

NOTICEBORED

Probing and investigating information security awareness

Issue 74

Digital forensics

July 2009

Editorial

Forensic computer analysis has strong parallels with the Turing test. You examine information from a computer system, and then you try to draw conclusions from that information.

Dan Farmer & Wietse Venema, [Forensic Discovery](#)

Many of us have watched television programs about detectives, forensic scientists and spies hunting criminals using clues left at the crime scene. In TV-land, investigators are able to obtain highly incriminating evidence from offenders' computers, PDAs *etc.* simply by attaching their special machines that go ping. As each data item is sucked out of the device, the system invariably clicks or beeps as a stream of colourful characters swirls across the TV screen. Even better, encrypted data are decrypted before our very eyes after the system mysteriously cracks the password one character at a time, just in the nick of time to defuse the bomb! Magic! Sheer nonsense of course.

Unfortunately, the reality is far more arcane. Forensic investigation of computers, cellphones, PDAs, USB memory sticks *etc.* obtained from the scene of crime is a tedious, painstaking process involving the systematic collection, storage, examination, analysis and interpretation of the data they contain. Anyone who has sat patiently through the process of a taking a "bit copy" of a hard drive will surely appreciate why TV programs necessarily gloss over the details, but that's precisely what forensic investigators must not do, many times over. The saying goes "the devil's in the details" – well in digital forensics, those little details and discrepancies often make or break the case. ■

Gary Hinson, NoticeBored Editor

Background

Digital forensics, the capture and analysis of digital evidence for presentation in court, is an increasingly important topic not just for law enforcement but for ordinary organizations and even individuals. Given a finite number of highly trained and trustworthy forensic investigators able to conduct digital forensic investigations competently, the police are fully stretched to keep up with the wave of electronic/online crime. Investigators working for large organizations often complain that the police will only take on computer frauds and similar cases if they are provided with all the necessary evidence, all neatly bagged and ready to go to court.

Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums ["media" – ed.]. Computer forensics is also known as *digital forensics*. The goal of computer 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?"

[Wikipedia](#)

Awareness of the procedures and issues involved in digital or computer forensics might interest people enough to take up the challenge and complete the training, or at least give them the basic knowledge to be able to select and/or work with digital forensic services from third party specialists or indeed the police and forensic science units.

Risks associated with/arising from digital forensics

Threats

Real world criminals don't come quietly, in the main. They evade arrest and do their best to cover their tracks. The same basic principles apply in the virtual world of online criminals: they conceal the nature of their crimes to fool the victims, and do their level best to destroy or hide incriminating digital and physical evidence from the investigators. Deception and concealment is an inherent part of digital crimes such as computer fraud, identity theft and hacking, meaning that some criminals are well versed in the techniques for secreting information about their crimes, as well as details about the proceeds of crime, their criminal associates and so on. As a result, criminal investigations are often faced with the difficult task of reconstructing chains of events from incomplete evidence, and recovering evidence that criminals have deleted, encrypted or concealed in some way.

Strong encryption can be a particularly tough challenge for digital forensic investigators but thankfully criminals, like the rest of us, are only human: it is not unknown for them to choose easily guessed passwords, or drop clues in plain sight. Even hackers who thrive in the cloak and dagger underworld sometimes give themselves away for the most simple errors, such as including their names or tags in malware code and bragging about their crimes to their peers.

Even with their gloves on, IT enabled criminals leave digital fingerprints

Private forensic investigators are at a disadvantage compared to the police in that they typically experience significant difficulties accessing information sources from third parties such as records from the phone and network companies, at least without a court order. Having said that, the police also struggle with privacy laws and uncooperative companies or individuals reluctant to let them in or provide the information requested. Even a short delay in providing access can threaten a case, for example if the criminals have the chance to disappear across an international border before the police move in for the arrest.

In some cases, the sheer volume of evidential materials collected from the scene can be a threat in another way. Sifting through terabytes of data and slack space on server disks to find incriminating evidence would be practically impossible without suitable forensic search tools. The time and effort and hence expense incurred in making an examining evidential copies of large disk arrays can be daunting, particularly if the original owners of the systems or disks are pushing for their hardware to be returned to service urgently for business reasons.

Information overload is a genuine threat

The legal process itself presents a number of threats to ill-prepared, incompetent or unlucky forensic investigators, particularly concerning the integrity of evidence and hence its admissibility to the court. There are quite specific rules in place regarding the protection required for evidence but these rules have mostly been invented in response to legitimate legal challenges, and of course someone had to be the first to suffer such a challenge. Given the rate of change in technology, the challenges and hence the rules are evolving all the time. Likewise, forensic tools and techniques are being continually developed, challenged and (hopefully) proven.

The world of digital forensics is changing not only within information technology but also within law enforcement. The challenge dealing with law enforcement is that (1) all too often existing laws are inadequate, (2) commonly, local law enforcement is not prepared for technology cases, (3) outside resources to law enforcement is often limited, (4) prosecutors commonly are not knowledgeable about technology and rely on "experts" who may not be qualified, (5) defense attorneys that understand technology sufficiently to perform adequately are not common, and (6) the majority of the judicial system is inadequately skilled to adjudicate such a case.

[Bob Johnston blog entry](#) January 2008

Presenting digital evidence in court is another minefield for forensic investigators, especially given the technical complexities of IT combined with the cunning and guile of fraudsters, hackers and other criminals, all sitting on top of the

fundamental volatility of digital data. The problems are ameliorated to some extent as IT literacy spreads among the legal profession and jurors but even IT professionals struggle to understand convoluted information security incidents involving, say, cross-site scripting or transnational network attacks.

Vulnerabilities

Crime always seems to happen - or rather be discovered - at the worst possible time, when resources are stretched and other priorities compete for management and staff attention. Victims are often torn between sealing the scene, collecting and examining forensic evidence and going after the perpetrators, or just mopping up quickly, resolving the incident as best they can, minimizing the business impacts and getting back to normal as soon as practicable. The period immediately following the revelation of a serious information security incident, or some other serious incident that in some way involves digital evidence, tends to be chaotic and confusing for all involved. Managers still struggling to come to terms with the incident may find it difficult to make key decisions and initiate the appropriate activities in good time, and meanwhile evidence may be decaying while perpetrators flee the scene.

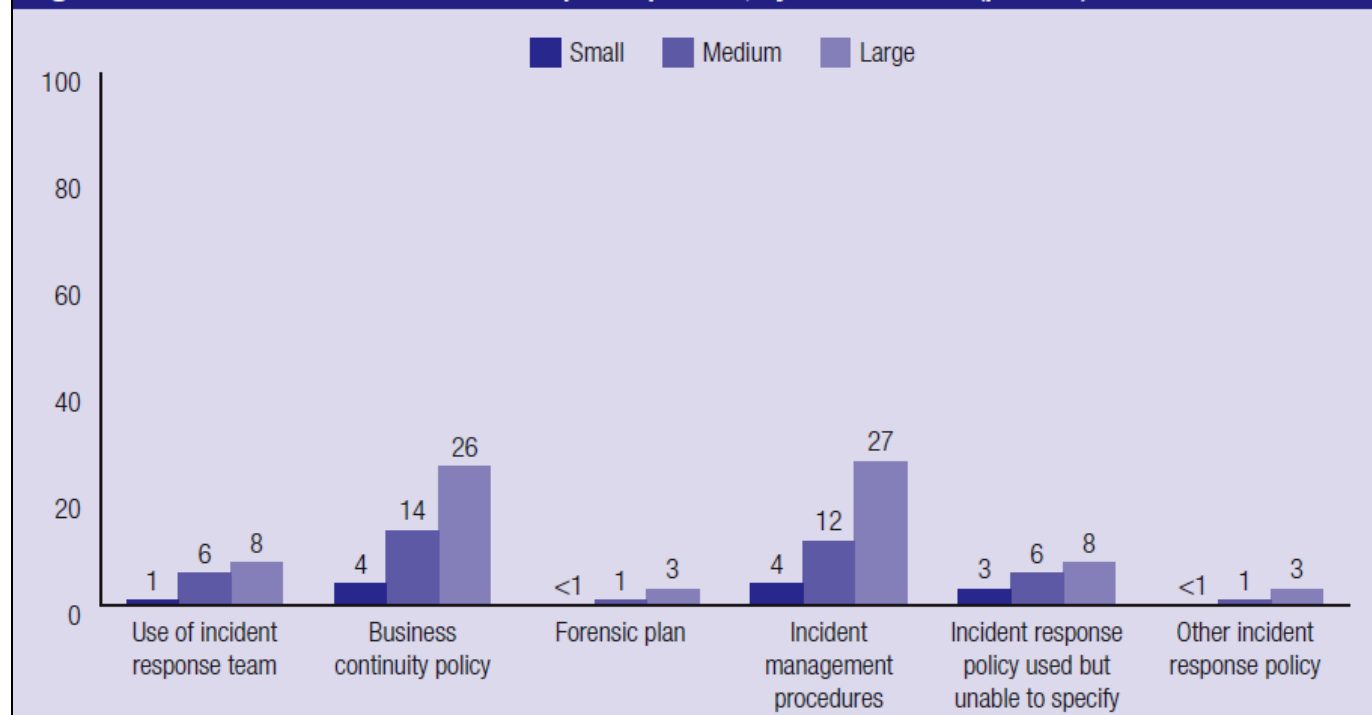
Lacking proper preparation for the kinds of serious incident that might require digital forensics is unfortunately a common vulnerability. The forensics plans, policies, procedures, tools and skilled people themselves need to be carefully prepared, and slotted neatly into the organization's incident management processes. Organizations that have yet to detect, if not experience their first major digital incident are probably less likely to have made the necessary preparations. This is really just another contingency planning issue, and arguably part of corporate governance.

Another vulnerability stems from the necessary disclosure or admission that the organization has fallen victim to a crime of some sort. Banks, for example, may be reluctant to admit publicly that they might have been hacked or defrauded as this naturally calls into question the effectiveness of their preventive information security controls. [On the upside, at least they appear to have detected and responded to the incidents in question!]

Admitting to being the victim of crime is admitting to weakness

The sheer mind-boggling tedium of many forensic processes can lead to inexperienced or

Figure 13 Businesses' use of incident response policies, by business size (percent)



Source: *The Australian Business Assessment of Computer User Security: a national survey, June 2009*

bored investigators 'cutting corners' unwisely, and perhaps damaging/destroying the evidence or missing vital clues as to the crime itself. Computers are much better than us at methodical activities and forensic tools can help immensely in the search for digital needles in virtual haystacks. Dedicated forensic hardware helps too, for example parallel multi-disk copying systems to create more than one evidential copy of a disk at a time.

Impacts

Forensic science as a whole has had an immense impact on the credibility of the legal system, significantly improving the objectivity and plausibility of claims made in court by providing undeniable evidence, or facts as they are known, and substantially reducing reliance on opinions and conjecture. Digital forensics is still an immature field but through both scientific developments and 'case law' (practices challenged and established in court, forming legal precedents), it has come a long way in the past 20 years. Furthermore as the Scientific American clipping below indicates, digital forensics has application in commercial settings as well as in criminal law cases, for example proving or disproving theft or plagiarism of intellectual property and detecting fake content.

"I am often asked to authenticate images for media outlets, law-enforcement agencies, the courts and private citizens. Each image to be analyzed brings unique challenges and requires different approaches. For example, I used a technique for detecting inconsistencies in lighting on an image that was thought to be a composite of two people. When presented with an image of a fish submitted to an online fishing competition, I looked for pixel artifacts that arise from resizing. Inconsistencies in an image related to its JPEG compression, a standard digital format, revealed tampering in a screen shot offered as evidence in a dispute over software rights."

Hany Farid, [Scientific American](#) June 2008

The significant costs incurred in collecting, securing and investigating digital evidence represent a financial cost impact, of course, but also has a more subtle impact in that many legitimate cases never proceed simply because of the up-front investment required. Legal and

scientific fees soon mount up and in situations where the other party is not in a position to repay the compensation and costs that may be awarded against them (assuming they lose!), it makes little sense to proceed purely on economic grounds. However there may well be other reasons such as retribution and/or to deter others. Finally, the full expense of mounting a case based on digital forensics may not be known until towards the end, by which time the costs are sunk and there is probably a psychological commitment to see it right through, regardless.

Presenting digital forensic evidence in court creates its own challenges, especially if the judge and jurors are not particularly comfortable with IT concepts. Skilled forensic experts and counsel may use diagrams and demonstrations to put their points across but there remains a risk that they will be seen as 'too complicated to believe' or alternatively perhaps condescending!

The impacts of getting it wrong are clear enough: cases that appear absolutely valid and convincing to those involved sometimes fail to persuade the judge and/or jury, so the case is lost, perhaps "on a technicality". When this results in an innocent man being convicted for a crime he did not commit but was unable to disprove, this has wider ramifications than just the impact on the man himself: it discredits the legal system. In some jurisdictions, serious criminal cases are judged not "on the balance of probabilities" which applies to lesser cases, but "beyond reasonable doubt". Acceptance that a greater number of guilty parties will escape justice is implicit in this requirement for a greater level of proof, but the integrity of the judicial system takes precedence over individual cases. Miscarriages of justice are damaging to society as well as the wrongfully convicted.













Conclusion

Digital forensics was a fascinating but challenging security awareness topic to cover, though we hope worthwhile. Differences in the laws and rules of evidence between jurisdictions mean that some of the content is probably inaccurate in specific circumstances, and it is certainly far from complete. Please remember that NoticeBored is merely a security awareness service and this is definitely not legal advice. Consult a lawyer and take care out there. ■



Awareness content for July


The following security awareness materials are available for NoticeBored subscribers:


Awareness materials for all employees

1. **Security seminar: digital forensics**  9 slides
Those who have only seen CSI Miami and the like may have a rather distorted view of what *really* happens in a typical investigation.
2. **Awareness posters: forensics**  x6
Professional pin-up security reminders.
3. **Screensavers: forensics**  x4
Based on the presentations and poster images.
4. **Awareness stickers: forensics** 
Useful labels – adapt as you wish.
5. **Case study: digital forensics**  2 pages
Based on a recently-reported true story, the case study involves someone who did her own forensic investigation to catch a laptop thief.
6. **Top tips: forensics**  1 page
Simple tips help visualize and recall the issues.
7. **Take home messages: forensics**  1 page
Advice to consider carefully if computer-related crimes occur either at work or at home. If an online predator “groomed” *your* kids, how would you react? Would you know exactly what to do?
8. **Crossword puzzle: forensics**  2 pages
9. **Security awareness survey form**  1 page
10. **Security awareness test: forensics**  1 page
11. **Glossary: forensics terms**  3 pages
12. **Forensics hyperlinks collection**  HTML
Read more about [digital forensics and related issues](#) on the Internet.


Awareness materials for executives


13. **Mind-maps: forensics**  5 Visio diagrams
Get your mind around the key aspects of digital forensics and their interrelationships.
14. **Board agenda: forensics**  1 page
Preparation is the key to effective forensics, and it starts right at the top.

15. **Model policy: forensic investigation**  2 p.
Just 1 axiom and 5 specific policy statements.


16. **Mgmt seminar: digital forensics**  8 slides
A process overview for managers.

17. **Elevator pitch: digital forensics**  1 page
Key issues for management, in a nutshell.

18. **Exec briefing: digital forensics**  1 page
Execs have an interest in the kinds of serious incidents that require digital forensics.


19. **Mgmt briefing: managing digital forensics investigations**  7 pages

Managing the process properly is vital to avoid accidentally damaging or discrediting the evidence and hence ruining a case.


20. **Security metrics: digital forensics**  3 pages
[If you have enough cases to make it worth measuring and improving the process, maybe you need to work harder on prevention?!]


Materials for IT professionals

21. **This newsletter: digital forensics**  6 pages
A newsletter with topical news and issues provides a gentle introduction to the topic.

22. **Awareness activities for July**  7 pages
Includes a long reading list this month.

23. **Tech seminar: digital forensics**  11 slides
What to do, and more importantly what not to do when investigating digital incidents.


24. **Tech briefing: forensics grab-bag**  2 pages
What goodies should the grab-bag contain? Who should decide, and on what basis?

25. **Tech procedure: digital forensics**  7 pages
Sure it's generic and not legal advice but if you don't already have one, start here.

26. **Custody form**  2 sides

27. **Evidence form**  2 sides

Two sample forms help ensure that, when evidence is collected for forensic analysis, the proper process is followed. Take legal advice!

28. **Checklist: digital forensics**  6 pages
How do your organization's processes stack up? Are they barely adequate or best practice?

NoticeBored diary

NoticeBored's rolling security awareness plan gives us some flexibility to pick up on new information security issues as they arise. The topics we are currently researching and preparing for delivery over the next three months are as follows.

August – email and desktop security

Email is just one of many ways we keep in touch with friends and colleagues. There are a multitude of security issues associated with email, IM, Skype, Twitter and so on, and a multitude of other technologies that have invaded the average modern office. Awareness helps us cross the security minefield in the office just a little more safely.

September – personal privacy and commercial confidentiality

How does privacy differ from confidentiality, exactly, and why should we care? September's module will dip into both personal and proprietary information, privacy and secrecy.

October – third party security issues

There are definitely information security aspects to dealing with business partners, suppliers, customers, regulators, advisors and so forth, but what *are* the main information security risks and what can we do about them?

Your input is welcome

If you'd like to contribute to our planned awareness modules, suggest new topics or different types of awareness materials, please email info@NoticeBored.com. Unless you tell us what you want, we can only guess. Investigate our digitals on the [NoticeBored website](http://www.noticebored.com). ■

NoticeBored & IsecT news

The free induction module

In parallel with researching and writing the awareness modules listed to the left, we're working hard on a revision to the [NoticeBored induction module](#), intended both for inducing or orienting new employees towards security and to launch new security awareness programs based on the unique NoticeBored approach. We provide this module as a complimentary bonus to welcome our new customers. More details of the changes will follow next month but meanwhile do get in touch if you have good ideas along these lines, or want to see the module.

A new author joins the NoticeBored production team

Rob Slade, renowned virus researcher, academic, author and harsh-but-fair reviewer of *many* information security books, has joined the NoticeBored team just in time to lend his technical expertise to this month's forensics module. Rob's expertise is enormously helpful in preparing and polishing-off the awareness materials and, as an added service, he gets to review and comment on our product before it hits the streets. Welcome aboard Rob, and thank you in advance for all those "improvement suggestions" you're brewing up! ■



Newsletter published by:

[IsecT Ltd.](#)
Castle Peak
1262 Taihape Road
RD9 Hastings
New Zealand

Tel: +64 6874 3344

Copyright and disclaimer

All NoticeBored materials including this newsletter are protected by international copyright law. For more information, please contact the copyright holder, IsecT Limited (visit www.isect.com or see above for our contact details).

You are encouraged to circulate the Adobe Acrobat version of this newsletter to anyone *provided* that it remains unchanged and intact (including this copyright notice), is not embedded in any other product or service and is provided free of charge.

The information in this newsletter is provided free, for information only and 'as is'. Whilst believed partially correct, it is in no way comprehensive and certain parts are unlikely to be entirely true. It is provided for interest only and is not intended to be relied upon as formal advice. **It is not legal advice.** Seek your own legal advice from a qualified and competent legal practitioner familiar with the applicable laws and rules of evidence. No liability is accepted for any errors or for any losses that may be incurred if any such information is relied upon.