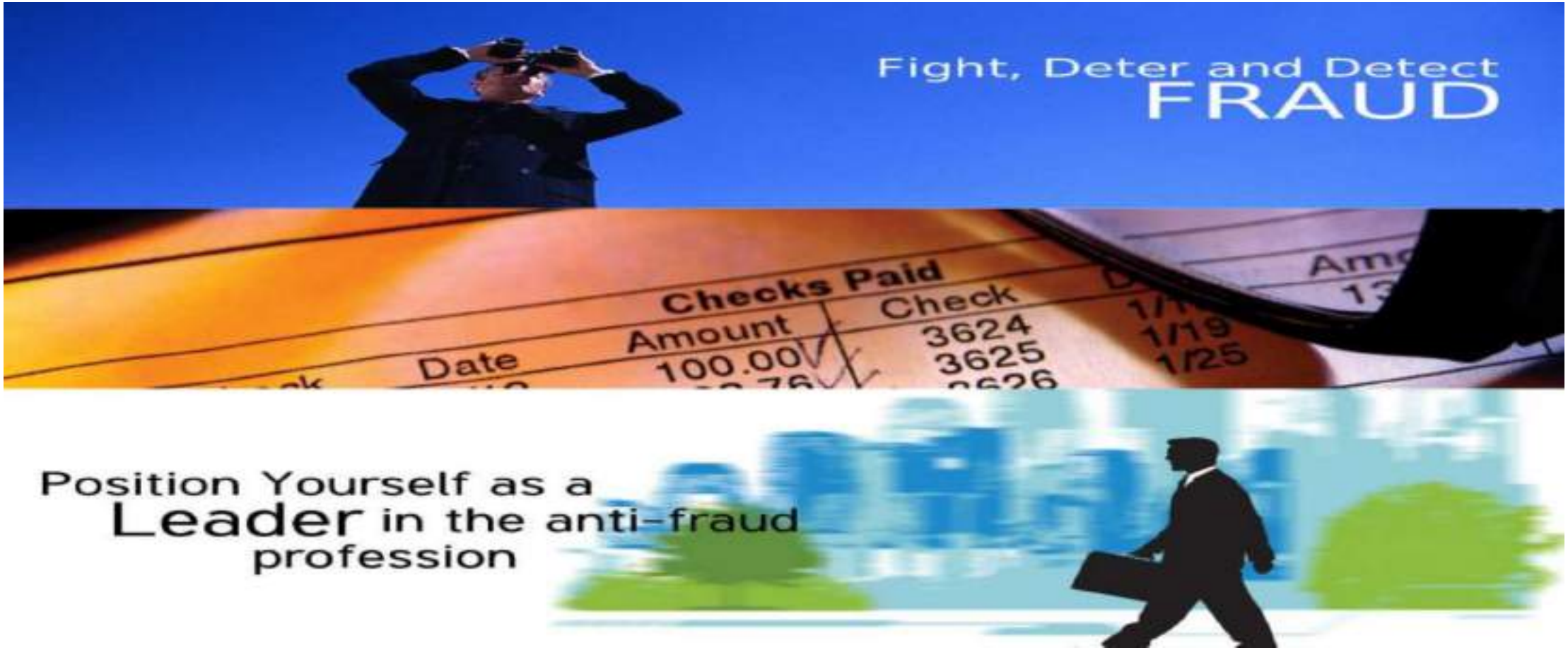
CA. Makrand Wagh

When FRAUD happen Forensic need to be done



Types of FRAUD

- Corporate Fraud -Data Theft, Vendor favouritism, kickbacks etc

    - Financial Fraud-Tax fraud, money laundering
    - Bank Frauds, NPAs,Public sector frauds
    - Intellectual Property Theft/Crime
    - Cyber frauds
    - Corporate Fraud
    - Insurance Fraud –Document forgery, Fake claims etc

What is Forensic Accounting

- The Inegration of accounting, auditing and investigative skills yields the speciality known as Forensic Accounting.

- In other words:
  - The identification, interpretation, and communication of the **evidence** of economic transaction and reporting events
  - **Forensic accounting** is the specialty practice area of accountancy that describes engagements that result from actual or anticipated disputed or litigation “Forensic” means “suitable for use in a court of law”

Forensic Audit Vs Normal Audit

- Forensic Audit is collection ,examination & reporting of evidence admissible in a court of law.
- Forensic audit is issue based or related to specific problem
- Various stages in forensic audit
    - Accounting Review
    - Digital forensic analysis
    -On site investigations
- Audit depends on documentary evidence, while a forensic audit examines the reliability of
- Documentary evidence

Investigation Procedure

- Perform an preliminary investigation-Identify basic information required & accordingly decide **scope of work**
- **Planning** –should identify target to be achieved & Plan audit methodology.
- **Collect relevant info-**

  -Examination of hard copy & electronic info

  -Electronic data-Desktops,laptops, servers, & other data storage devices

  -Collect the data In forensically sound manner so that it is admissible in court

  proceedings.

- **Perform the analysis-**

  -Collect the case background

Investigation Procedure Cont.

-Plan your analysis as per the case requirement

-Gathering relevant data collected from various evidences & reviewing it according to the engagement

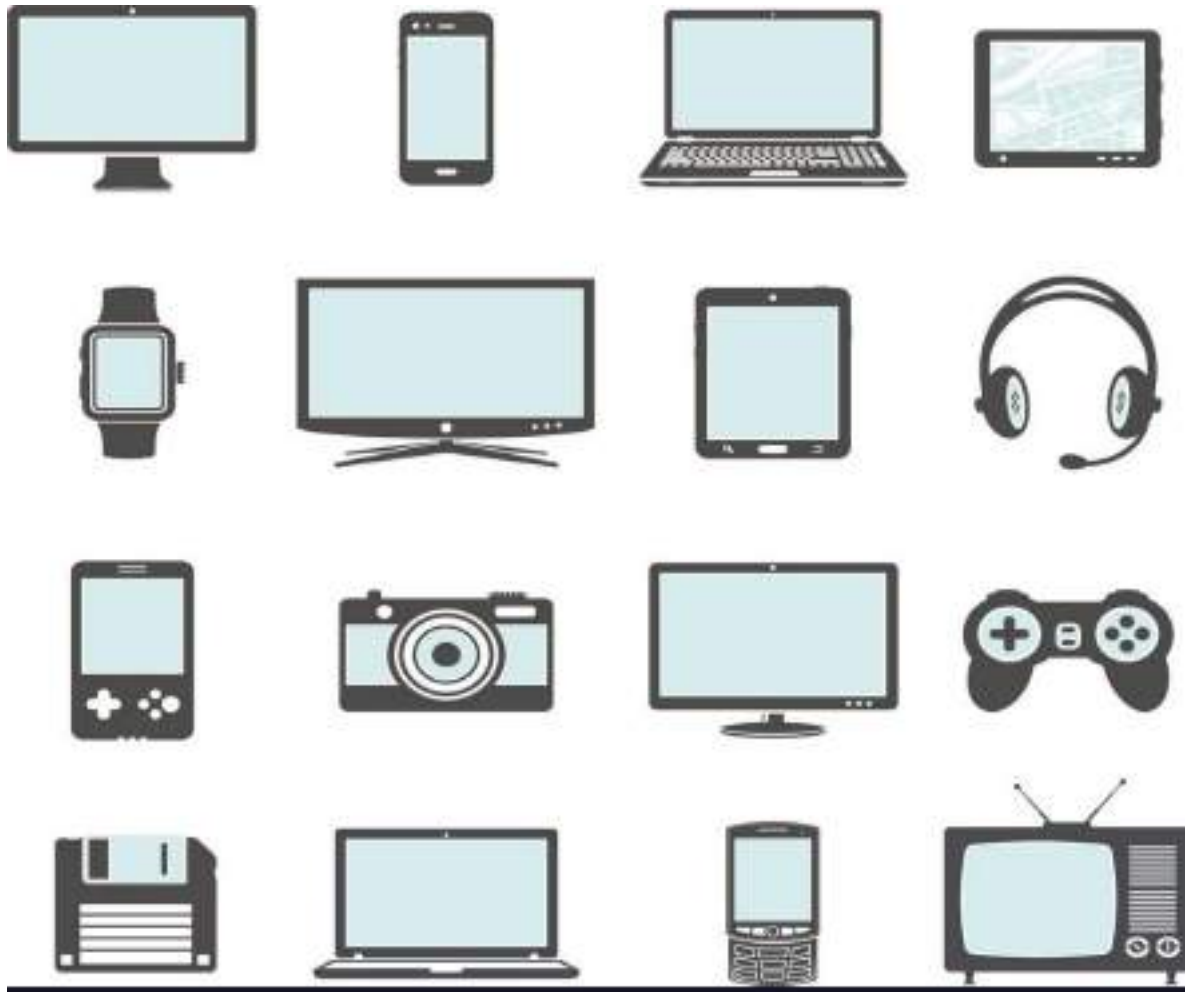
- **Prepare the report-**

  -Should contain details of the engagement, case background

  -identify those involved & create a fact based report

  -Detailed summary of the findings.

Most of Evidence are in Digital device



- When we talk about forensic then that data having itself prove original.
- Most of evidence having data in eletorinc from which is stored into digital device.
- That data is also need to extract from digital device forensically sound.
- Some e.g. of digital device

Scientific Cyber Forensics?

What ? The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

How ? Through the digital forensics investigation process including: Identification, Preservation, Analysis, and Presentation (IPAP).

Why? Used in criminal investigations to identify what happened, how it happened, when it happened and the people involved.

Types of Cyber Forensic

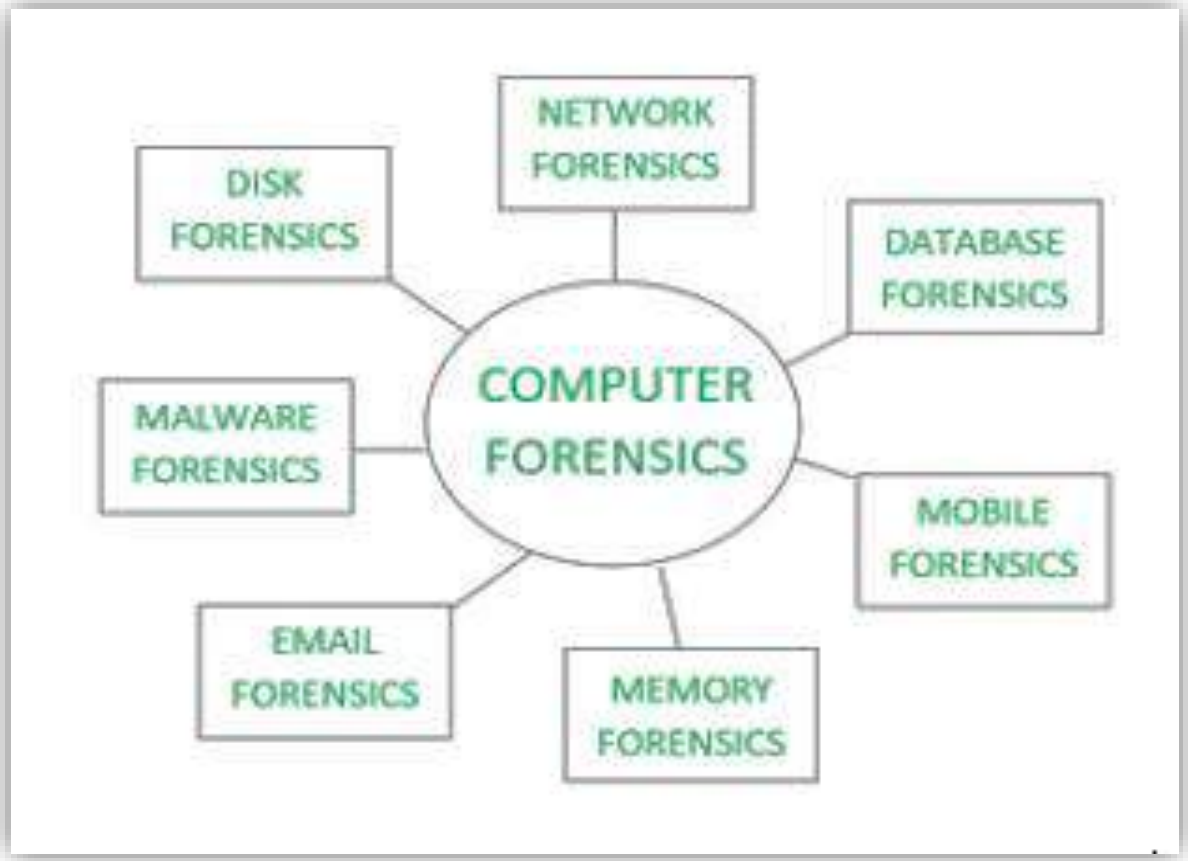
Live Forensic:

- Network Analysis
- Log Generation
- Malware Forensics/Behavior

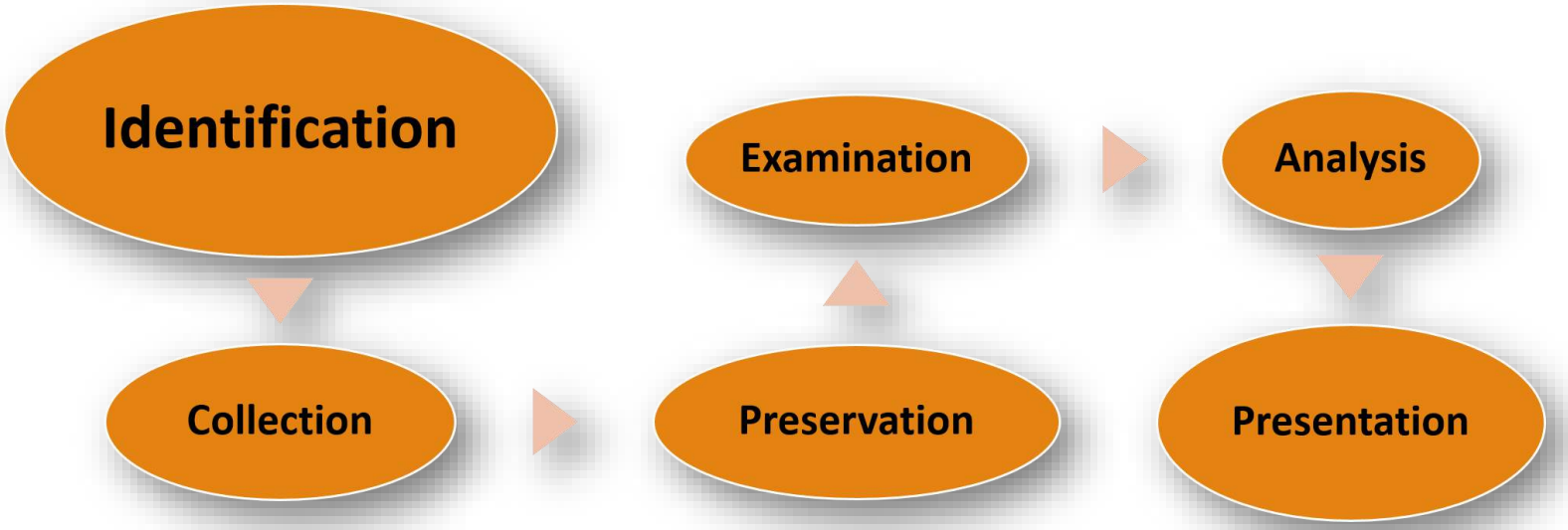
- *Dead Forensics*
- Computer Forensic
- Mobile Forensic
- Network Forensic
- Audio Forensic
- Video Forensic

What is Computer Forensics?

Cyber Forensics is a scientific method of investigation and analysis in order to gather evidence from the digital devices or computer networks and components which is suitable for presentation in a court of law or legal body.



Cyber Forensics Investigation Process Model



Step 1 : Identification Continued....

Internal Hard Disk

External Hard Disk

Memory Cards

CD/DVD

Floppy

SIM Card

Step 1 : Identification Continued....

Mobile Phones

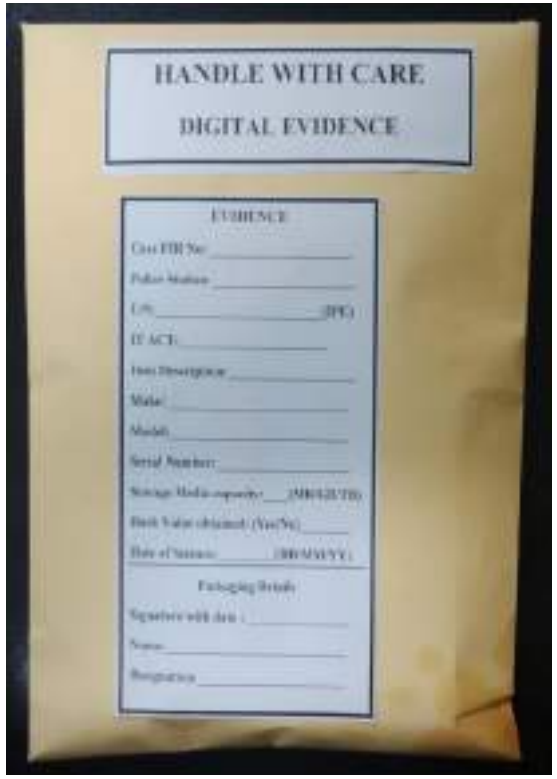
Packaging and Transportation

Hard disk (Evidence)

Anti-Static Wrap

Bubble Wrap

Packaging and Transportation



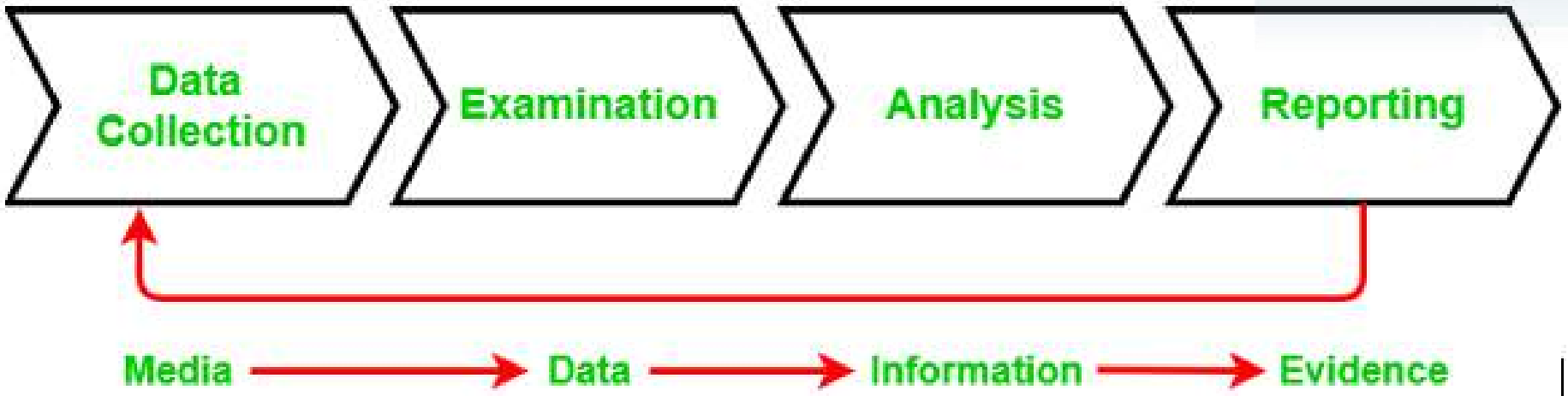
Evidence Labeled

Envelope Seal

Sample Seal

Documentation and Reporting : Chain of Custody

- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
- It demonstrates trust to the courts and to the client that the evidence has not tampered.



Forensic Imaging of the evidence

- Introduction to Imaging
- Importance of Imaging
- Hash algorithms
- Integrity of the evidence
- FTK/Encase Imaging and Write Blockers

What are Write Blockers?

Write Blocker is a tool designed to prevent any write access to the hard disk, thus permitting read-only access to the data storage devices without compromising the integrity of the data

Different types of Write Blockers:
Hardware Write Blocker and Software Write Blocker.

Hash Algorithm

=

79054025
255fb1a2
6e4bc422
aef54eb4

Hash Values: When a forensic investigator creates an image of the evidence for analysis, the process generates cryptographic hash values like MD5, SHA1, etc. Hash Values are critical as:

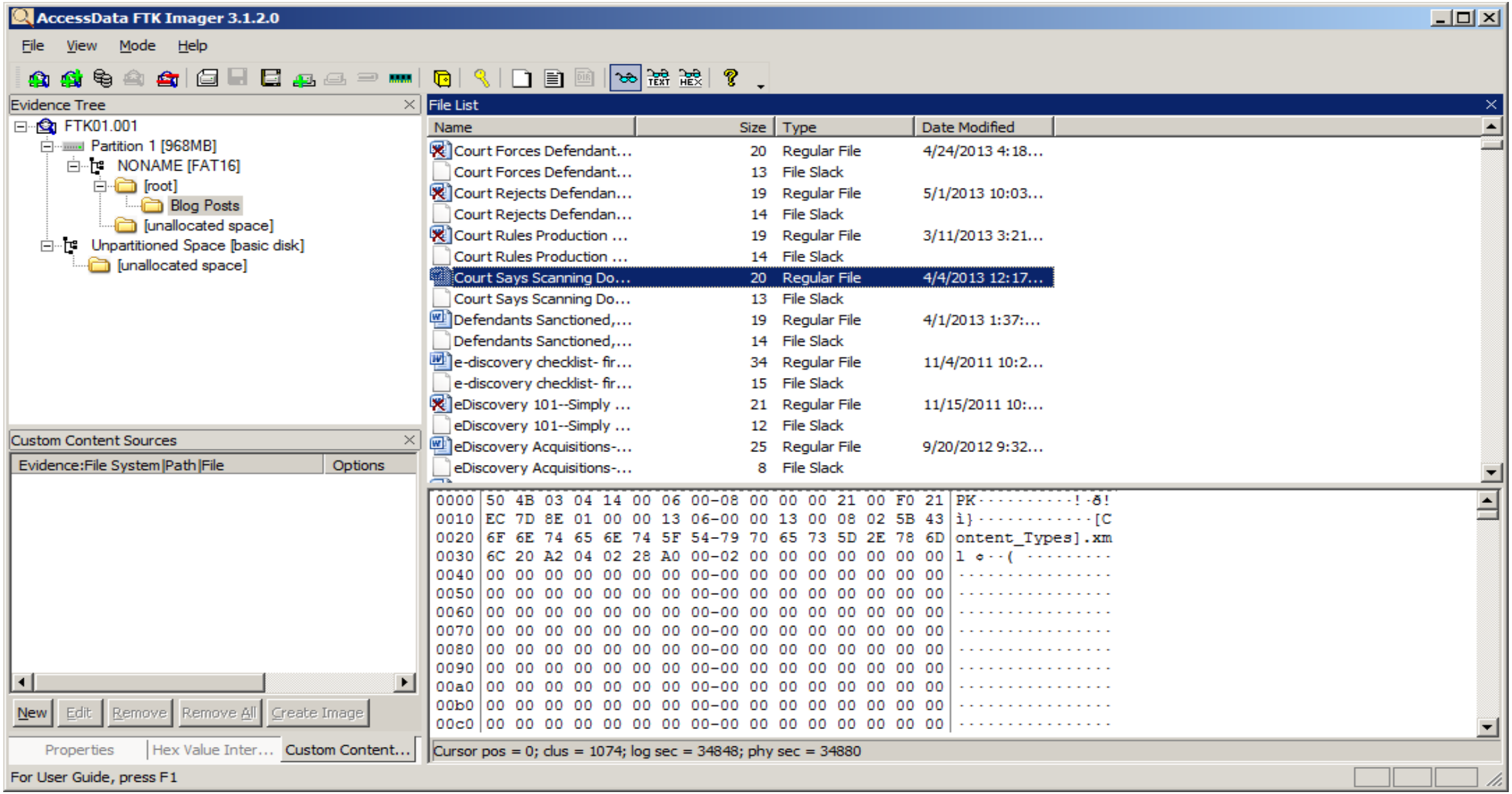
• They are used to verify the Authenticity and Integrity of the image as an exact replica of the original media.

• Type of Hash value

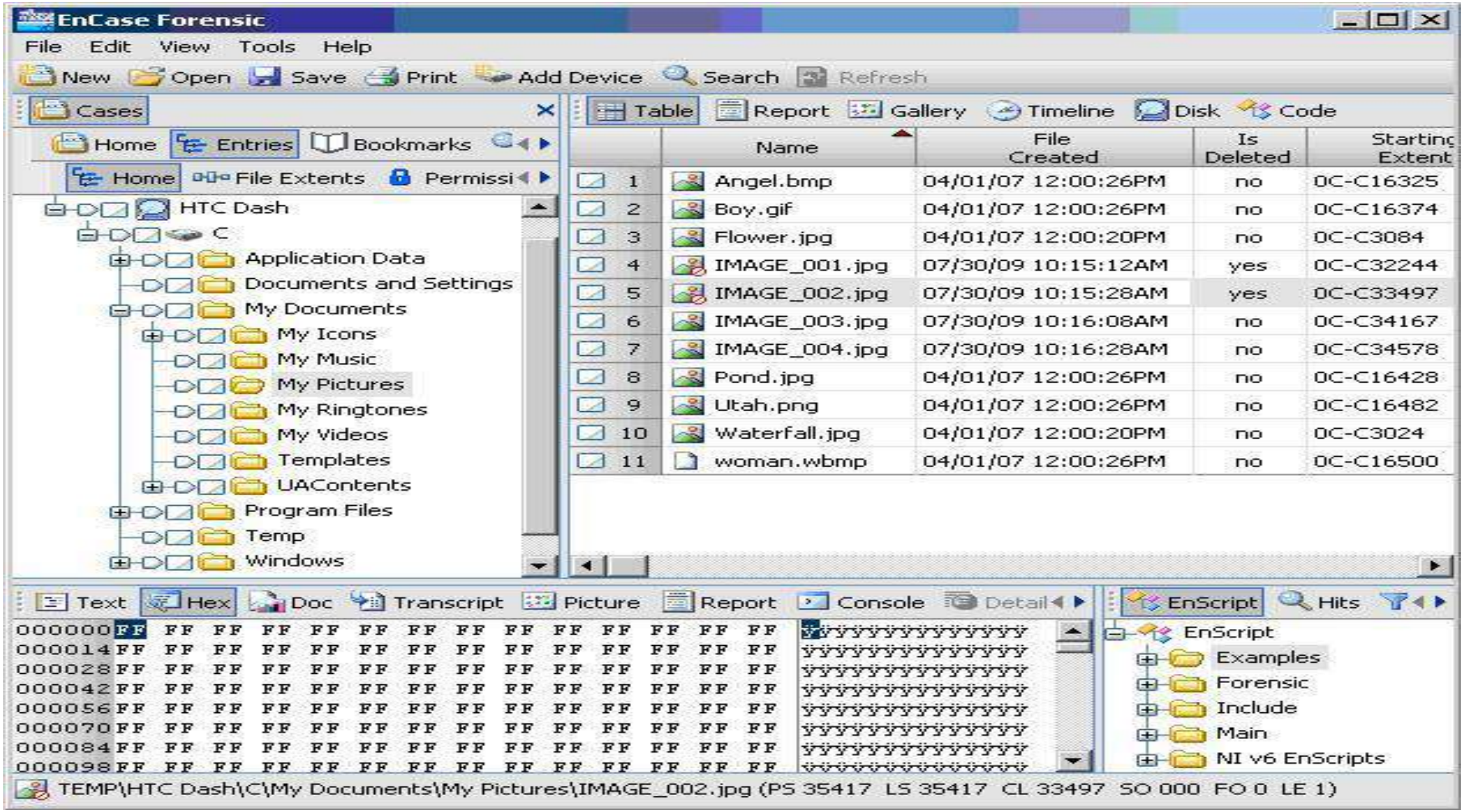
1. MD 5
2. SHA 1
3. SHA 2

If the hash values of the image and the original evidence do not match, it may raise concerns in court that the evidence has been tampered with.

FTK IMAGER


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
FTK01.001
Partition 1 [968MB]
NONAME [FAT16]
[root]
Blog Posts
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name Size Type Date Modified
Court Forces Defendant... 20 Regular File 4/24/2013 4:18...
Court Forces Defendant... 13 File Slack
Court Rejects Defendan... 19 Regular File 5/1/2013 10:03...
Court Rejects Defendan... 14 File Slack
Court Rules Production ... 19 Regular File 3/11/2013 3:21...
Court Rules Production ... 14 File Slack
Court Says Scanning Do... 20 Regular File 4/4/2013 12:17...
Court Says Scanning Do... 13 File Slack
Defendants Sanctioned,... 19 Regular File 4/1/2013 1:37:...
Defendants Sanctioned,... 14 File Slack
e-discovery checklist- fir... 34 Regular File 11/4/2011 10:2...
e-discovery checklist- fir... 15 File Slack
eDiscovery 101--Simply ... 21 Regular File 11/15/2011 10:...
eDiscovery 101--Simply ... 12 File Slack
eDiscovery Acquisitions-... 25 Regular File 9/20/2012 9:32...
eDiscovery Acquisitions-... 8 File Slack
0000 50 4B 03 04 14 00 06 00-08 00 00 00 21 00 F0 21 PK..........!.ð!
0010 EC 7D 8E 01 00 00 13 06-00 00 13 00 08 02 5B 43 ì}..........[C
0020 6F 6E 74 65 6E 74 5F 54-79 70 65 73 5D 2E 78 6D ontent_Types].xm
0030 6C 20 A2 04 02 28 A0 00-02 00 00 00 00 00 00 00 l ¢..(........
0040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
00c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ....
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Content...
Cursor pos = 0; clus = 1074; log sec = 34848; phy sec = 34880
For User Guide, press F1

Encase Imager



Computer Forensics provide following: deleted data as well as present data.

Personal Information
User Accounts

System Information
OS Details , Mac Address , IP address , Program or Software installed , Logs

Web browser items
Bookmarks, Cookies, History , Search Hits

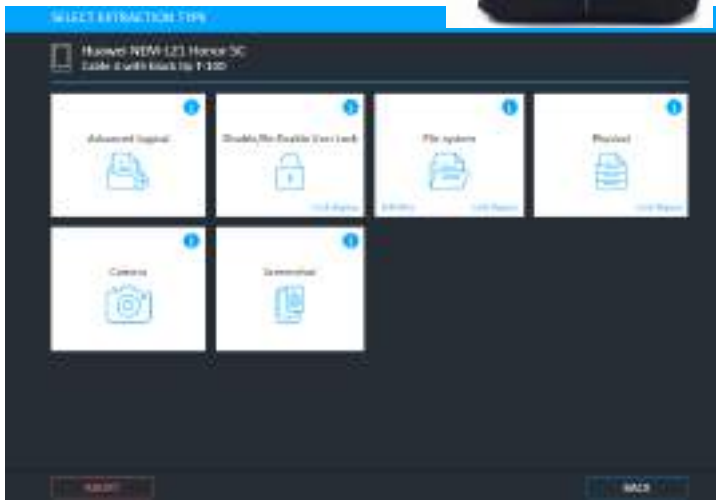
GPS information
Fixes, Journeys, Locations

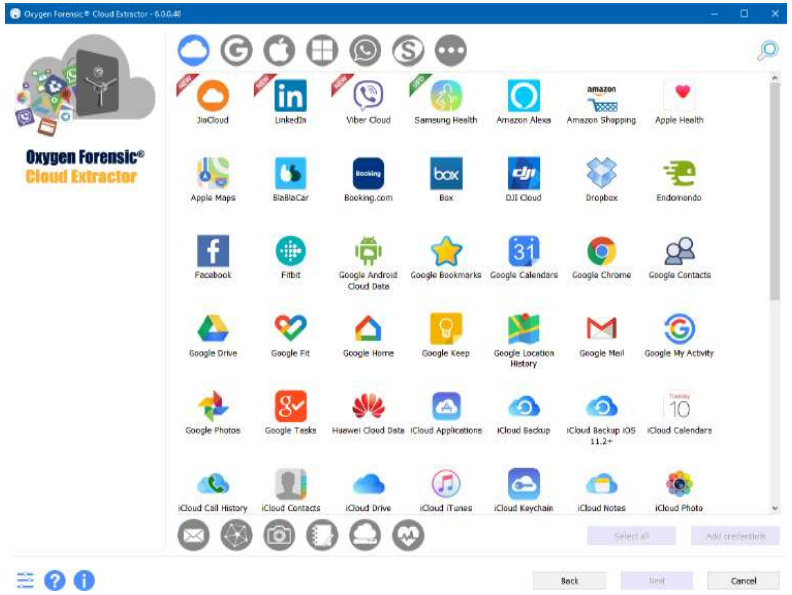
Data Files Images , Videos, Audio, Text, Databases, Configurations, Applications, Documents

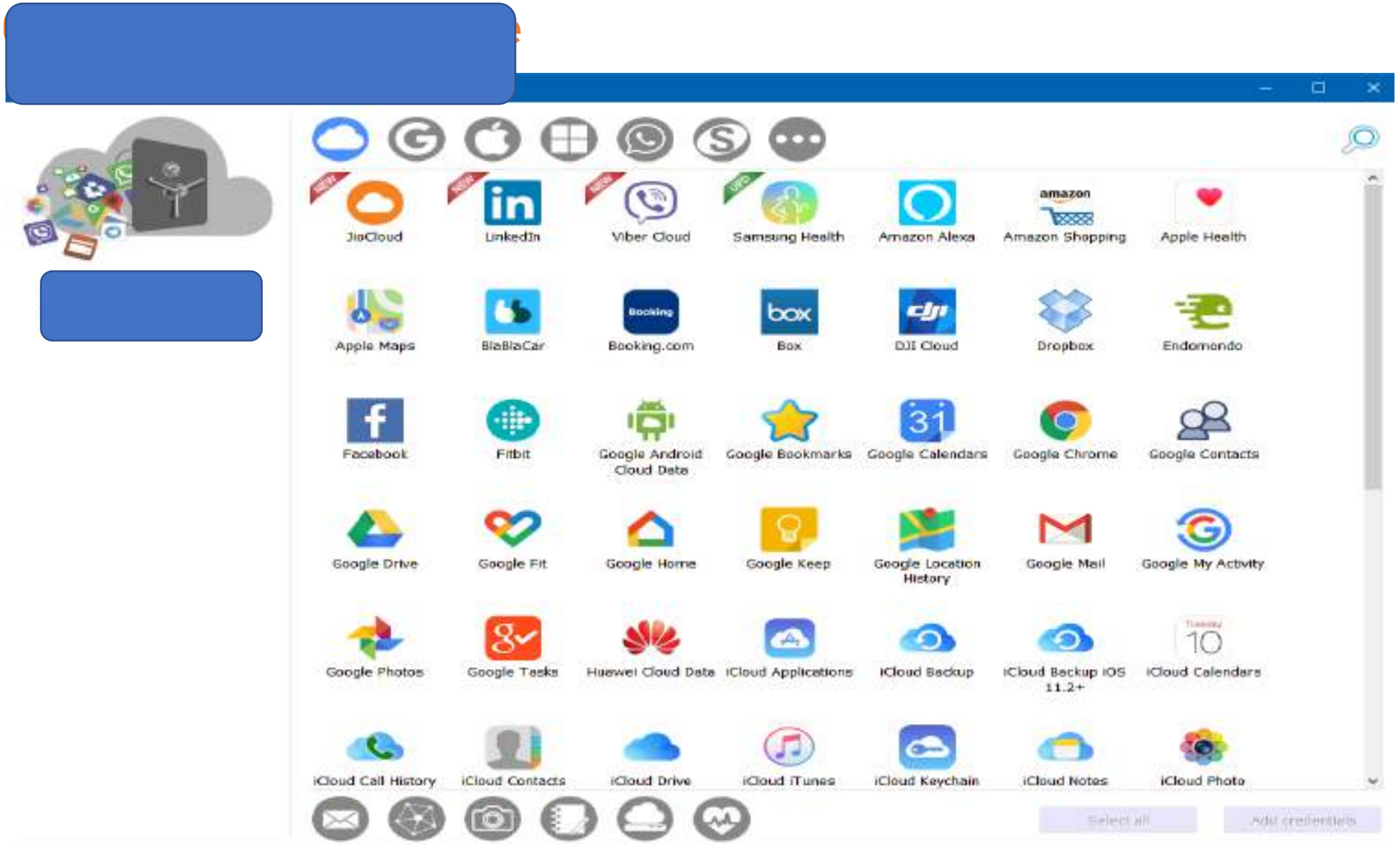
Mobile extraction of data provide following:

(depend on the device manufacturer and device model)

- Personal information - Calendar, Call Log, Contacts, Notes, User Dictionaries, User Accounts
- Messaging items – Chats, Email, Instant Messages, MMS, SMS
- Web browser items - Bookmarks, Cookies, History
- GPS information – Fixes, Journeys, Locations
- Device information - Application Usage, Bluetooth Pairings, Cellular Locations, SIM Data, Wireless Networks
- Data Files - Images , Videos , Audio, Text, Databases, Configurations, Applications, Documents






JioCloud
LinkedIn
Viber Cloud
Samsung Health
Amazon Alexa
Amazon Shopping
Apple Health
Apple Maps
BlaBlaCar
Booking.com
Box
DJI Cloud
Dropbox
Endomondo
Facebook
Fitbit
Google Android Cloud Data
Google Bookmarks
Google Calendars
Google Chrome
Google Contacts
Google Drive
Google Fit
Google Home
Google Keep
Google Location History
Google Mail
Google My Activity
Google Photos
Google Tasks
Huawei Cloud Data
iCloud Applications
iCloud Backup
iCloud Backup iOS 11.2+
iCloud Calendars
iCloud Call History
iCloud Contacts
iCloud Drive
iCloud iTunes
iCloud Keychain
iCloud Notes
iCloud Photo
Back
Next
Cancel

CA. Makrand Wagh

sridevi.shetty@macans.in

THANK YOU