

CYBORTS

QAZI JAWAD ZAHEER

DIGITAL FORENSICS

TASK:1

What's digital forensics?

Digital forensics is the process of collecting, analyzing, and preserving data from electronic devices (like computers, phones, or USBs) to investigate crimes or security incidents.

What is the main goal of digital forensics?

The main goal is to find reliable digital evidence that helps explain what happened, how it happened, and who was involved—without changing the original data.

What tool is commonly used to create an image of a hard drive in digital forensics?

Tools like **FTK Imager**, **dd**, or **EnCase** are commonly used to create a bit-by-bit copy (called a disk image) of a hard drive for investigation.

Which storage devices can hold digital evidence?

Digital evidence can be found in devices like hard drives, SSDs, USB flash drives, memory cards, mobile phones, tablets, CDs/DVDs, and even cloud storage.

Why is it important not to modify the original evidence during a digital investigation?

If the original evidence is changed, it can no longer be trusted or used in court. Keeping it untouched ensures the data is authentic and can be verified later by others.