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?

.....

- When you search for tools, keep in mind what file types you'll be analyzing.
- For example, if you need to analyze Microsoft Access databases, look for a product designed to read these files.
- If you're analyzing e-mail messages, look for a forensics tool capable of reading e-mail content.

Tasks Performed by Computer Forensics Tools

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