CYBER FORENSIC | CYBER CRIME INVESTIGATION | CYBER LAW

Intelligent Quotient Security System

Cyber Forensics

BY:

Dr Harold D’Costa

CEO – Intelligent Quotient Security System

Cell: 09637612097,

Email :hld@rediffmail.com

Website : cybersolution.in

Computer Forensics

omputer forensics is the practice of collecting, analysing and reporting on di
ta in a way that is legally admissible.

can be used in the detection and prevention of crime and in any dispute whe
idence is stored digitally.

omputer forensics follows a similar process to other forensic disciplines, and
ces similar issues.

Uses of computer forensics

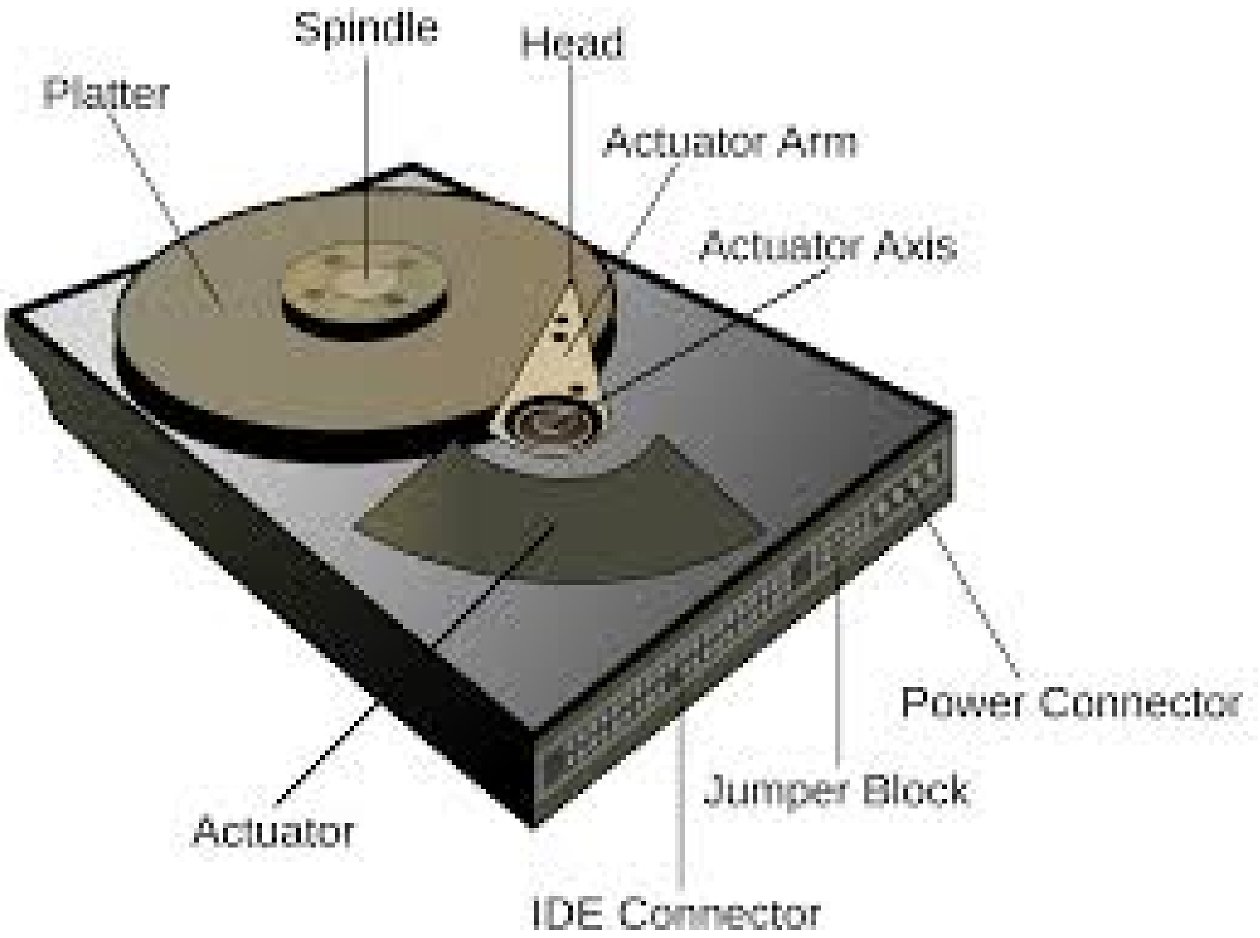
omputer forensic examination may reveal when a document first appeared on a mputer, when it was last edited, when it was last saved or printed and which user rried out these actions.

ore recently, commercial organisations have used computer forensics to their bene ariety of cases such as;

llectual Property theft
ustrial espionage
ployment disputes
ud investigations
geries
kruptcy investigations
ppropriate email and internet use in the work place
ulatory compliance

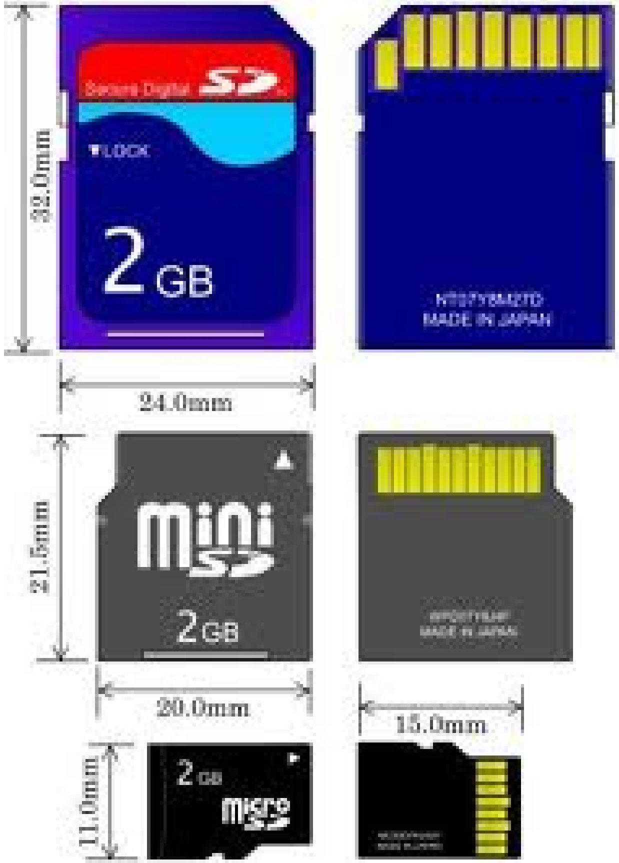
Hard disk

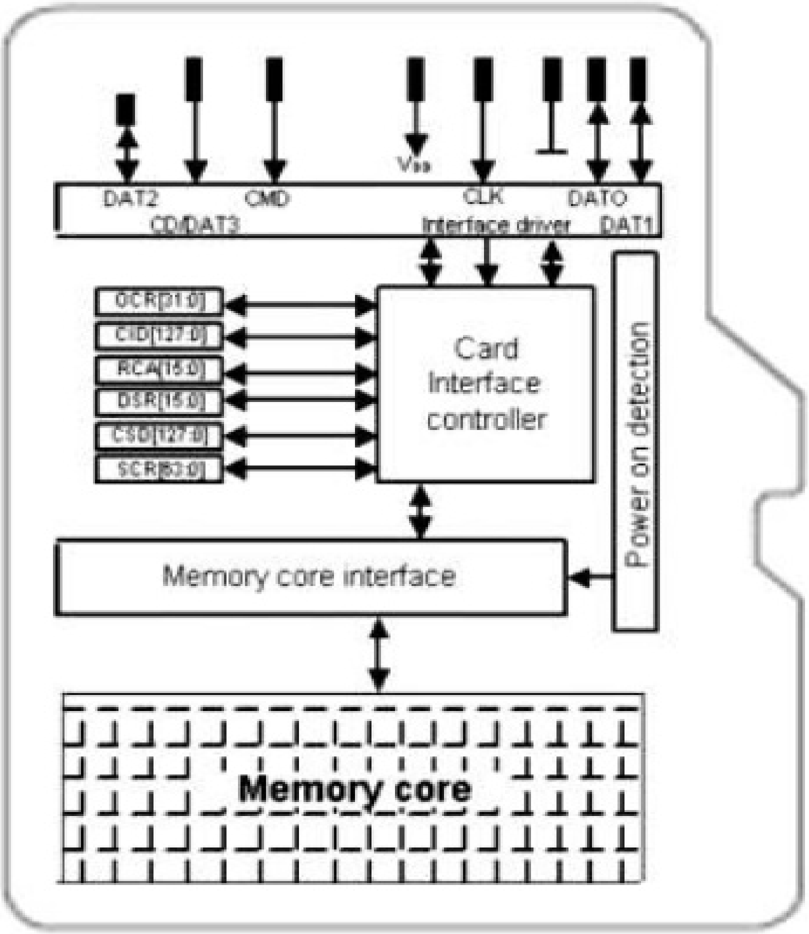
data storage device used for storing and retrieving digital information using one or ("hard") rapidly rotating disks (platters) coated with magnetic material.



Memory Card

memory card or flash card is an electronic flash memory data storage device usec
toring digital information.





Seizure of Devices

hen it comes to collection of evidence, the procedure for thering evidences from switched-off systems and live stems have to be complied with the search and seizure.

evices seizure include, seizure of stem(Desktop/Laptop),Memory devices/storage media

Hashing

ashing used to ensure the integrity of the digital evidence and the media content.

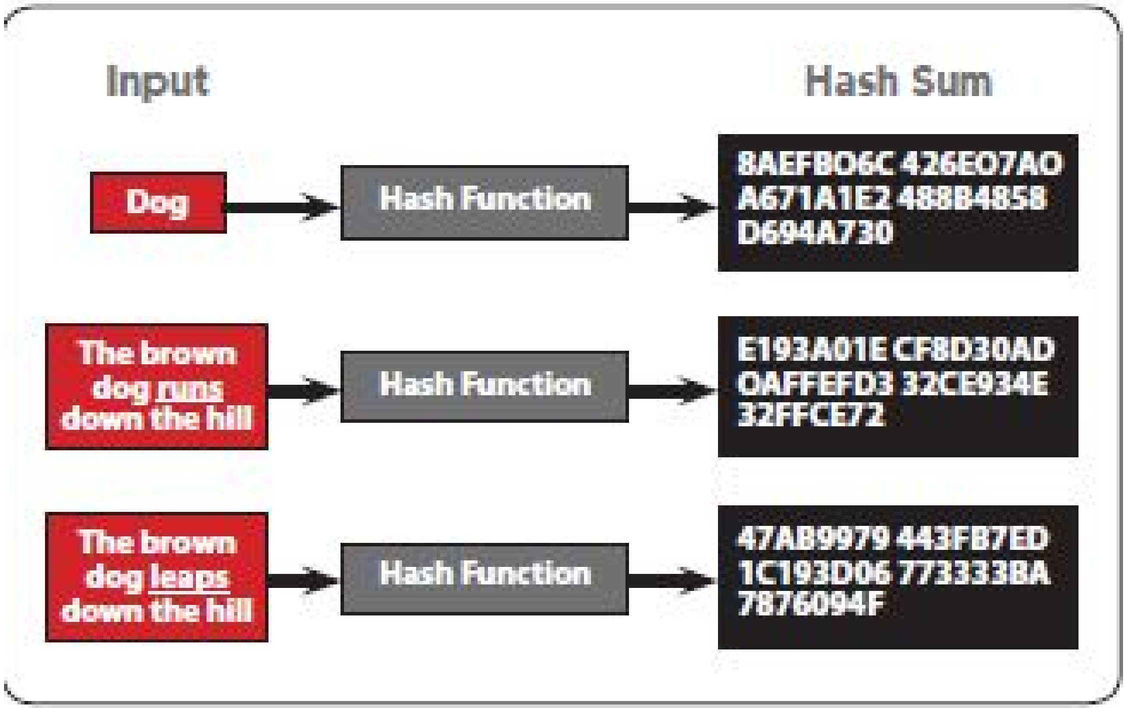
efore hashing a **Write-Blocker** hardware must be used Hashing is done using a has gorithm in which certain mathematical computations are used which creates a uni lue called **Hash Value**.

the evidence is *altered* in any way, the hash value will also change.

Hash Value

hash value is a result of a calculation (hash algorithm) that can be performed on a ring of text, electronic file or entire hard drives contents.

ch hashing algorithm uses a specific number of bytes to store a “ thumbprint” of t ntents.


Input
Hash Sum
Dog
Hash Function
8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730
The brown dog runs down the hill
Hash Function
E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72
The brown dog leaps down the hill
Hash Function
47AB9979 443FB7ED 1C193D06 773333BA 7876094F

xamples of hash values for the same text file using different Algorith

D5: 464668D58274A7840E264E8739884247

A-1: 4698215F643BECFF6C6F3D2BF447ACE0C067149E

A-256: F2ADD4D612E23C9B18B0166BBDE1DB839BFB8A376ED01E32FADB03A0D1B720C7

A-384:2707F06FE57800134129D8E10BBE08E2FEB622B76537A7C4295802FBB94755B
BEE814B101ED18CC2D0126BD66E5D77B6

A-512:C526BC709E2C771F9EC039C25965C91EAA3451A8CB43651EA4CD813F338235F495D37891
D25FE456FE2A8CA89457629378BE63FB3A9A5AD54D9E11E4272D60C

EMD-128: A868B98EAEC84891A7B7BA620EDDE621

ER: F31A22CEED5848E69316649D4BAFBE8F9274DED53E25C02D

NAMA: 7E703B1798A26A0AF21ECD661CBADB9C72B419455814CA7B82E29EE0C03FA493

Write Blockers

rite blockers are devices that allow acquisition of information on a drive w
eating the possibility of accidentally damaging the drive contents.

Cloning

isk cloning is the process of copying the contents of one computer hard disk to anc
sk or to an "image" file.

ction 65(B) of Indian Evidence Act. :Admissibility Of Electronic Recor

Notwithstanding anything contained in this Act, any information contained
electronic record which is printed on a paper, stored, recorded or copi
optical or magnetic media produced by a computer (hereinafter referred
the computer output) shall be deemed to be also a document, if the cond
mentioned in this section are satisfied in relation to the information
computer in question and shall be admissible in any proceedings, without fu
proof or production of the original, as evidence of any contents of the origi
any fact stated therein of which direct evidence would be admissible.

e conditions referred to in the Sub-section (1) in respect to the computer ut shall be following, namely:

(a) the computer output containing the information was produced by computer during the period over which computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the u of computer.

(b) during the said period the information of the kind contained in the electronic record or of the kind from which the information so contained i derived was   regularly fed into the computer in the ordinary course of the said activities.

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was n operating properly or was out of operation for that part of the period, was such to affect the electronic record or the accuracy of its contents.

(d) The information contained in the electronic record reproduces or is derived from such information fed into computer in ordinary course of said activities.

here over any period, the function of storing and processing information for
oses of any activities regularly carried on over that period as mentioned in C
Sub-section (2) was regularly performed by the computers, whether-

(a) by a combination of computer operating over that period, or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over th
period of time; or

(d) in any other manner involving successive operation over that period, in
whatever order, of one or more computers and one or more combinations
computers,

Thank You