

Computer Forensics: The Six Steps

Adrian T.N. Palmer

Managing Director, Kroll Ontrack Computer Forensics

Computer-based information is a key source of evidence in an increasing number of investigations and legal matters. This trend is not surprising as the proportion of corporate communication created electronically is now over ninety-three percent. This increase in creating and using electronic documents now means that computers are quickly becoming a critical point of investigation for any company that needs to locate information about its business activity. As such, computer systems, be they one hard drive or a network of servers, are now routinely identified as the best place to begin collecting potential evidence.

The types of investigations which centre on computer-based evidence are numerous and varied, from the personal to the political, fraud to theft. A growing number of these cases have highlighted the need for comprehensive computer forensic analysis in investigations that incorporate electronic data. Organisations need to make sure that the electronic evidence they collect is done in a manner which does not threaten the integrity of their data while also accurately identifying the *what, where, how* and *whom* of the computer-related behaviour.

There are typically six stages in a computer forensic investigation:

Consultancy

The most effective place to begin a computer forensic investigation is to consult with client/expert to create a strategy for collecting, analysing and processing the data. This strategy may include analysis of where the critical information resides, as well as the identification of protocols that will ensure the admissibility of the data into evidence in a court of law, should it become necessary.

Before any hard drive exploration begins, protocol dictates that forensic experts identify where key evidence is likely to be located and piece together user and system information in order to obtain a comprehensive and thorough account of the technological landscape. This first step in the computer examination is, therefore, to understand where data resides, what conduct is at issue, what the aim of the investigation is and what output is sought.

Data Preservation

Electronic evidence, like other types of evidence, is fragile. Entering data, loading software, performing routine system maintenance or simply booting a computer can destroy certain files or metadata (key facts about the data, such as its creation or last modified dates) that is stored on the hard drive. A computer forensic expert should ensure that:

- Potential evidence is not damaged
- Computer viruses are not introduced
- Extracted data is protected from mechanical or electromagnetic damage
- A proper chain of custody is maintained throughout the process

Failure to adhere to strict industry standards regarding data preservation will not only result in the loss of critical data but may impinge the credibility of any data that is recovered, potentially rendering it unreliable or inadmissible in a court of law.

Data Collection

Once the location of the relevant data is identified, it must be retrieved. Computer forensic experts can retrieve data from virtually all storage and operating systems, including many antiquated systems. Using proprietary tools, experts can collect a wide range of data and can:

- Retrieve data from seemingly inaccessible media
- Access active data on the media
- Recover deleted data and/or deleted email

- Access inactive and unused data storage areas of various computer media and retrieve potentially important text
- Access password protected and encrypted files
- Gather information from databases, contact managers, electronic calendars and other proprietary software

Regardless of how the data is collected, a copy of all media (computer hard drives, servers, disks, tapes, etc.) must be made using appropriate and usually proprietary imaging software. This imaging process provides the client and computer forensic investigators with a “snap-shot” or mirror image of the data contained on the media. The “snap shot” is a perfect sector-by-sector copy of the drive, including all of the unused and partially overwritten spaces, the nooks and crannies where important evidence may reside.

The imaging process is non-destructive to the data and does not require the operating system to be “booted”, which ensures that the system is not altered in any way during the imaging process, thus preserving its evidentiary value. It is not commonly understood that the mere act of booting a computer will damage critical evidence and may change metadata, such as create dates or modified dates associated with particular files. Also, booting the system may cause the hard drive to be reconfigured in a way that overwrites data that would have remained more accessible if the “boot” did not occur.

Often, the data collection can be completed during non-business hours so that business operations are affected only for a limited time (if affected at all) during the imaging process, or so that the target of an investigation is not even aware that the imaging process has occurred. After this is complete, the computer forensic analysis begins. This must be performed on a copy of the system, hard drive, etc. to ensure that the original data is kept intact.

Data Recovery

The data recovery process is an important stage of forensic analysis. This stage reveals the mass of evidence which can then be “mined” for documents and data relevant to the investigation or case. Several classes of information can be recovered through this process. The categories include:

- **Active Data:** This term describes the original accessible data from the hard drive or tape. This is the data that was accessible to the particular user working with the computer.
- **Recovered:** This term refers to files and directories that were recovered after being deleted from the Active Data. Some of the files are recovered completely and are easily identifiable. Other files can just be in bits and pieces which then require expert analysis to try to put the puzzle back together.
- **Unused:** This term describes the “free space” or unallocated portion of the hard drive. It will contain two types of files, both of which essentially comprise the portions of the drive that are either: (1) free and open because they have never been used, or (2) free because the information contained there has been deleted, and the computer has marked that space as available for new information.

The possible results of the data recovery stage are endless. In some instances, recovery of the “smoking gun” email can transform a contentious legal battle into settlement discussions.

Computer Forensic Analysis

Beyond just retrieving files, forensic investigators often can determine whether computer evidence was tampered with, altered, damaged or removed. They can examine hidden information associated with recovered files (including deleted data or data from inactive or unused storage areas on the media) and provide a historical ledger of the content contained in the files. In essence, they can reveal evidence of the conduct of those people who had access to the drive. Computer forensic engineering analysis can include:

- Recreating a specific chain of events or user activity, including internet activity and email communication
- Searching for key words and key dates
- Searching for copies of previous document drafts
- Authenticating data files and the date and time stamps of those files

- Comparing and contrasting computer code to determine whether a particular program is original or copied from a similar program
- Advising on what evidence is likely to be found on the computer media and identifying the most effective set of data to search

Expert Reports & Testimony

Once the data analysis is complete, computer forensic investigators can help support the client's court case by:

- Customising reports about the data collected and produced to support the case
- Providing data for affidavits or other pleadings
- Providing expert testimony and reports

The value of such expert testimony was revealed in a recent computer forensics case where the Defendant, a network administrator, planted a computer "time bomb" in the central file server of his employer's computer network. The program was "detonated" after he was fired. The "time bomb" resulted in the complete destruction of his employer's manufacturing programmes, paralysing the company and ultimately resulting in the loss of more than 80 jobs. In this case, forensic investigators performed detailed and complex forensic analysis on the company's computer system and on back up tapes located at the Defendant's residence. The experts then testified at the criminal trial that the "purge" of the company's files was intentional, and that only someone with supervisory-level access to the network could have accomplished such a feat.

Customised reports, expert affidavits and testimony complement the forensic process and outcome. These services should be offered from the initial stages of the investigation to ensure the correct protocols are followed from the start. As such, considerations such as these should naturally be included in the consulting phase.

As computers continue to become commonplace in today's electronic working environment, computer forensic evidence is becoming a vital part of investigations and legal matters. In assembling the computer forensic puzzle pieces, it is vital that forensic professionals identify a strategy for the investigation, ensure data preservation, collection and recovery, and generate the forensic analysis, testimony and reporting. Following the above procedures will ensure that no electronic pieces of the evidence puzzle are left out when building your case or completing your investigation.

ⁱ 93% of business documents are now created electronically. Crane, Kevin, Designing a Document Strategy, McGrew & McDaniel Group, Inc. (2000).

This document is neither designed nor intended to provide legal or other professional advice but is intended merely to be a starting point for research and information on the subject of electronic evidence. While every attempt has been made to ensure accuracy of this information, no responsibility can be accepted for errors or omissions. Recipients of information or services provided by Kroll Ontrack shall maintain full, professional, and direct responsibility to their clients for any information or services rendered by Kroll Ontrack.