**Volatile Evidence– Electronic Evidence General Procedure**

**Volatile data collection from the Window system-**

Forensic Investigation: Capturing the system’s RAM allows forensic investigators to analyze the volatile data present in the memory. This data can provide valuable insights into the state of the system at the time of an incident, such as active processes, network connections, and open files.

Evidence Preservation: RAM captures serve as a means to preserve potential evidence that may be lost once the system is powered off. By capturing the volatile data, investigators can ensure that critical information is not lost and can be used for further analysis and evidence gathering.

* Live System Analysis: Analyzing the system’s RAM in real-time provides a snapshot of the system’s current state. This can help investigators identify running processes, active network connections, malicious activities, or any unauthorized access to sensitive data.
* Memory Artifacts: The RAM contains various artifacts, such as passwords in clear text, encryption keys, clipboard data, and recently accessed files, which may not be available through traditional file system analysis. Capturing the volatile data allows investigators to uncover these artifacts and gather valuable information for their investigation.
* Malware Detection: Volatile data collection from RAM can help in identifying and analyzing malware residing in memory. Malicious processes or suspicious activities can be detected by examining memory structures, code injection, or abnormal behavior patterns, aiding in the identification and removal of malware.
* Incident Response: Capturing volatile data from RAM is crucial for incident response teams to understand the scope and impact of an incident. It provides real-time visibility into system activities and helps in making informed decisions regarding containment, remediation, and preventing further damage.

procedure for electronic evidence-

The only options to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence court or it's copy by way secondary evidence U/s 65A/65B of Evidence Act. Thus, in the case of CD, DVD, Memory Card etc.

Section 65B - Admissibility of Electronic Records

Sec. 65B(1): Notwithstanding anything contained in this Act, any information contained in an electronic record -

• which is printed on a paper, stored, recorded or

• copied in optical or magnetic media

• produced by a computer

# shall be deemed to be also a document, if the conditions mentioned in this section are satisfied

• in relation to the information and

• computer in question and

# shall be admissible in any proceedings, without further proof or production of the original,

# as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Sec. 65B(2):

# The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used;

# Information was fed in computer in the ordinary course of the activities of the person having lawful control over the computer;

# The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

# Information reproduced is such as is fed into computer in the ordinary course of activity.

Sec.65 B(3):

The following computers shall constitute as single computer-

# by a combination of computers operating over that period; or

# by different computers operating in succession over that period; or

# by different combinations of computers operating in succession over that period; or

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

Sec. 65B(4):

Regarding the person who can issue the certificate and contents of certificate, it provides the certificate doing any of the following things:

• identifying the electronic record containing the statement and describing the manner in which it was produced;

• giving the particulars of device

• dealing with any of the matters to which the conditions mentioned in sub-section (2) relate.