OnLine Digital Forensic Suite™

...next-generation software for investigations of live computers in enterprises

Incident Response – E-Discovery – Compliance

Respond Quickly to Computer Security Breaches
Examine Live Systems Rapidly With No Impact on Operations
Deploy Quickly, Manage Easily, No Agents to Pre-Install
Conduct Investigations from Anywhere

The OnLine Digital Forensic Suite™ (OnLineDFS™) from Cyber Security Technologies enables rapid, cost-effective examinations of live, running computer systems.

OnLineDFS is designed specifically for information technology security professionals in corporations, government agencies and law enforcement. It is a valuable tool for real-time incident response, non-disruptive compliance auditing, and cost-effective e-discovery.

OnLineDFS is simple to deploy and operate, adheres to digital forensics best practices, and provides an extensive array of tools for data acquisition, search and investigation. To ensure accurate, thorough record-keeping, OnLineDFS automates the logging and reporting of all investigative actions.

Rapid Response: Whether you are responding to a suspected break-in or an internal breach of organization policy, OnLineDFS enables you to conduct an investigation in real time.

Unobtrusive Examination: OnLineDFS enables the examination of computer systems quickly and inconspicuously, capturing relevant data — including running state — while the system being investigated continues to run.

On-Site or Remote Investigation: With OnLineDFS, the investigator can work on-site or from a remote location, saving travel time and expense.

Analyze Running Computer Systems
Investigate On-Line From Anywhere

- Examine a running computer live
  - Conduct investigations discreetly, without disrupting operations
  - Examine mission-critical systems without down time
- Capture and record volatile running state information of the target computer
  - Acquire vital information on running programs, network connections, data transmissions, memory and registry
  - Capture information that would be lost if the system were shut down
  - Gather information in context
  - Automatically examine selected systems on a scheduled basis
- Acquire static data selectively, focusing on information relevant to the investigation, from an individual file to entire drives

Key Benefits

- Deploy quickly, manage easily and inexpensively
  - No agents to pre-install and manage
- Focus investigations immediately
- Reduce investigation costs
- Act discreetly, unobtrusively, non-disruptively
- Perform real-time incident response
  - Immediately assess threat and risk
  - Take rapid corrective action
- Simplify and cost-reduce e-discovery information collection
- Meet compliance regulations and goals

Product Specifications and Features

Simple Set-up and Operation

- Only one OnLineDFS installation is needed to investigate all machines within a firewall
- No agents to be pre-installed on the target computers
- Up and running in minutes
- An OnLineDFS examination can be conducted on-site or via a secure Internet or other communications connection

Data Recording and Connectivity

- Acquired data may be recorded on the OnLineDFS system's internal hard disk or on external data storage devices for easy transport and isolation of evidence
- Investigators may access OnLineDFS remotely using a Web browser capable of secure (SSL) connections via HTTPS, such as Microsoft Internet Explorer 4.0 or higher, Mozilla Firefox, Mozilla Suite, or Netscape Navigator 4.0 or higher

Supported Target Platforms

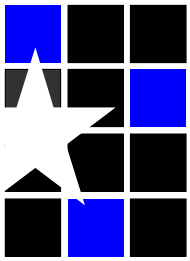
Microsoft Vista
Microsoft Windows XP Professional
Microsoft Windows 2000
Microsoft Windows NT 4.0 or higher
Microsoft Windows Server 2003
Popular versions of Unix and Linux

Supported OnLineDFS Platforms

Microsoft Vista
Microsoft Windows XP Professional

Key Features

- Real-time investigations of live systems
- Capture running state of target system
- Capture memory and registry
- Unobtrusive network application
- Remote control of application via Web browser and any communications link
- Extensive tools for data sorting and analysis
- Extensive search capabilities
- Scheduled data capture
- Multiple file viewing capabilities
- Data capture from single file to full disk mirroring
- Organized reporting in clear, structured formats to increase investigator productivity
- Structured, documented processes adhering to digital forensics best practices
- Verified authenticity via cryptographic hashing
- Automated log for detailed audit trail
- Consistent framework for investigations



Cyber Security Technologies

an affiliate of Architecture Technology Corporation

9977 Valley View Road * Suite 200 * Eden Prairie, MN 55344
Telephone: 952-937-6258 * Fax: 952-937-1998 * info@cyberstc.com * www.cyberstc.com