

Mobile Application Development



## Incidence Response and Digital Forensics

Securing its business information is critical for every organization. We almost on daily basis hear or read about high profile attacks on corporate and government web sites. Bank computers are broken every year and important account data and credit card data is stolen by criminals. Besides having business and financial impact resulting from these attacks - there are legal issues resulting from these attacks. You need a well qualified team of security professionals to safeguard your network, your data and your equipment. This is what we at Rapidsoft can do for you. At Rapidsoft Systems, we specialize in four main practice areas: Assessment, Managed Security, Remediation, and Response in order to appropriately secure your organization's most critical information.

### Dealing with Incidents and Digital Forensics

Incident response services deal with any known or suspected breach of your security. The main important goal is to detect the extent of the damage, take protective actions, collect and preserve evidence of criminal activities. A typical methodology for digital forensics which apply to Windows incidents as well as other OS platforms:

1. **Acquire the evidence without altering or damaging the original.**
2. **Authenticate that your recovered evidence is the same as the originally seized data.**
3. **Analyze the data without modifying it.**

### What Do you Need in a Incidence Response Plan

Every company needs to have an incident response plan in place - even if expert support is immediately available. Here is where Rapidsoft Systems can help you. Our experts will develop policies and procedures - and most importantly train the people on the front line of incident detection and response.

Rapidsoft Systems offers a whole new way to deal with incident response and forensics. Result of any forensic investigation is directly relevant to incident response. Incident Response, by definition, requires fast intervention which requires a use of framework for Security Information and Event Management (SIEM). The ability to detect a threat, notify a security professional, perform a detailed investigation of that threat, and take appropriate actions is perhaps the most necessary function of Incidence Response Team. The United States government defines the requirement for incident response as needing to be "timely" and "rapid"—with good reasons. Every minute between the detection and notification of an incident, and the successful exploitation or theft of a protected asset, costs a company money, exposure, and liability.

Our security experts are trained to deal with emergencies and can help in the following ways.

#### 1. Stop the Attack As Fast As You Can

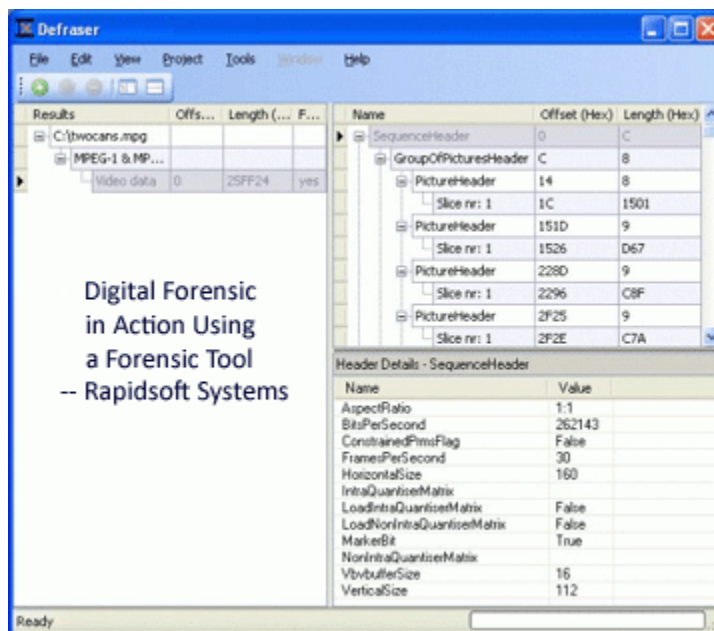
The first objective of incident response is to stop the attack. Whether it's internal or external, the attack can shut down your business, compromise confidential information, and erode the trust of your customers.

#### 2. Contain the Damage

Once the attack has been stopped, we focus on minimizing damage and improving the system to prevent future incidents. Speed and quality are essential. They often determine the ability of a business to recover and contain damage.

#### 3. Gather Forensic Evidence

We also investigate to determine the extent of the damage and gather evidence. Evidence is essential when credit card data or other confidential information has been compromised. It may also be part of legal or contractual requirements.



A Digital Forensic Testing in Progress

## Computer or Digital Forensics

The goal of computer forensics, also known as Digital forensics, is to explain the current state of a digital artifact. The term digital artifact can include a computer system, a storage medium (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 the present situation?"

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.

## Incident Response

In the unlikely event that an incident does occur, an efficient and organized response is required to minimize the impact and preserve evidence. Our Incident Response services include:

- Network/Firewall/Application breach emergency response
- Identification and cleansing of malicious code, malware, spyware, system file hacks
- Identification and manipulation of swap files, Temp files, file system, logs IDS, sniffers
- Support an organization's internal response team

## Forensics Support in Response to Incidence

We apply a best practice approach in searching for evidence by preserving the integrity of the source and authenticating and securing any evidence collected. Our Incident Handling services include:

- **Preliminary Investigation to locate data that is accessible, recoverable and relevant**
- **Data/Content Recovery in Functioning Media**
- **Data/Content Recovery in Non-Functioning Storage Devices**
- **Drive Sanitation to completely and safely remove data (performed off-site)**

## **Zero-Day Threats**

Real-time, operational forensics allows a security professional to perform ad-hoc correlation of data to detect, track, and remediate complex attacks as they occur—the ability to provide zero-day response to complex threats. That means the ability to use a security tool to see threats that haven't yet been defined within event correlation rules (of course, pre-defined rules exist as well, for automation of well-known attacks).

An expert at Rapidsoft Systems can answer all the above questions and help your company assess your risks and create an effective policy for your organization.

## **Why Rapidsoft Systems:**

With over 350+ software projects executed, you can simply count on our expertise, experience in giving you the right solution at absolutely lowest possible cost. If you would like more information, or want us to submit an estimate or a "no-obligation" quote for your project, contact us for more information.

## **Rapidsoft Systems, Inc,**

**(<http://www.rapidsoftsystems.com>)**

### **Offices and Project Centers:**

New York (USA), San Jose (USA), Singapore, New Delhi (India), Noida (India), Gurgaon, (India), Chennai (India), Mumbai (India)

**For General Enquiries:** [info@rapidsoftsystems.com](mailto:info@rapidsoftsystems.com)

Phones: 1-609-439-4775 (Sales Direct), 1-609-439-9060 (US East Coast, NJ Office)  
1-408-829-6284 (Sales Direct), 1-408-890-2509 (US West Coast, San Jose Office)

USA Office Central PBX: 1-609-356-5121 (Multiple Lines -Support Sales, Service and Admin)  
Fax: 1-831-855-9743