

DISCREET INVESTIGATIONS

RECOVER DESTROYED/  
DELETED INFORMATION

ANALYZE RECOVERED DATA

RECOVER & EXAMINE  
FORMATTED HARD DRIVES

ACCESS HIDDEN FILES

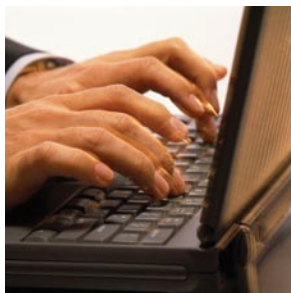
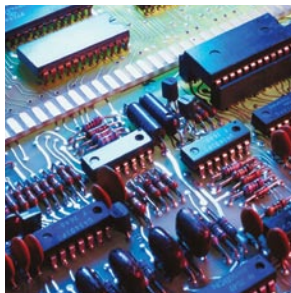
CRACK PASSWORD  
PROTECTED FILES

UNCOVER COMPUTER USAGE  
TIMELINES

DETERMINE INTERNET  
ACTIVITY

RECOVER TEXT MESSAGES

RECOVER E-MAILS



The rapid proliferation of technology and the increasing dependence on it for both personal and business use have vastly increased the accessibility and vulnerability of information. Add to this the growing portability of devices and it becomes clear that, more than ever before, companies are susceptible to theft and misuse of digital assets and product information that could compromise the integrity of their enterprise.

T&M's Data Forensics division responds to reactive and proactive situations in which evidence is required to conduct an internal investigation of suspected wrongdoing or to support litigation. Violations of employee policies, theft of intellectual property, claims of harassment and financial fraud have

**The proliferation of technology and the growing portability have increased the accessibility and vulnerability of information**

been uncovered through the use of data forensics. Using the most sophisticated, state-of-the-art technology, data is preserved and discreetly accessed or extracted using stringent best practices and in compliance with domestic and international data privacy laws. All data is held in the strictest confidence and proven data protection procedures ensure that the data is securely handled. Chain-of-custody logs and court-accepted processes ensure that the data and findings are admissible in court should the information recovered result in litigation.

### The Challenge:

- Discretely discover the facts surrounding suspected dishonesty
- Extract misused or compromised information stored on computers, servers, cell phones, memory sticks (flash/thumb drives) and company phone systems
- Understand what pages were accessed on the Internet
- Access 3rd party e-mail activity, chat logs, and blog postings made by employees
- Identify inappropriate or illegally stored electronic data on the network, a workstation, a cell phone or a portable device
- Ensure that data is securely handled and admissible as evidence in a court of law

### Benefits of T&M:

The use of data forensics can often confirm or negate the suspicion of wrongdoing and shed light on even the most sophisticated fraudulent events. T&M's team of experts, led by a nationally recognized industry expert, has significant experience conducting forensic examinations and providing written and oral testimony at time of trial. Data forensics can reveal hidden files, e-mail communications, text chat sessions and compromised information, even if the device has been formatted or the data has presumably been destroyed. Whatever the situation, T&M's Data Forensics division has the tools to uncover the data that can help understand the truth. In the end, data doesn't lie.



T&M maintains a state-of-the-art computer forensics facility housing the most advanced forensic tools for expert analysis of data recovered on electronic devices. Our three phase approach has been used in hundreds of investigations, including some highly publicized legal matters, in which computer data played a significant role. Our team of testifying experts possesses a wealth of technical and investigative knowledge specifically tailored to analyze computer data and produce findings in support of an investigation or legal action.

### **Phase 1 – Data Preservation and Collection**

Our team of experts starts by first understanding your technology landscape and identifying where potential evidence is likely to exist. With strict adherence to protocol, computer data is extracted from computers, cell phones, backup tapes, servers, and other devices. Using advanced tools and our exclusive process, data is quickly captured without ever modifying or altering the original. Data collection is often performed during the night to minimize any impact on operations and leaves no trace. This ensures that the matter remains completely confidential and does not alert the parties being investigated. During this phase, proper chain-of-custody documentation is maintained and the data is handled appropriately to protect its integrity.

### **Phase 2 – Data Analysis**

Once the data is uploaded to our secure evidence servers, it is analyzed using a comprehensive process that reveals all data on the device – including deleted, password protected, and encrypted files. The analysis may uncover 3rd party e-mail addresses, text logs, web sites visited, search history, and hidden files and folders. Using keywords and defined time frames, our forensic examiners quickly find results and reconstruct a time line of activity.

### **Phase 3 – Reporting**

Perhaps the most significant advantage of T&M's Data Forensics service is our ability to convey the findings in a meaningful and easily understood manner. Findings are delivered through oral or written reports, and our experts are available to help construct additional legal requests, or for oral and written court testimony.

- Discreet investigations of electronically stored information
- Proven experience in retrieving data in a court accepted manner
- Recovery of destroyed or deleted electronic data
- Recovery and examination of formatted hard drives
- Access to hidden electronic files
- Cracking password protected files
- Uncovering computer usage timelines
- Determining Web sites visited and internet activity
- Recovery of text messages and other communications
- Recovery of E-mail sent via third party services
- Determining theft of intellectual property



#### **Contact**

Paul G. Lewis  
Vice President  
Data Forensics  
Direct: 908.537.4000  
plewis@tmprotection.com