Anil Naraine

Assignment 2

Part 1

1. Volatile data is data than can be lost when shutting down or rebooting the machine. Example, memory stored in RAM such as passwords.
2. Volume slack is unused space between the end of the file and the end of the partition.
3. File carving is the process of reassembling computer files from fragments in the absence of file system metadata.
4. the process of making a file system ready to be used by the operating system, typically by reading certain index data structures from storage into memory

Part 2

1. T
2. T
3. F
4. T
5. F

Part 3

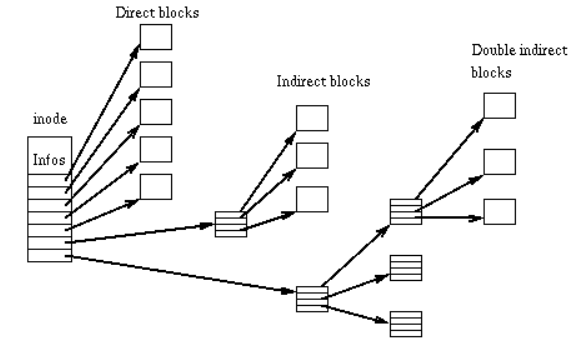
1. B
2. D
3. D
4. A
5. D
6. B
7. A
8. B
9. D
10. D
11. A
12. D
13. b
14. D
15. B
16. D
17. b
18. C
19. A
20. D
21. B
22. B
23. d
24. b
25. a

part 4

1. mft
2. string, binary, and DWORD
3. event, security, and audit
4. running processes, and system state
5. hard, and soft link. Symbolic
6. d
   1. 2
   2. 6, D,E,F,G,H,I
   3. 8
   4. 13 and 16
   5. 4
   6. K-1, k being the number of values
   7. a
7. 1024 bytes
8. 2

Part 5

1. Each inode can store the addresses of the first 12 blocks that a file has allocated which is called a direct pointer. If more blocks are needed the block is allocated to store the remaining addresses-this is called an indirect pointer. The larger the file the more indirect blocks it needs.



1. Unencrypted data, passwords in clear text, web caches, encryption keys.
2. Network tools, services, open files, processes, logged-on users, system uptime.
3. Fat- the root directory is after the FAT area before the data area.

NTFS- after the $MFT entry

ExtX- inode 2

1. Network forensics relates to the monitoring and information gathering of network traffic. Packet sniffers, ICMP traceback, and honeypots are all part of network forensics.
2. A public key encrypts a random symmetric key, the recipient of the message uses asymmetric decryption to decrypt the symmetric which in-turn is used to decrypt the message.