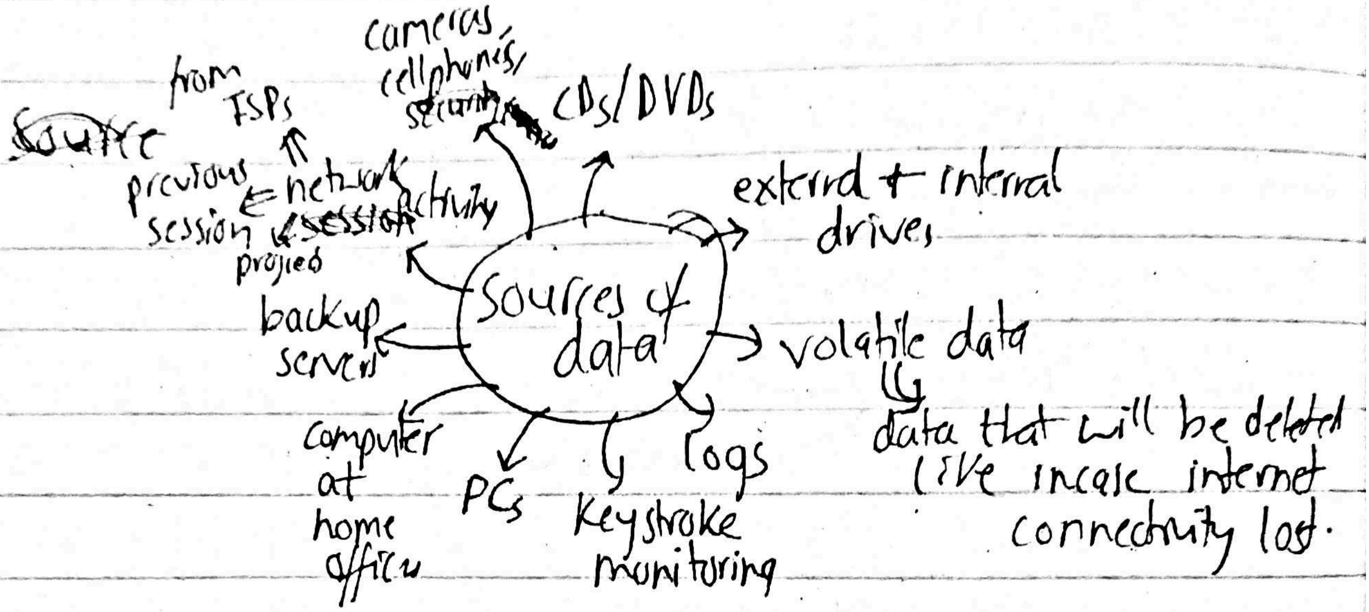
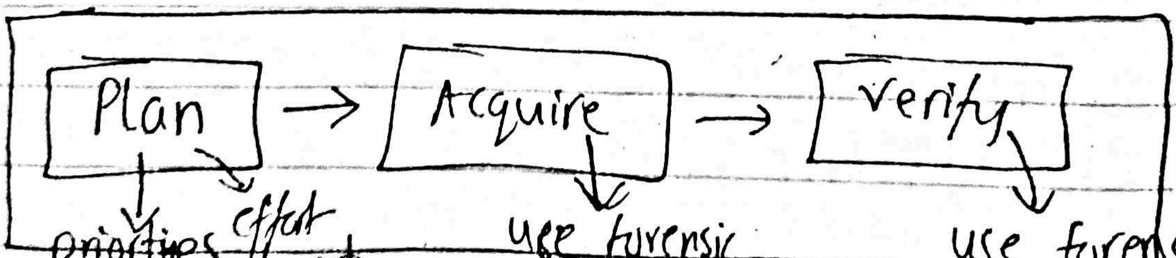
Digital Forensics

→ collection and analysing data to ensure integrity.




Sources of data
cameras, cellphones, security
CDs/DVDs
external + internal drives
volatile data
data that will be deleted like incase internet connectivity lost.
logs
Keystroke monitoring
PCs
computer at home office
backup servers
network ~~session~~ activity
previous session
projied
from ISPs
~~Source~~

step 1) Collection



Plan:

priorities ~~source~~
- volatile data (high priority)
- non-volatile (low priority)

effort to get data

Acquire: use forensic tools to collect volatile data. duplicate non-volatile source

Verify: use forensic tools to generate hash values to test integrity of data.

Chain of custody.

→ log of who has physical custody of evidence and what they did with the data

- make a copy of evidence and perform examination + analysis on the copy and verify the ~~orig~~ integrity with original

step 2) Examination

Hurdles

i) bypass controls

↳ OS and applications may have encryption, compression or ACLs.

ii) sea of data

↳ a HDD may have 1000s of files, not all of which are relevent

iii) what tools to use to filter and exclude data from searches

Step3) Analysis

identify people, places, items and events, and determining how these elements are related so that a conclusion can be reached → inshort, putting the pieces together

step4) Reporting

① Case summary → how investigator got involved
→ ~~initial~~
↳ concise

② Forensic Acquisition and examination preparation → details on how you acquired data and how you preserved it
↳ throughly documentation
↳ how examination was done

③ Finding and report (analysis)
logs
screenshot
highlighting
date items
digital audio over text

④ Conclusion
↳ summaries

→ if not mentioned in report, you cannot testify about it