SNS COLLEGE OF ENGINEERING

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IoT, Cyber Security including Blockchain Technology)

19SB502 – CYBER FORENSIC AND INVESTIGATIONS

III YEAR/ V SEMESTER

UNIT 2 – EVIDENCE COLLECTION AND FORENSICS TOOLS

TOPIC 3 –Computer Forensics Tools

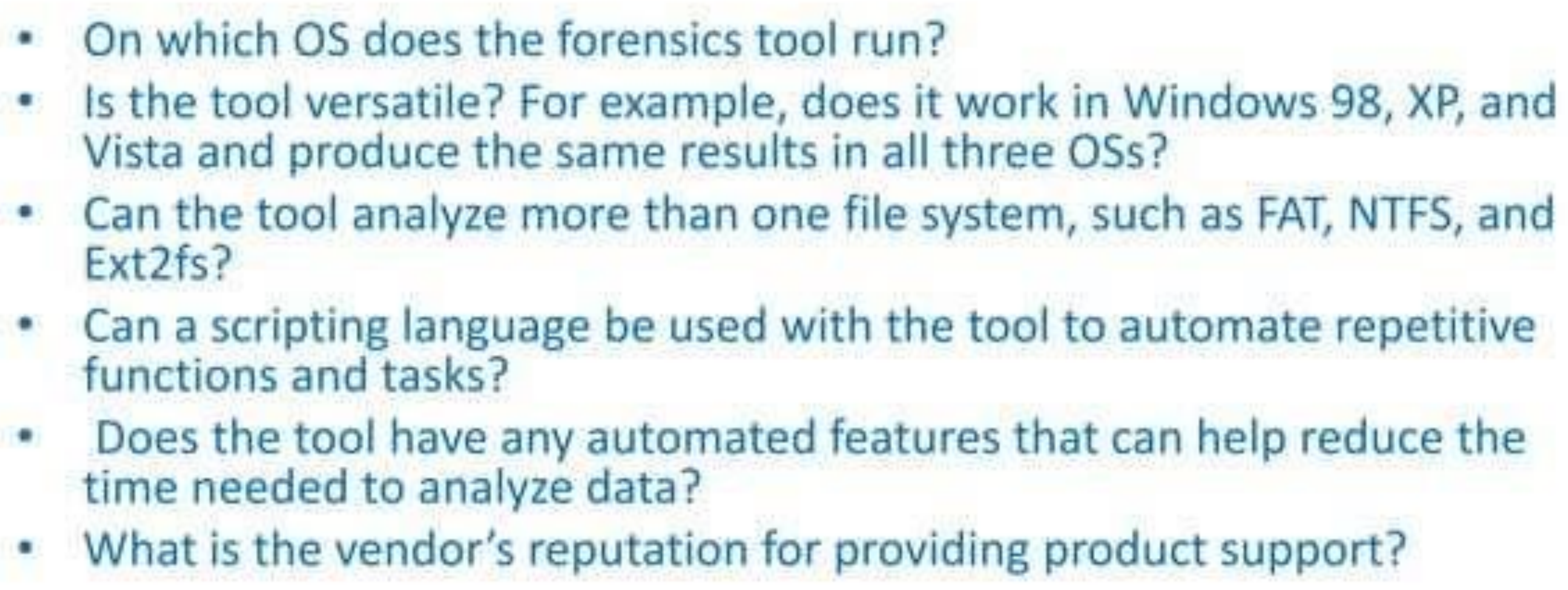
9/3/2024

Current computer Forensic tools

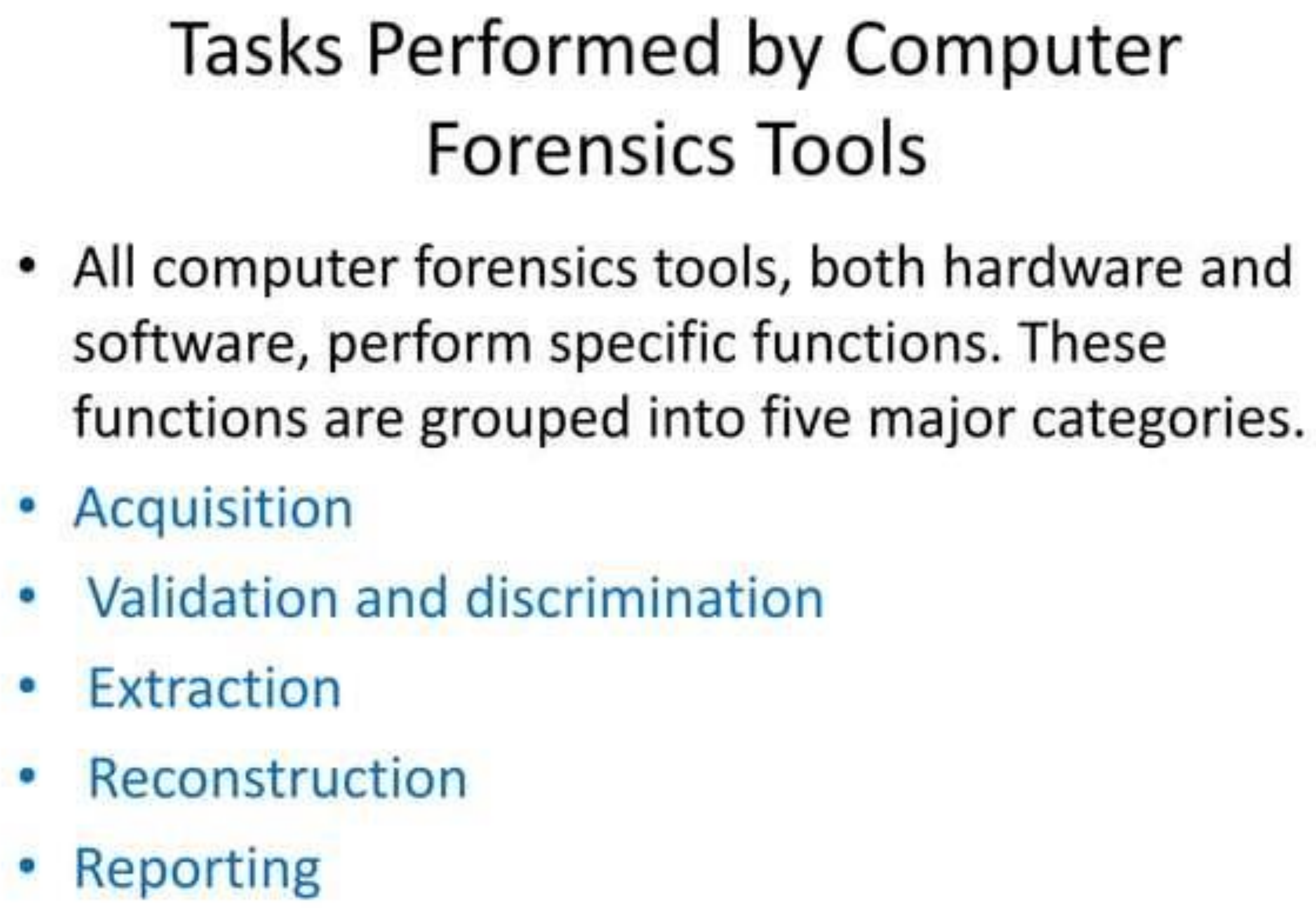
- Computer forensics tools are constantly being developed, updated, patched, and revised. Therefore, checking vendors' Web sites routinely to look for new features and improvements is important.
- Before purchasing any forensics tools, consider whether the tool can save you time during investigations and whether that time savings affects the reliability of data you recover.

Evaluating Computer Forensics Tool Needs

Some questions to ask when evaluating computer forensic tools:



- On which OS does the forensics tool run?
- Is the tool versatile? For example, does it work in Windows 98, XP, and Vista and produce the same results in all three OSs?
- Can the tool analyze more than one file system, such as FAT, NTFS, and Ext2fs?
- Can a scripting language be used with the tool to automate repetitive functions and tasks?
- Does the tool have any automated features that can help reduce the time needed to analyze data?
- What is the vendor’s reputation for providing product support?

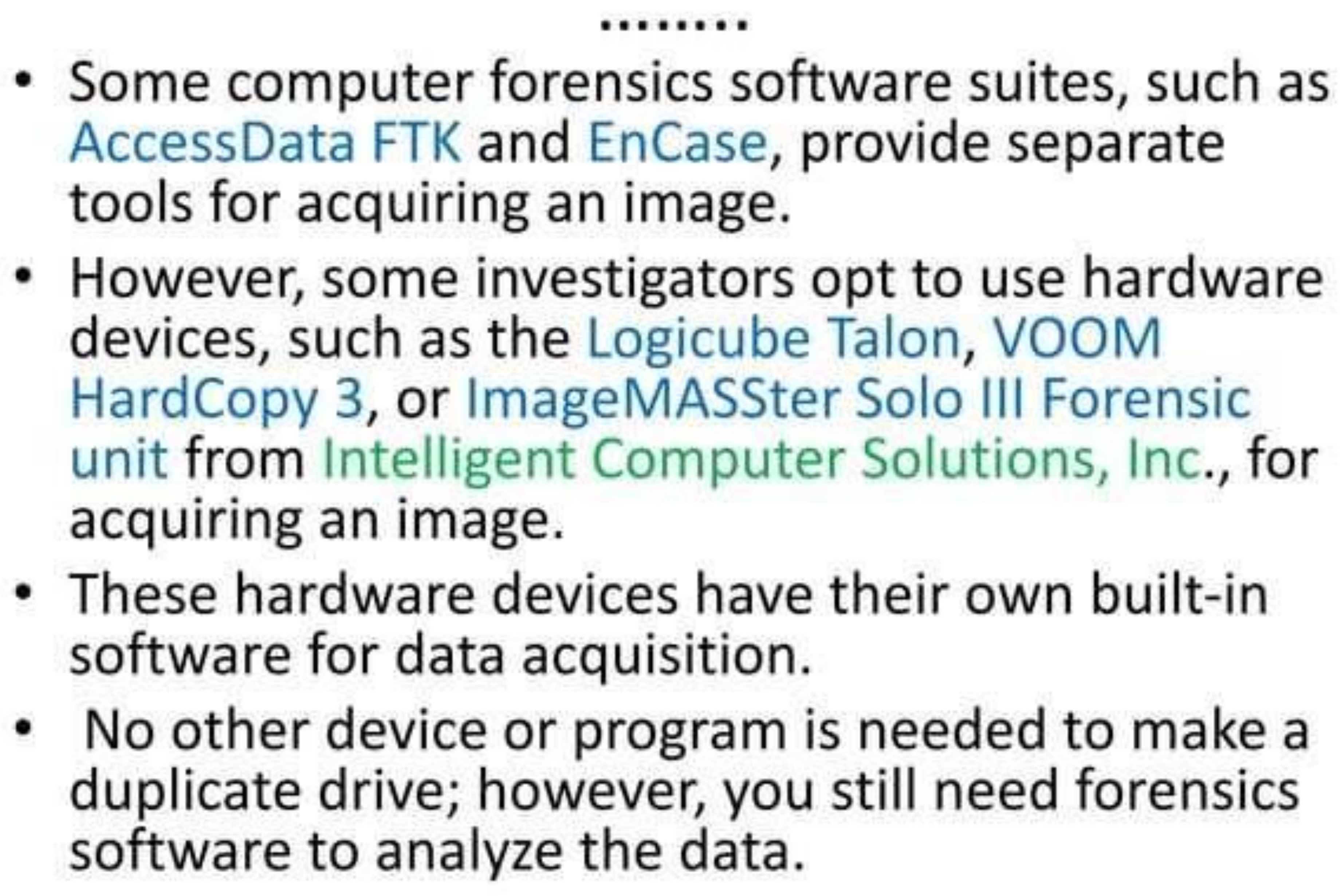


Tasks Performed by Computer Forensics Tools

- All computer forensics tools, both hardware and software, perform specific functions. These functions are grouped into five major categories.
- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

Acquisition

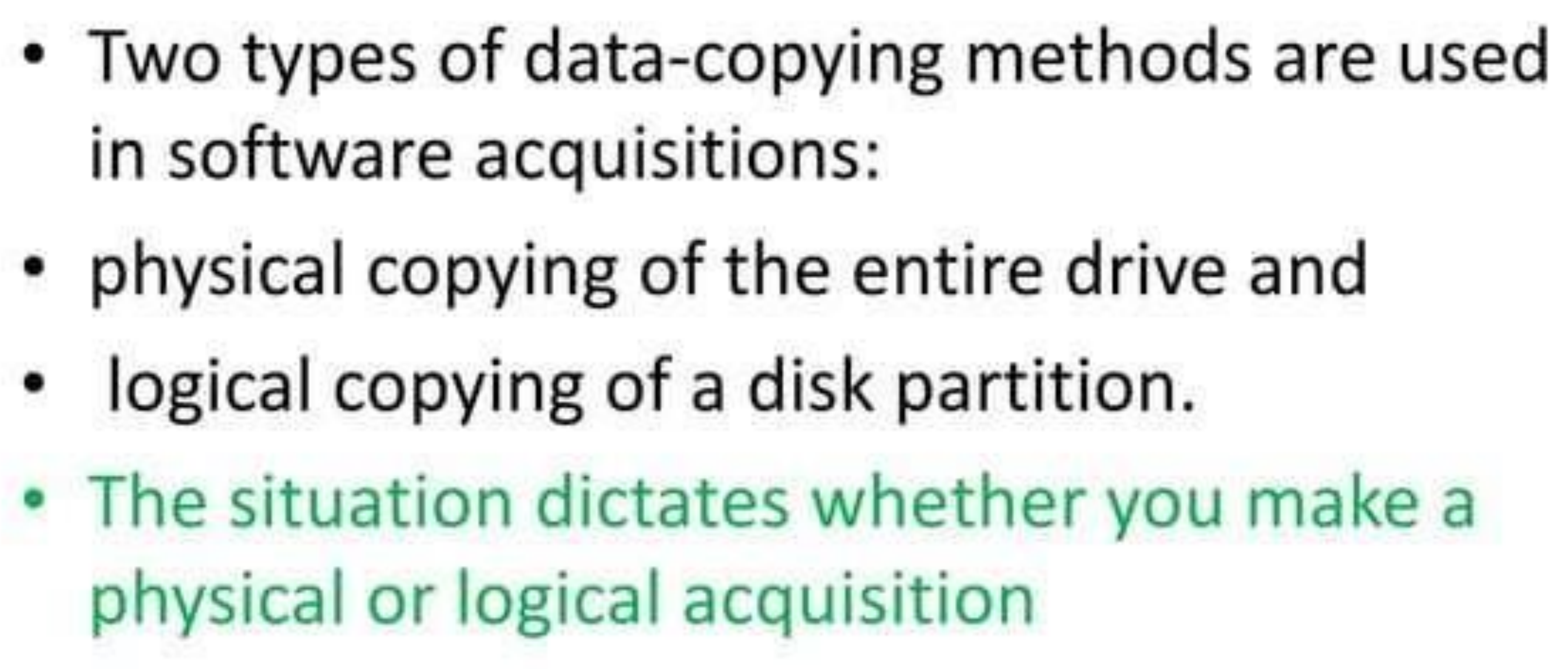
- Acquisition, the first task in computer forensics investigations, is making a copy of the original drive.
- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote acquisition
- Verification



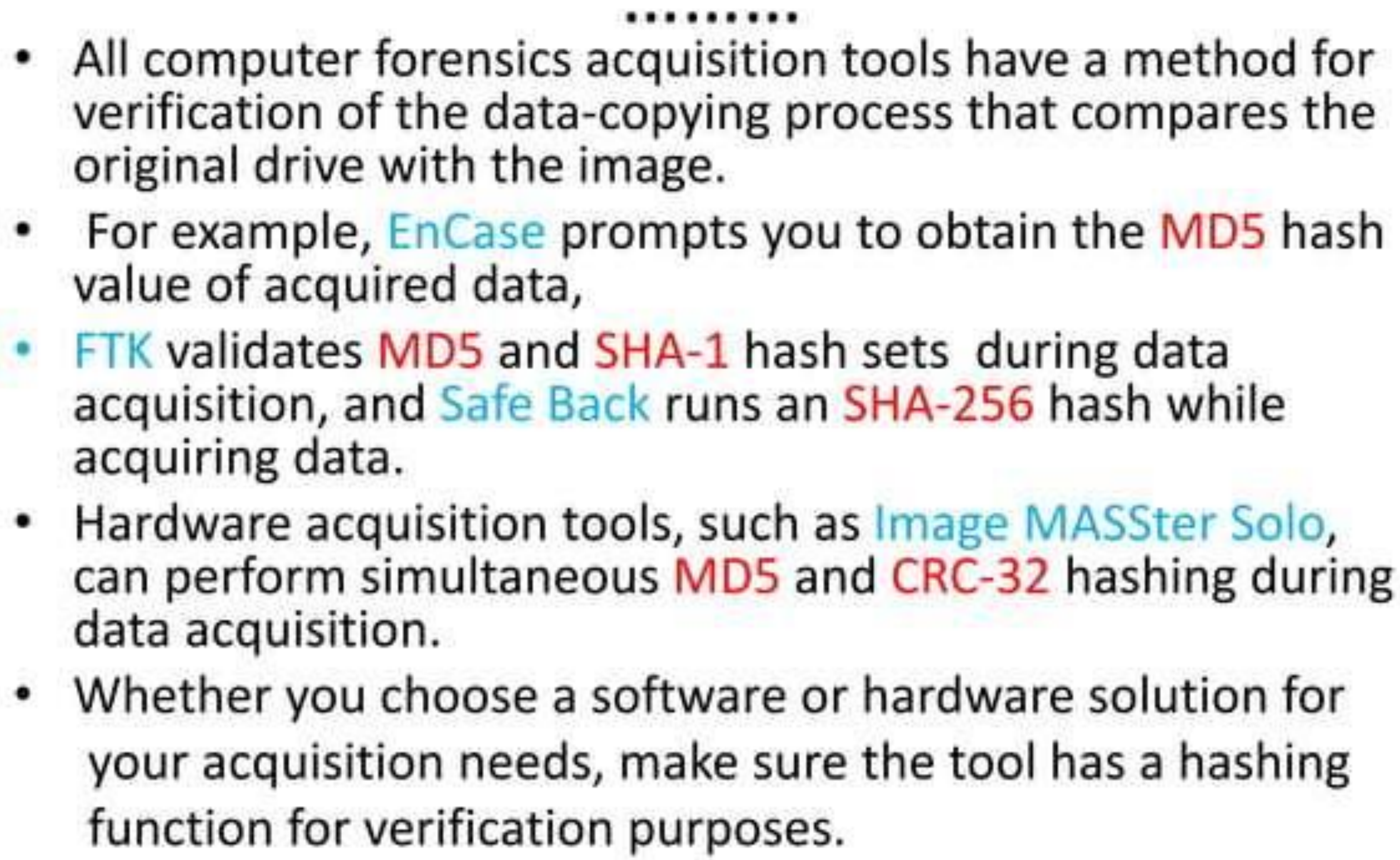
……..

- Some computer forensics software suites, such as AccessData FTK and EnCase, provide separate tools for acquiring an image.
- However, some investigators opt to use hardware devices, such as the Logicube Talon, VOOM HardCopy 3, or ImageMASSter Solo III Forensic unit from Intelligent Computer Solutions, Inc., for acquiring an image.
- These hardware devices have their own built-in software for data acquisition.
- No other device or program is needed to make a duplicate drive; however, you still need forensics software to analyze the data.

....



- Two types of data-copying methods are used in software acquisitions:
- physical copying of the entire drive and
- logical copying of a disk partition.
- The situation dictates whether you make a physical or logical acquisition



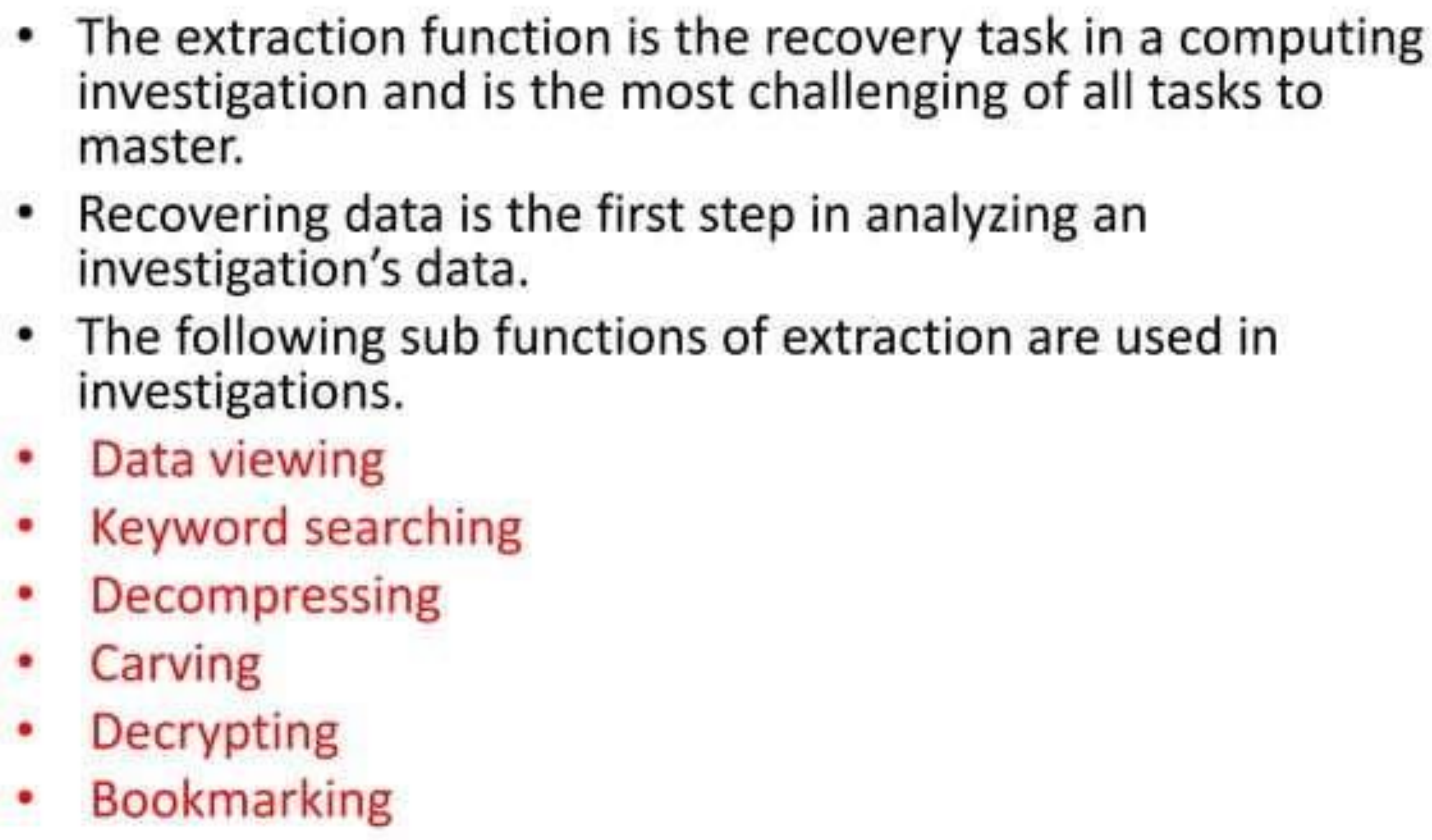
....

- All computer forensics acquisition tools have a method for verification of the data-copying process that compares the original drive with the image.
- For example, EnCase prompts you to obtain the MD5 hash value of acquired data,
- FTK validates MD5 and SHA-1 hash sets during data acquisition, and Safe Back runs an SHA-256 hash while acquiring data.
- Hardware acquisition tools, such as Image MASSter Solo, can perform simultaneous MD5 and CRC-32 hashing during data acquisition.
- Whether you choose a software or hardware solution for your acquisition needs, make sure the tool has a hashing function for verification purposes.

Validation and Discrimination

- Two issues in dealing with computer evidence are critical.
- First is ensuring the integrity of data being copied—the validation process.
- Second is the discrimination of data, which involves sorting and searching through all investigation data.
- Many forensics software vendors offer three methods for discriminating data values.

Extraction



- The extraction function is the recovery task in a computing investigation and is the most challenging of all tasks to master.
- Recovering data is the first step in analyzing an investigation's data.
- The following sub functions of extraction are used in investigations.
- Data viewing
- Keyword searching
- Decompressing
- Carving
- Decrypting
- Bookmarking

SNS COLLEGE OF ENGINEERING

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IoT, Cyber Security including Blockchain Technology)

19SB502 – CYBER FORENSIC AND INVESTIGATIONS

III YEAR/ V SEMESTER

UNIT 2 – EVIDENCE COLLECTION AND FORENSICS TOOLS

TOPIC 4 –Computer Forensics Tools(Hardware and Software Tools)

THANK YOU