

# Remote Forensic Software

Gartner RAS Core Research Note G00171898, Jay Heiser, 4 November 2009, R3325 20110331

Remote forensic software tools can help meet demands for an increasing number of internal investigations of inappropriate or illegal activity, security intrusions, and document discovery. Corporate investigative staff and external investigators can use these products to efficiently and effectively collect legally admissible data from servers, workstations and laptops across the enterprise.

## Key Findings

- Forensic agents on the desktop can enable the investigation of workstations, even when the hard drive is encrypted.
- Remote investigation tools can dramatically reduce the need for travel, improving the efficiency and response time of corporate investigators.
- Traditional forensic data collection techniques that involve the physical collection of evidence are still appropriate for many investigations, but, in a growing number of cases, it is impractical or impossible to use them.
- A remote investigation is invisible to the subject, unlike a traditional investigation, which requires physical access to the workstation, which is likely to tip off subjects that they are being watched.

## Recommendations

- Multilocation organizations that are already conducting digital investigations should investigate the use of remote forensics.
- Do not start choosing software tools before investigative protocols and approval processes have been implemented and qualified staff are in place.
- Plan for – or even deploy – remote forensic agents before they are actually needed, working with IT administrators to ensure compatibility with network, security, encryption and administrative privileges.
- Before performing remote investigations across borders, management and the in-house counsel must ensure that the enterprise is aware of the privacy laws in all affected jurisdictions and has processes to ensure that they are followed.

## ANALYSIS

A type of investigative tool referred to as “remote forensics” or “enterprise forensics” provides a viable mechanism to overcome the complications of geographic separation and hard-drive encryption. These products use agent software on the workstation, allowing an authorized investigator to remotely search the contents of the hard drive, including deleted files and “slack space,” collecting evidence data from those workstations over the network in a legally defensible manner.

The use of this remote investigative technology is completely invisible to a user being investigated, functioning in the background as long as the user’s workstation is turned on and connected to the network. When the user is logged in and active at his or her workstation, the operating system will automatically decrypt the contents of the hard drive, making it accessible to any authorized process, including remote forensic agents.

There are times when a system or its data cannot be accessed. But overall, remote forensics are practical more often than traditional forensics that rely on physical access to the target system. It is even possible for forensic consultants located outside of the enterprise to conduct investigations through the firewall. Most importantly, in this sensitive legal context, the commercial remote forensic products have demonstrated the validity of network-based data collection, and evidence collected by these tools has been accepted by multiple courts of law in multiple jurisdictions.

Remote forensics should not be confused with network forensics. Network forensic tools use privileged access to the network to monitor activities at the packet level. Remote forensic tools use privileged access to a host to examine the contents of persistent storage and volatile memory. Although some of the same material might be gathered (in different ways), and, in many cases, both technologies could be usefully applied to capture complementary information, they represent two very different types of investigative technology.

Not every remotely enabled tool is equally suitable for all forms of investigation. The three primary forms of digital investigation follow somewhat different processes and seek to gather different kinds of information in different time frames.

### Traditional Investigation

Traditional forensic investigation techniques were developed by law enforcement agents to search PCs and collect information, including deleted or hidden information, that could aid in solving a crime. The need for evidence that is admissible in a court of law meant that digital forensic practice has always emphasized

robustness, accuracy and process documentation. These same techniques are increasingly used for internal corporate investigations that may not end up in a courtroom, but that could result in the dismissal of an employee for inappropriate behavior. The traditionally preferred form of primary evidence is an original hard drive, sealed in an evidence bag and stored in a locker after it has been forensically duplicated.

Sending trained staff out to collect hard drives is expensive, and it makes the target system unavailable for use.

As long as an agent with system privileges is installed on the target system, remote forensic tools are able to access and search the contents of all local storage devices. They also have the ability to capture the complete image of a hard drive, including the “slack space” that is not currently occupied by files. The practicality of imaging a drive over the network is dependent on bandwidth and the size of the drive.

However, a successful remote investigation is rarely dependent on capturing a complete disk image. Searching visible files, hidden files and slack space can be performed on the target system by the agent, dramatically reducing the amount of data that needs to be reviewed across the enterprise. Furthermore, the vendors of forensic software have successfully demonstrated in multiple courtrooms that their software can accurately extract a subset of the data from a live hard drive, while still defending the integrity of the result.

It is often desirable to conduct surveillance over a period of time, watching the subjects of an investigation to learn more about what they are doing and who they are communicating with, without the subjects being aware of it. If some form of disciplinary action, or even a criminal prosecution, is anticipated, the initial examination of a subject’s workstation might not yield sufficient evidence, another reason for conducting extended surveillance. Remote tools, which can operate on the desktop in a stealth mode so that their presence and activities are invisible to the user who is being investigated, are ideal, providing investigators with an ongoing surreptitious view of desktop activities.

### Security Incident Response

Incident response refers to the investigation of a compromised or hacked computer in order to determine what happened, and hopefully learn how the attack was conducted and who is behind it. This type of investigation is less concerned with the contents of data files, and more concerned about the state of the network and operating system.

A great deal of information is found in the network state tables, in the operating system tables and in the context of the currently logged-in user. Referred to as “volatile data,” because it is constantly changing, and will disappear entirely if a computer is shut down, it is of vital importance in analyzing an attack. Remote forensic tools designed to support incident response have mechanisms to quickly and reliably capture as much information about the current state of a computer as can feasibly be done. This data typically includes:

- Logged-on users
- Process tables (running processes and open files)
- Network connections and listening processes
- Memory
- Clipboard
- User command history

## E-Discovery

Electronic discovery is a form of investigation that locates business records dealing with specific topics and provides them for use in civil litigation. Increasingly, the files located on user workstations are being treated as records that must be produced in a discovery request. This puts a huge burden on the organization responsible for production, because not only are no mechanisms in place for retrieving such files, there are not even any mechanisms for finding them.

Several enterprise forensic products are proving very useful for enabling the methodical and documentable searching of a set of workstations for files that contain specific text, and retrieving that text in a well-documented and reliable fashion. Remote forensic products are typically used for the initial data collection, but the analysis and reporting tasks are usually performed with software specifically intended for e-discovery use.

## When Should You Consider Remote Forensics?

Remote forensics is rapidly becoming a standard investigative process for both internal corporate security departments and external consultants. It provides both cost-efficiencies and unique capabilities, and should be considered when:

- Your investigators (internal or external) are spending too much time (and money) traveling.
- You are hiring outside investigators for purely logistical reasons (e.g., it’s easier to pay someone from outside the organization than to use your own employee).
- Your organization has multiple locations that could benefit from a central digital analysis service to provide forensics, e-discovery and incident response.
- You need to conduct surveillance of employee activities over a period of time and collect legally admissible evidence.

## Available Products

Remote forensic products are available from most of the companies that provide traditional stand-alone forensic tools. The most widely used products, with the highest level of support internationally, are from Guidance Software (makers of EnCase), and AccessData (makers of Forensic Toolkit [FTK]). These products are often used by corporate investigative departments to support all three types of investigation.

Some of the vendors of full-drive encryption are working directly with these two providers of forensic software, ensuring compatibility. Other products suitable for multiple forms of investigation that have also proven themselves in courts of law include Technology Pathways’ ProDiscover, Paraben’s Enterprise Edition, SMART from ASR Data, and Cyber Security Technologies’ Online Digital Forensic Suite (OnLineDFS). BlackBag Technologies’ MacQuisition CF is a forensic product intended specifically for investigation of Macintosh systems.

The vendors of products that are intended primarily for capturing volatile data are less capable at doing search, and are not intended to search or capture large amounts of remote data. However, these vendors have been beefing up their ability to locate and analyze malware, including hacker tools, and provide more functionality for attack analysis than do the traditional forensic tools. Such products include Responder Pro from HBGary, Gargoyle Investigator Enterprise Module (GEM) from WetStone, and Mandiant First Response.

Although not a traditional forensic product, F-Response provides a useful functionality for remote investigations. It essentially allows the remote “mounting” of a target system’s storage and live memory, providing remote network enablement to other products. Although this arguably reduces the ability of a forensic product vendor to charge extra for an “enterprise license,” several of the traditional product vendors have decided it is advantageous to provide their customers with as many options as possible, so they are explicitly supporting F-Response.

## Best Practices

The choice of a forensic tool should never be the starting point for building an investigative capability. Organizations that have not yet begun doing their own digital forensic work should either hire consultants or build their own internal capability, starting with people, policies and process, before considering the purchase of specific tools. Knowing the capabilities of remote forensic tools, however, can help strengthen the business case for creation of an in-house digital analysis function. Multisite organizations that already have digital investigative capabilities in-house should consider whether their existing toolset is adequate, or if it can be improved through the acquisition of products that can support remote investigations.

Remote forensics can be used from outside the enterprise, which can provide huge cost savings on the time and travel billed by consultants and external forensic investigators. Like any form of sensitive remote access, external access to the corporate network should go through a VPN, and use the strongest form of authentication available.

For political and practical reasons, investigators should avoid installing remote forensic functionality before consulting with senior system administrators (these tools can often be used to investigate system administrator activity). Some of the best practices in preparing an enterprise for successful digital investigation, remote or traditional, include:

- Develop an overall plan or strategy for remote investigation that takes into account both the technical and policy issues.
- Investigators should work with the workstation administrators for the initial deployment and ongoing functionality. This ensures that the agent is installed with privileged access, and that there are no conflicts with security or encryption software.
- If a high number of remote investigations are anticipated, the agent software can be predeployed by making it part of the standard workstation build.
- Do not allow the use of nonstandard encryption on workstations. If encryption is needed for laptops (and it is generally needed), choose a corporate standard product and enforce a standard configuration. Ensure that authorized administrators have the ability to decrypt the drives on those workstations, so that routine maintenance, clear text backup, data recovery and remote investigations are possible.
- Institute a policy of retaining the hard drive of departing employees who are leaving especially sensitive jobs, or who are leaving under controversial circumstances.
- Before redeploying a PC or hard drive, use data-wiping mechanisms to completely remove all data.
- Develop an “investigative protocol” (process) specifying the types of investigations that will be performed by which people and under what circumstances. This policy and process document must be approved by the managers of the corporate, security, legal, IT and HR departments. This should be in place before performing investigations.

Remote forensic tools are being successfully used by organizations in multiple countries and, in many cases, between countries. The regulations affecting remote forensics vary between jurisdictions, and Gartner cannot provide a legal answer as to whether or not this is acceptable in a particular situation. Before performing any form of investigation that could potentially impact the privacy of individuals, including employees and contractors, work with the corporate counsel and HR to ensure that all relevant laws and corporate notification and ethical standards are followed.