

Computer Counter-Forensics

The last decade has seen meteoric rise in the use of computer and network connections, with almost no aspect of everyday life escaping reliance on digital communications. The cost of computing devices has dropped sharply in recent years, spurring even greater demand. The information age has allowed old crime to be effected in new and devastating ways (e.g. advanced fee fraud), as well as paving the way for new offences such as computer misuse (e.g. Hacking) and telecommunication fraud.

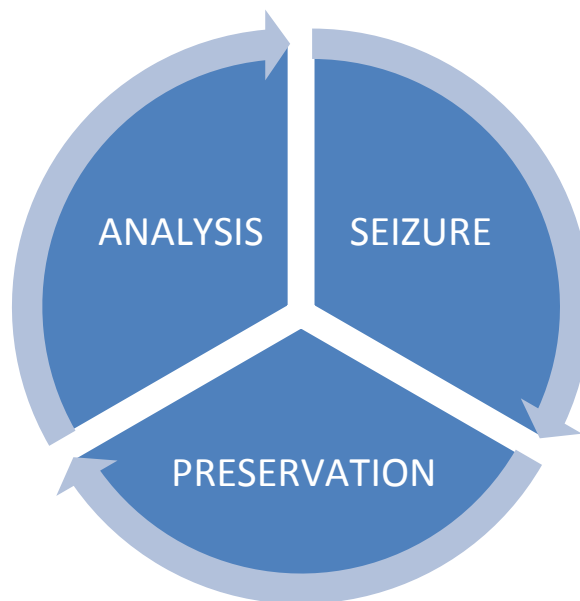
The past few years have seen an increase in criminals taking steps – sometimes very sophisticated measures – to thwart the efforts of computer crime investigators and the authorities.

Digital Evidence Triad

The fragile nature of digital evidence, coupled with the complexity and skill required to conduct an assessment that will bear the scrutiny of a court of law, makes it important to independently validate and verify the findings of the forensic assessor.

Case preparations involving scientific evidence must consider three core areas in detail, exploring each facet of evidence to assess whether Best Practice and prevailing regulations have been adhered to. This also ensures a full appreciation of the available digital evidence, which can be placed into the context of the allegations and accompanying physical evidence. These three spheres are illustrated in Figure 1A.

Figure 1A - Forensic Triad



- Search & Seizure

The means by which the target media (e.g. hard disks and CD's found on the suspect or at a specific location) were acquired by law enforcement agents and their subsequent preservation through the 'chain of custody'.

- Preservation of Evidence

Containment and protection of evidence exhibits so as to ensure fragile and volatile digital evidence is neither corrupted nor tainted.

- Forensic Assessment & Analysis

Evaluation of media and raw materials to furnish law enforcement agents with forensically sound evidence that can be presented in a court of law.

Efforts geared towards thwarting or impacting on the forensic computing process are levelled at one or more of these spheres.

Physical Safeguards

In the context of countering digital forensic practices, physical security is based on the principle that if a computer system cannot be found, then it cannot be seized by the authorities for examination.

Locked cabinets and steel laptop cables will frustrate efforts to remove devices from the suspect's premises; however, they will be defeated given adequate time and resources. More advanced approaches towards protecting computing devices include concealing key computer drives or media under the floorboards, in the loft space or in out-house facilities such as a garage. This can afford a degree of security and ensure that devices remain hidden from investigators. Communication with the device can be achieved without tell-tale cabling, relying instead upon encrypted wireless signals.

Anti-tamper devices, such as specialist alarm units that reside within computer casing, can be used to upset and hinder the search and seizure process. More complex approaches towards asset protection can include integrated 'anti-seizure' devices that are attached to the computer drive. These are designed to corrupt the computer drive data should any attempt be made to remove the disk or access the system without the use of a special hardware token and password.

File & Application Security

Investigators will naturally gravitate towards files and folders that appear to have titles of relevance to the case in hand. Perhaps the simplest approach to concealing files or folders is to rename them to something innocuous and unlikely to arouse suspicion.

A more considered approach to hiding information involves the moving of user data, such as textual reports or financial spreadsheets, into archives which normally contain only files required by the computer for operation (e.g. the system32 or config folders).

Both of these approaches help conceal information from the curious or casual browser, but the material will undoubtedly be uncovered during the course of a comprehensive forensic evaluation of the computer drive.

A different approach involves changing the way in which the computer operating system interprets files. Microsoft Windows™, the most prevalent desktop computing environment, identifies files and the program that should be used when they are being opened by the extension associated with the filename. Extensions take the form of a full stop and three letters appended to a filename – for instance the popular .doc extension that indicates a Microsoft Word™ document.

A somewhat crude but nonetheless effective approach to obscuring information is to change the associated file extensions. This could make a Word document (.doc extension) to appear as a bitmap graphic (.bmp extension). If a user attempts to open the file, the default program associated with the file-type, Microsoft Paint™ in this instance, will be invoked. Since the file data is actually in Microsoft Word format, Microsoft Paint will not be able to render the information and will return an error.

Such efforts are likely to help sensitive materials pass under the nose of casual observers¹ and those intent on identifying files of a particular type, such as graphical images which feature the extensions including .bmp or .jpeg.

A more conventional approach towards protection of information is to employ passwords. Starting with Microsoft Office 95, it became possible to password protect office productivity files to prevent unauthorised access². Well equipped forensic laboratories have specialist equipment to allow dictionary and brute-force attacks (trying all possible character combinations) against password protected files and programs, so unless a particularly complex pass-phrase is used the security is likely to be broken fairly quickly.

Most users employ passwords based on words found in the English dictionary or words that have meaning to them, such as the name of their wife or pet. These passwords are not complex enough to thwart concerted efforts to break the security. Passwords based upon non-English words, greater than eight characters in length and using both numbers and non-alphanumeric characters (e.g. exclamation or punctuation marks) provide a level of complexity that is extremely difficult to break.

1 More advanced forensic techniques comprehensively consider the composite code of a specific file and as such as would identify the actual data structure and content.

2 The security mechanisms employed in Microsoft Office applications versions 95 through 97 are considered fairly weak and passwords can be broken almost instantly.

3 Roman Emperor Julius Caesar (100-44 BC) is credited with designing and employing a cipher system involving the substitution of alphabet letters. To this day, simple substitutions ciphers are often referred to as 'Caesar Ciphers'.

4 For a discussion on Cookies, Temporary Internet Files and the Index.dat archive, please refer to article 'Internet History', part of the AFENTIS 5 Minute Forensic series.

5 Onion Routing Publications – Reference: <http://www.onion-router.net/Publications.html>

6 Trojan Defence Acquits British Teenager. Reference:
<http://news.zdnet.co.uk/internet/security/0,39020375,39117209,00.htm>

7 R v Fellows and R v Arnold (CACD Sep 1996)

8 R v Porter (Warwick Ross) [2006] EWCA Crim 560

9 Regulation of Investigatory Powers Act 2000. Reference:
www.opsi.gov.uk/acts/acts2000/20000023.htm

However, password protection can have serious shortcomings that can be exploited by forensic investigators. Protection of this type usually places a barrier up at the beginning of the file, which means if this safeguard can be by-passed, the actual data contained within can be extracted. A classic example is a forensic examiner using a plain text editor, such as Notepad, to open a password protected document. All controls, safeguards and features that may be in place through Microsoft Word are thus circumvented.

Taking file and application level protection to the next level is the practice of cryptography - the science of securing information through the use of reversible transformations. The word "cryptography" has its roots in the greek terms "cryptos", meaning secret, and "graphy", meaning writing. Simple ciphers, known as mono-alphabetic or Caesar systems, involve the substitution of letters³. The development of digital computing revolutionized cryptography and made today's highly complex and secure cryptographic systems possible.

With the introduction of Microsoft Windows XP™ an enhanced security feature known as Encrypting File System (EFS) has become readily available to desktop computer users. EFS is a cryptographic support system that enables files, folders and even sections of the hard disk file system to be encrypted using a variant of the Data Encryption Standard (DES) algorithm.

Attacking cryptographic materials is known as cryptanalysis and requires highly experienced consultants for any reasonable chance of success. Attacks can be levelled against the protocol (i.e. the mechanics of the encryption system employed), the protected file/data, or the interface and environment (i.e. the manner in which the user has interacted with the cryptosystem and/or computer system to create the secured material).

A more complex approach to concealing information involves placing it within or around another open and public source, a practice known as steganography. Classic examples of stego' include invisible inks or the use of grilles to cover a written message and reveal only selected words or phrases. In a digital context, steganography involves embedding the code that constitutes one file, for instance a graphical image, into the code structure of a secondary file.

The use of steganography can be difficult to detect even with the benefit of specialist forensic tools and when employed correctly can allow suspect material to evade even the most astute investigator. When combined with cryptography, steganography can be an especially powerful means of safeguarding both the presence and content of information.

Another approach to concealing information is to embed data in special sections of the file system structure. Alternative Data Streams (ADS) was a design feature introduced into the Microsoft Windows™ operating system with the NTFS™ file system as a means to provide compatibility with the Macintosh Hierarchical File System™ (HFS).

The way the Macintosh's file system works is it uses both data and resource forks to store its contents. The data fork is for the contents of the document while the resource fork is to identify file type and other pertinent details. There has been a marked increase in the use of these streams by malicious hackers wanting to store their files once they have compromised a computer. Not only that, it has also been seen that viruses and other types of malware are being placed there as well. The crux of the matter is that these streams will not be revealed using normal viewing methods, whether via a command prompt or using the Windows Explorer.

Whilst data embedded within ADS will remain invisible during all normal operations, forensic examiners can identify such material using complex data analysis tools. When information is encrypted, embedded within other file code (steganography), and finally hidden in an ADS, it is likely that the material will be safe from even the most astute investigators.

Internet Privacy

The Internet is an essential tool for business and leisure but is also a compelling resource for those commissioning or researching criminal activities.

Reading email or browsing the World Wide Web (WWW) leaves traces on the host computer that can be recovered by forensic investigators to give an indication as to website visited, terms used on search engines and conversations held in online chat-rooms⁴.

Whilst popular browser applications such as Internet Explorer and Mozilla feature routines to remove personally identifiable information, a more considered approach to eliminating any local traces of online activity would involve the use of a specialist application such as 'Evidence Eliminator'.

To add a layer of security between the computer and Internet, and thus protect against any potential eavesdropping on the telephone/broadband network, an approach known as Onion Routing may be employed. Developed by American researchers⁵, Onion Routing employs a complex series of relays, routers and encryption protocols to ensure anonymity and confidentiality of traffic.

Whilst investigators without the capacity or capability to undertake complex cryptographic evaluations may be at a loss to identify the content of such protected internet content, it may be possible to glean useful information through the use of 'traffic analysis'. Here the intention is to identify patterns and norms. For instance, it may not be possible to determine what website an individual is accessing, but through cataloguing the traffic it can be possible to say, with certainty, when a user was online. Should this be backed up with physical surveillance that can attest the individual was alone at the premises under observation at a particular point in time, then should further evidence come to light at a later point (perhaps as a result of performing a forensic analysis of the suspect's computer, following a search/seizure order), it can neatly tie the suspect to the computer keyboard.

Exploiting Forensic Methodology

Whilst the approaches previously discussed have focussed on obscuring or concealing either the physical computer devices or the digital evidence contained therein, the following techniques are geared towards thwarting the forensic process of examination of digital media.

Operations upon files and folders are recorded in timestamps, which provide details as to when the file/folder was created, when it was last accessed, and when the file/folder was last modified. Timestamp data is recorded automatically by the operating system and provides crucial evidence as to actions and times/dates when they occurred. However, appreciating how valuable timestamp data can be to investigators, tools have been created by various Hacking groups to allow manual or

automatic modification of timestamps. This technique is known as “fuzzing” and can make attribution of the file – or who was at the keyboard at a specific point in time – near impossible. Furthermore, fuzzing taints the evidence so that the integrity of the timestamps is damaged to a degree that would make them inadmissible in a court of law.

ACPO Guidelines for the seizure of computer devices, suggest immediate disconnection of the power unit, so as to preserve information on the system computer drive(s). This is regarded as Standard Operating Procedure (SOP) by investigators around the world, but it does have one very serious shortcoming. By disconnecting the power, any information stored within the volatile memory (e.g. RAM) will automatically be lost and cannot be retrieved. Hacking tools have evolved to take advantage of this investigative procedure; having scripts and applications that run exclusively in memory so that no traces will survive on the disk should the computer be seized by the authorities. It is considered to be only a matter of time before this counter-forensics technique becomes even more widely adopted by those intent on using computers for the commission or support of criminal enterprise.

Legal Context

Whilst not a security technique or forensic safeguard, some criminals have shown remarkable forward planning as a precaution if they one day have to stand trial for an offence.

In legal circles there have been a number of high profile cases involving computer abuse/misuse, where the line of defence has been that the computing device had been under the control of an unknown third party. In many cases the assertion is the computer has been broken into by a Hacker, who used the device as a platform for perpetrating their crime. This has become known as the ‘Trojan defence’ and was applied successfully in the matter of R v Aaron Caffrey, who was charged with breaking into computer systems owned by the American port authority in Houston⁶. It has been known for criminals to purposefully infect their computers with viruses and malicious code, laying the foundations for just such a defence should the need ever arise.

The technical arguments as to whether computer code, which is what essentially all digital media is, can constitute obscene media have long been agreed in the rulings of R v Fellows and R v Arnold⁷. In matters involving obscene images and media, the recent ruling in R v. Porter⁸ has put flesh on the bones of the argument as to what constitutes ‘possession’ in a technical sense. In this case the presiding Judge gave directions as to whether the jury could consider that deleted images, recoverable only using advanced forensic means, could still be considered in the possession of the owner.

Recently the Home Office announced plans to begin enforcing provisions outlined in Part 3 of the ‘Regulation of Investigatory Powers Act’⁹ (RIPA). The wording of this act would make it an offence for an individual or entity to refuse or be unable to disclose passwords or encryption keys specifically requested by the authorities in relation to an investigation. One argument against these provisions

is that it reverses the burden of proof and makes a party guilty of an offence should they be in a legitimate position to be unable to comply with a disclosure order.

One of the main criticisms of the act, however, is whether or not it will have the desired effect in enabling criminals abusing or leveraging technology to suitably punished. The oft-quoted example is that of an individual arrested on suspicion of possessing obscene images and media. Should the computer drive be strongly encrypted, the authorities may attempt to coerce the decryption keys via RIPA. However, it would clearly not be in the individual's best interests to comply as this would reveal the extent of their cache and almost certainly result in a punishment that would far outweigh that which would be on the table as punishment for non-compliance with the RIPA provisions.

Security vs. Accessibility

When considering security controls and countermeasures a careful balance must always be achieved, as to how to maintain reasonable accessibility to the data whilst ensuring confidentiality.

A collection of obscene images could, for instance, be grouped into one archive that is strongly encrypted and the resulting code embedded into the file structure of an innocuous file that is in turn buried deep within the computer's file system. This computer drive may then be concealed within the loft crawl space and communications with the device achieved using encrypted wireless protocols. Clearly this would afford a good degree of secrecy to the material, but does make it increasingly difficult to access or retrieve for any practical purposes.

The accessibility angle is used to the advantage of investigators, who will routinely scan suspect premises for wireless communication signals or follow computer data or power cables to identify any hidden devices.

Summary

Criminals and those engaging in offences involving the use or support of information technology continue to use various means to thwart the efforts of investigators to secure digital evidence. Whilst countermeasures range from the crude yet novel (e.g. burying devices under the floorboards) to the highly sophisticated (e.g. encrypting information and concealing the code within redundant areas of the computer file system) – it is clear that defensive practices of this nature are becoming increasingly prevalent. Equally, these efforts are becoming worryingly effective in hindering the efforts of law enforcement.

History has taught us that attacks against systems – whether physical or digital in nature – only increase in efficiency and effectiveness over time.

This article is not a 'how-to' guide and certain details from both the defensive and offensive perspectives have been intentionally omitted. The techniques described in this article are documented in a variety of public resources and in many instances employed quite regularly by criminals abusing or misusing technology.

It is considered more harmful to the forensic industry to operate under a veil of security and operate with a false sense that the practices employed are above reproach.

It is hoped that by highlighted this disturbing trend some of the challenges and limitations of current forensic computing practice can be appreciated. Furthermore, this can stimulate informed discussions that will lay the foundations for research into fresh approaches for countering counter-forensic practices.

Sam Patel is Head of VHCC Legal Accounts at the European digital evidence consultancy firm AFENTIS - specialists in complex crime and corporate offences involving the abuse/misuse of computers or telecommunication devices.

Expert features covering a variety of forensic computing disciplines – from recovering deleted text messages through to understanding the evolution of computer and information systems & network based crime - are available at www.afentis.com/forensic