Acquisition of Digital Evidence

Presented By Avinash Bhoyar

Our Agenda

01 Digital Forensics Steps

02 Imaging Process

03 Acquisition of Digital Evidence

04 Write Blocker

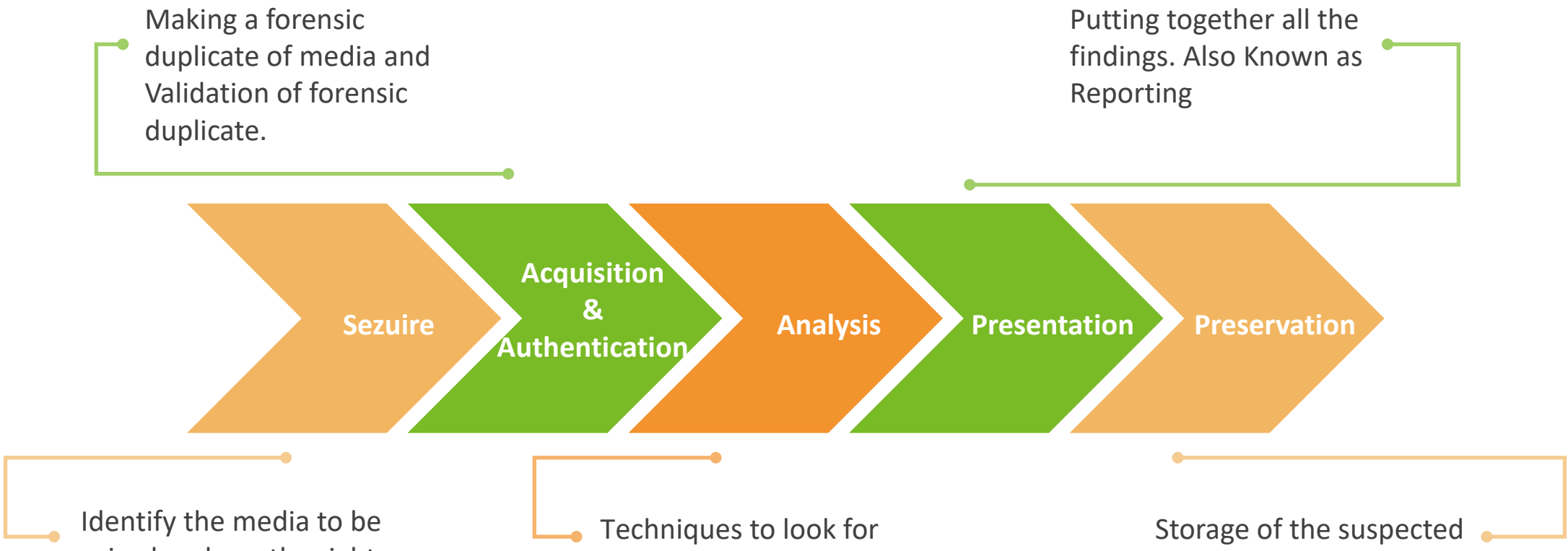
05 Hashing

06 Key for Successful Acquisition

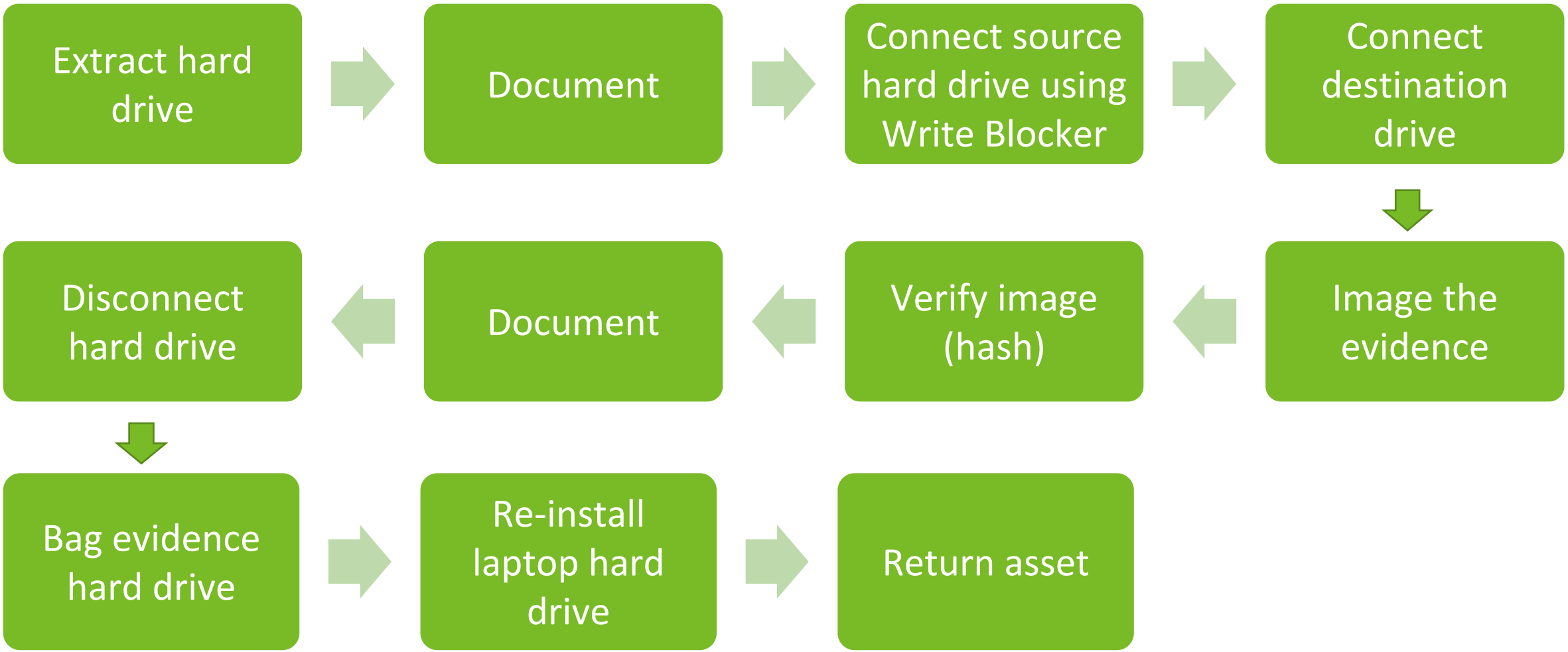
07 Challenges in Acquisitions of Digital evidence

08 Documentation

Digital Forensics Steps

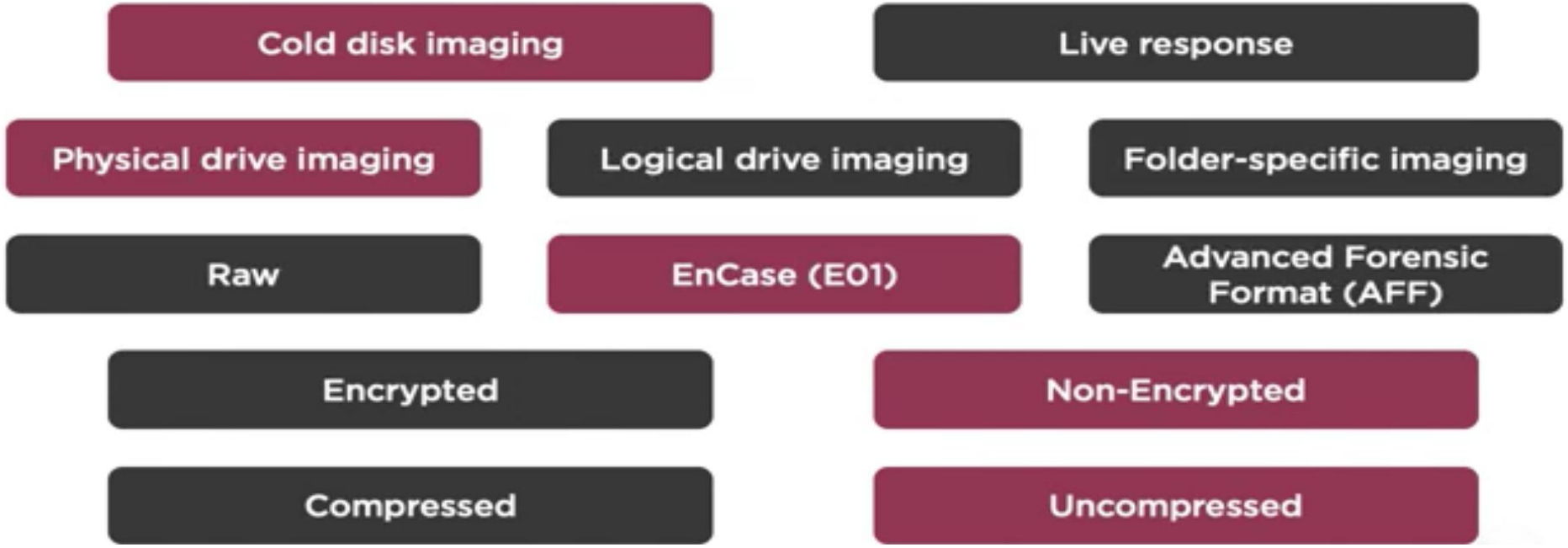


Imaging Process



Aquisition of Digital Evidence

- What is Imaging?
- Types Of Devices Need to be Acquire are as followed
  1. Hard Drive | SD Cards | Pen-Drive | SSD | CD | DVD
  2. Mobile Phones Both Feature-Phones and SmartPhones
  3. SIM cards
  4. Network Capture | RAM etc.
- Acquisition Types as follows



Aquisition of Digital Evidence

❖ File Extensions:

1. Vendor Specific: E01, UFD etc.
2. Open Source Format: DD, AFF4 etc.

RAW	Encase (E01)	Advance Forensic Format(AFF)
• A bit -by-bit copy of Storage • Nothing less, nothing more	• Bit-by-bit copy • Encryption & Compression • Includes metadata such as hashes, timestamps, case details	• Bit-by-bit copy • Encryption & Compression • Includes metadata such as hashes, timestamps

Aquisition of Digital Evidence

- ✓ First of All know to about Digital Device such as make, model, Capabilities etc.
- ✓ Use method accordingly.
- ✓ Types of Tools used:
  1. Stand-Alone Duplication Software
     - A program that run as a separate computer process, not an add-on of an existing process.
     - Example: FTK iamger, Belkasoft Acquisition Tool etc.
  2. Forensic Analysis Software Suite
     - Programs use for forensic analysis along with imaging digital evidences
     - Example: Encase, FTK Toolkit, Magnet Axiom, Autopsy, UFED 4PC etc.
  3. Dedicated Hardware Devices
     - It Independent hardware system capable of doing all work related to first response.
     - Example: UFED Touch2, Forensic Falcon, TD2, SOLO4 etc.

Aquisition of Digital Evidence

Collect Data using Write Blocker

Choose Proper Method of Acquisiton

Validate the Image

Generate the Hash value

Update the Chain of Custody

Write Blocker

- ✓ Use to Write commands to Source while Imaging
- ✓ preserves the integrity of the le metadata
- ✓ Types of Write Blocker
  1. Hardware Write Blocker
     - Its a Hardware Connected between Source and Imaging Workstation/Device.
     - Example: TABLEAU, Forensic ComboDock etc.
  2. Software Write Blocker
     - A software layer that sits in between the OS and the device driver for the storage device.
     - Example: Thumbscrew, FAST BLOC SE(Encase), Linux Write Blocker, Read Only Mounter etc

Hashing

- ✓In digital forensic, to validate digital evidence or to prove its integrity we use hash value. This hash value generate from hashing algorithm.
- ✓Hashing is the transformation of string of character into a usually shorter fixed-lenght hexadecimal value that represents the original string.
- ✓Compare two hard drives
- ✓There are several hashing algorithms that are commonly used, such as MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm), SHA256, and others

  MD5 128bit 32char(4bit/char) 16byte broken 2010

  Sha1 160bit 40char 20byte SHA-NSA Broken in 2015

  Sha2 256bit 64char 32byte

Hashing

- ✓ Use For Authenticating(Validating) digital evidence images.
- ✓ Hashing uses complex mathematical models to generate a unique string for a file
  - “Hash collision” likelihood low
- ✓ Three rules of hash
  1. you can,t predict the hash of file
  2. No two hash values be the same
  3. Anything changes in file or device the hash change
- ✓ The length of the hash depends on the type of hash used.
- ✓ It is one way encryption. Means it irreversible.
- ✓ Tools: Hashcal, Winhex, FTk, encase, Hashmyfiles, DC3DD(data dump) etc.
- ✓ Both encoding and encryption are reversible, and hashing is not.
- ✓ Example: MD5 hash :**4a24e1e50622c52122406b77e8438c5a**

Key for Successful Acquisition

Follow the forensic process

Ask your peer for review

Ensure chain of custody

Be prepared for the acquisition

Document everything

Rehearse the acquisition

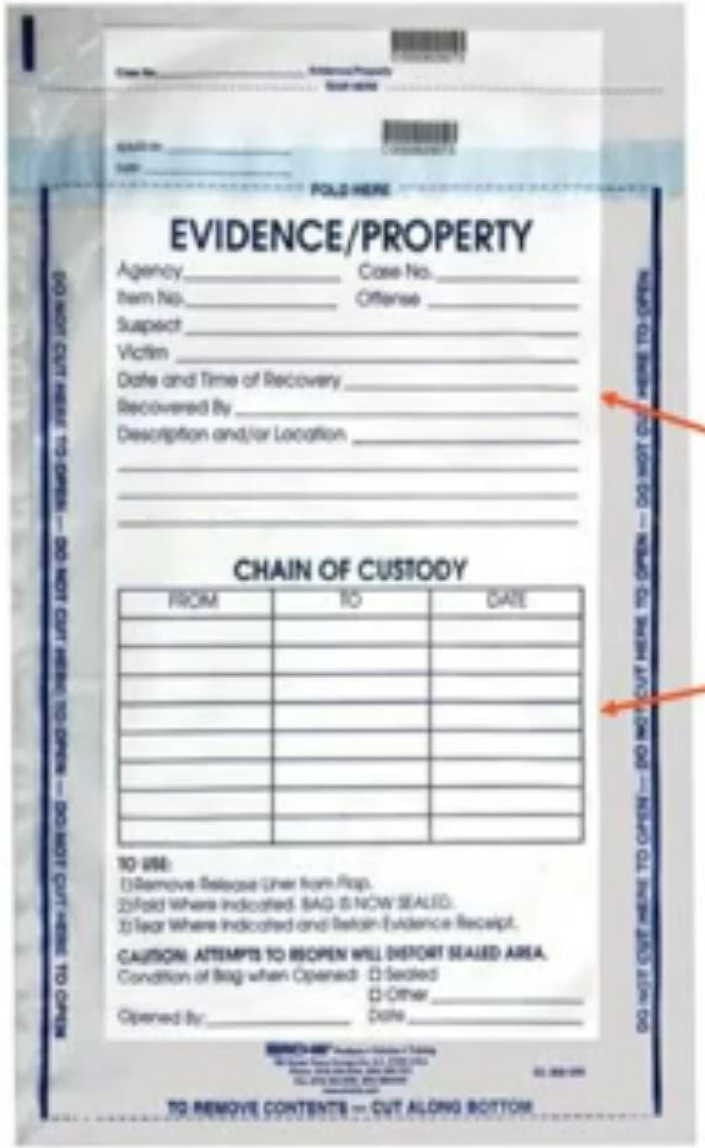
Be honest and communicate your mistakes

Be discrete and professional at the client

Challenges in Acquisitions of Digital evidence

- ✓ Data Volume
- ✓ Legal
- ✓ Advancement and Rapid Change in Technology
- ✓ Hardware Issues

Documentation



Put the evidence hard drive into a forensic bag

Use a new evidence bag

Complete the evidence information

Complete the chain of custody