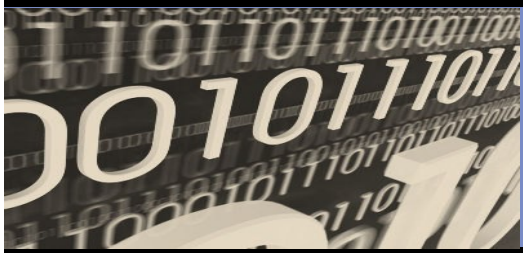
What is Digital Crime?

Digital Crime is any illegal activity involving an information technology infrastructure, including: unauthorized or illegal access, interception (by technical means of transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data).

Any of these breaches can occur from within or outside an organization. The immediate detection and interdiction of illegal activity is crucial. Data preservation and recovery are critical objectives in the fight against digital crime. Be sure to read the "Dos and Don'ts" area of our site so you'll know how to prevent further damage to a potentially compromised system.

Digital evidence relating to all types of crimes—can be located in many devices including cell phones, GPS, laptops, PC's and Servers. Types of crimes where digital evidence has been located:

Cyber-Threats, Cyber-Larceny – Frauds – Scams, Online Credit Card Fraud, Cyber-Identity Theft, Internet Counterfeit Products/Labels, Electronic Funds Trans. Fraud, Cyber-Harassment, Cyber-Theft of Trade Secrets, Computer Desktop Forgery, Cyber-Violations R/Orders, Cyber-Vandalism/Destruction, Electronic Counterfeiting, Cyber-Stalking, Cyber-Copyright Infringement, Online Auction Fraud, Prohibited Employee Conduct and more.



www.dcrime.com

Do's and Don'ts !

Safety, company integrity and business continuity are critical factors. Here are some important considerations:

- Do not allow access to the effected system until integrity is restored.
- Do not turn on or off any system until it is safe to do so.
- Do consider a network disconnect of the effected system based on continual risk factors.
- Do protect your data backups, physical off-site storage and cloud storage.
- Do make sure to consult with a technical expert who can properly advise you and forensically secure/preserve the scene as soon as it is safe to do so.
- Do consider calling law enforcement ASAP to report any attempted or actual data destruction, hacking, account take-overs or data/operational compromises to your network.

Every situation is unique and a specific approach and strategy should be on a case by case basis. We acknowledge the need for sensitivity and discretions with our investigations.

Digital Crime Examinations, LLC
Attn: John McLean
19 Grant Street
Woburn, MA 01801-5310 USA
1-781-983-6833
info@dcrime.com

www.dcrime.com

Computer Forensics

Data Recovery

Technology Consulting

Digital Crime Examinations

Making the Connection
781-983-6833

www.dcrime.com

www.dcrime.com

Digital Crime

Making the Connection

Who is DCrime ?

Digital **Crime** is a consortium of information technology experts, law enforcement professionals, trainers and educators, bringing decades of experience in data recovery, digital forensics, investigations, training, incident response and custom application development.

Our expertise in all aspects of information technology guarantees our clients comprehensive services for their corporate or private needs.

Our customers base include local and state government agencies, law firms, private investigators, financial and educational institutions and technology firms.

What is Computer Forensics ?

Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics.

The goal of computer forensics is to explain the current state of a digital artifact. The term digital artifact can include a computer system, a storage media (such as a hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image) or even a sequence of packets moving over a computer network.

The explanation can be as straightforward as what information is here? and as detailed as what is the sequence of events responsible for this current arrangement of bits?

What can Dcrime can do for you ?

There are many reasons to employ the techniques of computer forensics:

* In legal cases, computer forensic techniques are frequently used to analyze computer systems belonging to defendants (in criminal cases) or litigants (in civil cases).

* To recover data in the event of a hardware or software failure.

* To analyze a computer system after a break-in, for example, to determine how the attacker gained access and what the attacker did.

* To gather evidence against an employee that an organization wishes to terminate.

* To gain information about how computer systems work for the purpose of debugging, performance optimization, or reverse-engineering.

Special measures should be taken when conducting a forensic investigation if it is desired for the results to be used in a court of law. One of the most important measures is to assure that the evidence has been accurately collected and that there is a clear chain of custody from the scene of the crime to the investigator---and ultimately to the court.

Dcrime offers computer forensics, data examinations, data recovery and consulting services to large organizations, small businesses and individuals.

Making the Connection !