

1. Encase Forensic Tool

Encase Forensic Tool: EnCase Forensic Tool is a digital forensic software used for computer investigations and analysis. It allows investigators to collect, preserve, analyse, and present digital evidence in a court of law. Encase provides features such as disk imaging, file recovery, keyword searching, and timeline analysis to aid in investigations.

2. Digital Forensic and Incident Response (DFIR) Framework

Digital Forensic and Incident Response (DFIR) Framework: A Digital Forensic and Incident Response (DFIR) framework is a structured approach used by organizations to detect, respond to, and recover from cybersecurity incidents. It typically involves several phases, including preparation, identification, containment, eradication, recovery, and lessons learned. DFIR frameworks provide guidelines and procedures for handling incidents, preserving evidence, and mitigating the impact of security breaches. Popular DFIR frameworks include the SANS Incident Response Process and the NIST Computer Security Incident Handling Guide.