



Data Forensic Services

Supporting the Computer Forensic Needs of Business

DATA CAPTURE & DISCOVERY

When your discovery process requires capturing data for future analysis, JANUS technical experts will make an exact duplicate of the storage media. This results in an exact image of what existed within the target computer, such as empty sectors, data that is flagged as deleted, and temporary storage, to name a few. Every last byte of what currently exists can be preserved for future analysis without worrying that it will be overwritten with new data or permanently erased.

JANUS experts can either go to the site where the data resides or it can be brought to JANUS' secure laboratory.

Mobile Forensics Platforms . . . On-location, JANUS consultants can work through an entire site or in any portion of it – connecting our traveling forensics platforms to the targeted media and carefully reproducing an exact duplicate of whatever exists on that medium.

JANUS Secure Laboratories . . . JANUS maintains secure laboratories for evidence storage and forensics processing. Each of these fulfills the requirements for Department of Defense secret level information handling.

With JANUS you can rest assured that:

- The target machine will not be booted from the computer in question, thereby ensuring that no modifications will be made to the data.
- No alterations will be made to the operating system.
- All aspects of the original data will be preserved.
- No modifications will be made.

DATA RECOVERY

JANUS experts will utilize proprietary tools to attempt to recover data that you need. In many cases we can reconstruct damaged, deleted, reformatted, and erased files and directories and produce the resulting data for you. JANUS' techniques can also usually recover password protected or encrypted data.

This process is typically undertaken in the JANUS laboratory where our staff can work with a vast array of tools and techniques geared to carefully recover *all* the information that exists on the media in question and present it in a variety of formats, depending on your needs.

ANALYSIS

Analysis can begin from the first moment that we appear on a case. Counsel may need to determine what the possibilities are in structuring a production request.

JANUS staff can collaborate with the legal team, determining the 'sense' of the case, providing direction and/or support on how to structure the computer discovery tasks. Upon receiving production, we can assist in analyzing the documentation, utilizing our computer backgrounds to pinpoint additional discovery points that will provide fruitful information. This is a reiterative process in most computerized discovery situations and in each your JANUS technical partner will work through the technical aspects to provide existing pertinent information.

Evidence analysis can be a very tricky business. JANUS staff always duplicates the medium before beginning any analytical process. Even then, unless the defendant is cooperative and provides the names and versions of programs used, we must recover and then reconstruct the data only on a duplicate medium using JANUS proprietary tools so that we can format the data into easily readable documents for legal staff. Original capture media must be protected so that it retains its original structure.

FORENSIC PROTOCOL

Chain of custody procedures are maintained throughout the discovery process. JANUS staff are knowledgeable of and careful to maintain the integrity of the data at all times. Evidence is locked in a JANUS laboratory where it can be secured from unauthorized individuals.

NEUTRAL PARTY SERVICES

JANUS can perform services as a neutral agent of the parties when both agree. Often, acting as an agent of the Court, or as agreed to by the involved groups, JANUS will capture, recover, and filter the data in question.

Working with the attorneys or the Court, JANUS can utilize its proprietary techniques to find pertinent data and provide only non-privileged for discovery. This information can be provided in the manner required, to the Court, to each party, or to one party, according to the agreed upon disposition.

OTHER BUSINESS CONSIDERATION....

While the technology, techniques, and tools of computer forensics are similar in any environment, application of the forensics concept as an internal methodology for business requires more than technical skills and an understanding of the law. It requires **business savvy**.

For example . . .

While a court has the legal wherewithal to *order* an interruption of business operations for the purpose of evidence gathering or seizure, top executives in commercial ventures are generally unwilling to interrupt their own operations for such investigations.

Yet because the very equipment which drives most business today - computer equipment - is involved, is it possible to conduct such an investigation *without* such interruption? And, what other issues must be considered?

When businesses initiate their own computer forensics investigations, many factors come into play. Tough questions (and the right ones) must be asked, and answered - sometimes in very short time frames and under the pressure of a real-time security breach. Questions such as these:

- Do the benefits of and investigation outweigh the potential of loss?
- What action should be taken as a result of the findings? Prosecution? Personnel Action?
- If action is to be taken, has the right evidence been gathered in the right way, so as to support that action and can be upheld in court?
- Should law enforcement be brought in? Which agency? When?
- What about maintaining customer confidence?
- What if the media finds out? How should they be handled?
- What technology tools are required?
- What methods should be employed?
- What data should be recovered? When? Where? How?
- How do you avoid contamination of the evidence?
- What *is* evidence?

THE TECHNICAL SIDE OF FORENSICS

Examples of Areas Addressed Through Computer Forensics

- Modifications of the operating system
- Password recovery regarding encrypted files
- Identification of compressed files from header information
- Restoration of erased files through cluster chaining
- Identification of hidden Data Storage Areas
- Operation of dual function programs tied to security issues
- Use of automated fuzzy logic utilities to locate evidence
- Documentation of computer evidence processing

JANUS Will Help You With . . .

- Preservation of evidence
- Trojan horse programs
- File slack
- Revealing data hiding techniques
- E-commerce investigations
- Text search techniques
- Fuzzy logic tools used to identify unknown text
- Matching a diskette to a computer
- Identifying and detecting Internet abuse
- Boot process and memory programs

Examples of Tools Used to Accomplish the Above

- Program that validates the contents of one or more files
- Hard disk drive scrub utility used to eliminate all data
- Program that validates mirror image backup accuracy
- Disk catalog tool used to evaluate computer use time lines
- Intelligent fuzzy logic filter for use with ambient data
- Ambient data collection tool used to capture unallocated data
- Ambient data collection tool used to capture file slack
- Program used to document the CMOS systems time and date
- Forensic internet analysis software used to identify abuses
- Ambient data security scrubbing utility
- Documentation program for use in recording file dates, times and attributes
- Documentation program for use in recording file dates, times and attributes
- Program used to analyze the output of file list
- Text search utility used to locate key strings of text and graphic file

Summation

There are a multitude of issues to consider when thinking in terms of a data forensics project. Choosing the right partner can mean the difference between a successful project that allows you to accomplish your goals or possible failure in your efforts. Janus has the methodologies, personnel and experience that ensure your success in data recovery and analysis. Please feel free to contact us to discuss your Data Forensics needs.

JANUS is a certified, woman-owned small business. Please call our Data Forensics Group at 203-251-0200 to learn how your organization would benefit from our information security services.

JANUS Associates, Inc. 9 West Broad Street Stamford, CT 06902

www.janusassociates.com