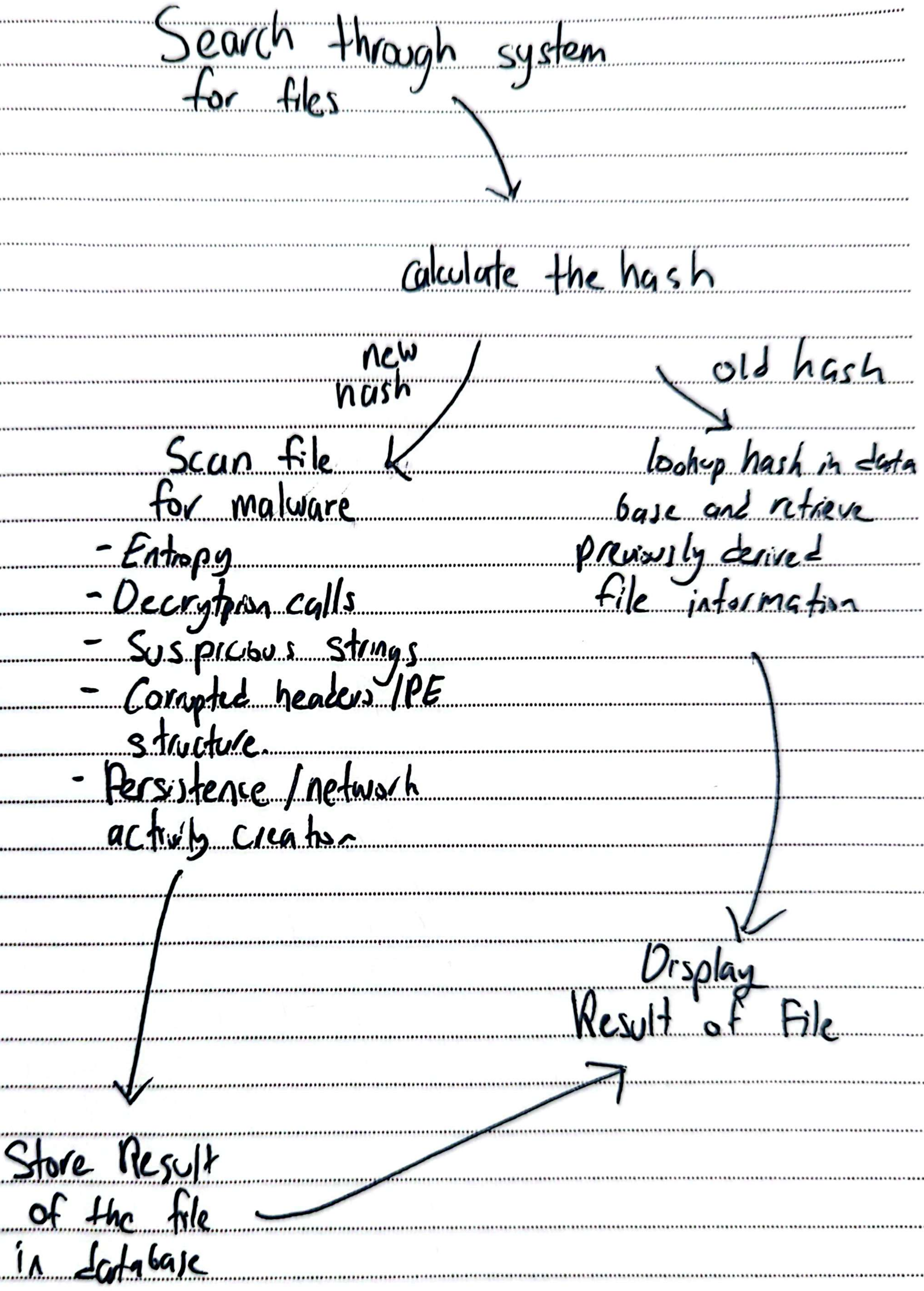
Search through system for files
calculate the hash
new hash
old hash
Scan file for malware
- Entropy
- Decrytpion calls
- Suspicous strings
- Corrupted headers /PE structure.
- Persistence /network activity creation
lookup hash in data base and retrieve previously derived file information
Display Result of File
Store Result of the file in database