

Computer Forensics

A Pocket Guide

Nathan Clarke

Copyright IT Governance Ltd

Provided by IHS Markit under license with IT Governance Ltd. See www.itgovernance.co.uk for details.

No reproduction or networking permitted without license from IHS.

Full document details: ITG 2010



IT Governance Publishing

Computer Forensics



Computer Forensics

A Pocket Guide

NATHAN CLARKE



IT Governance Publishing

Documents



Document Sharing Hub

Copyright IT Governance Ltd

Provided by IHS Markit under license with IT Governance Ltd. See: /, User=,

No reproduction or networking permitted without license from IHS.

Full document details: ITG 2010

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher or, in the case of reprographic reproduction, in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers at the following address:

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EH
United Kingdom

www.itgovernance.co.uk

© Nathan Clarke 2010

The author has asserted the rights of the author under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

First published in the United Kingdom in 2010
by IT Governance Publishing.

978-1-84928-040-2



Documents

Document Sharing Hub

PREFACE

Computer forensics has become an essential tool in the identification of misuse and abuse of systems. Whilst widely utilised within law enforcement, the rate of adoption by organisations has been somewhat slower, with many organisations focusing upon the traditional security countermeasures to prevent an attack from occurring in the first place. Such an approach is certainly essential, but it is also well understood that no system or network is completely secure. Therefore, organisations will inevitably experience a cyberattack. Moreover, traditional countermeasures do little to combat the significant threat that exists from within the organisation. Computer forensics is an invaluable tool for an organisation in understanding the nature of an incident and being able to recreate the crime.

The purpose of this pocket book is to provide an introduction to the tools, techniques and procedures utilised within computer forensics, and in particular focus upon aspects that relate to organisations. Specifically, the book will look to:

- develop the general knowledge and skills required to understand the nature of computer forensics;
- provide an appreciation of the technical complexities that exist; and
- allow the reader to understand the changing nature of the field and the subsequent effects that it will have upon an organisation.

Preface

This will allow managers to better appreciate the purpose, importance and challenges of the domain, and allow technical staff to understand the key processes and procedures that are required.

The final section of the text has been dedicated to resources that will provide the reader with further directions for reading and information on the tools and applications used within the computer forensic domain.

ABOUT THE AUTHOR

Dr Nathan Clarke is a senior lecturer at the Centre for Security, Communications and Network Research at the University of Plymouth and an adjunct lecturer with Edith Cowan University in Western Australia. He has been active in research since 2000, with interests in biometrics, mobile security, intrusion detection, digital forensics and information security awareness. Dr Clarke is also the undergraduate and postgraduate Programme Manager for information security courses at the University of Plymouth.

During his academic career, Dr Clarke has authored over 50 publications in referred international journals and conferences. He is the current co-chair of the Workshop on Digital Forensics & Incident Analysis (WDFIA) and of the Human Aspects of Information Security & Assurance (HAISA) symposium. Dr Clarke has also served on over 40 international conference events and regularly acts as a reviewer for numerous journals, including *Computers & Security*, *IEEE Transactions on Information Forensics and Security*, *The Computer Journal* and *Security and Communication Networks*.

Dr Clarke is a Chartered Engineer, a member of the Institution of Engineering and Technology (IET) and British Computer Society, and is active as a UK representative in International Federation for Information Processing (IFIP) working groups relating to Information Security Management, Information Security Education and Identity Management.

Acknowledgements

Further information can be found at
www.plymouth.ac.uk/cscan.

ACKNOWLEDGEMENTS

Thanks are due to Prof Steven Furnell for his insightful feedback on the draft version of the manuscript. Thanks are also due to my partner, Amy, whose invaluable support has helped immensely.

Copyright IT Governance Ltd
Provided by IHS Markit under license with IT Governance Ltd
No reproduction or networking permitted without license from IHS

CONTENTS

Chapter 1: The Role of Forensics within Organisations	10
Chapter 2: Be Prepared – Proactive Forensics	17
Chapter 3: Forensic Acquisition of Data	26
Chapter 4: Forensic Analysis of Data	34
Chapter 5: Anti-Forensics and Encryption	46
Chapter 6: Embedded and Network Forensics	52
Conclusion	58
Resources.....	60
Specialist books in Computer Forensics	60
Software and tools	64
Web resources.....	69
ITG Resources.....	73

CHAPTER 1: THE ROLE OF FORENSICS WITHIN ORGANISATIONS

The importance of information security within an organisation is becoming better understood. Regulation, legislation and good governance are all motivators for organisations to consider the role information security plays in protecting data. Whilst better understood, the adoption of good information security practices is far from uniform across all organisations, with enterprise companies faring better than many smaller organisations who are trailing in their knowledge and deployment of secure practices. With the significant growing threat arising from cybercrime and related activities, it is increasingly important that all organisations address the issue of ensuring good information security.

In order to appreciate the need for computer forensics within an organisation, it is important to look at the nature and scale of the threat that exists. Unfortunately, truly understanding the scale of the threat is difficult as the reporting of cybercrime is relatively patchy. Many organisations see such reporting as something that will affect their brand image and reputation. Whilst discussions are being held in some countries about implementing laws to force organisations into reporting incidents, at this stage the industry relies upon survey statistics to appreciate the threat. Many such surveys exist, but four in particular, used together, provide a good oversight of the cybercrime landscape:

1: The Role of Forensics within Organisations

- Computer Crime and Security Survey¹ by the Computer Security Institute (CSI) – an annual survey that typically has over 500 respondents with a focus upon the United States and a skew towards Enterprise organisations. This survey is a regularly cited source for understanding the nature of the threat.
- Global Information Security Survey² by Ernst and Young – another annual survey, but with a wider perspective. In 2009, the survey had almost 1900 organisations from over 50 countries across all major industries.
- Information Security Breaches Survey³ by the UK Department for Business, Enterprise and Regulatory Reform (BERR) – a UK-focused survey with over a 1000 respondents (in 2008). In comparison to the previous two surveys, the nature of the respondent group in this survey is far more focused upon SMEs rather than Enterprise organisations. It is possible, therefore, to appreciate a different perspective on the problem.

¹ *CSI Computer Crime and Security Survey*, Richardson R, Computer Security Institute (2008).

www.qocsi.com

² *Outpacing Change: Ernst & Young's 12th Global Information Security Survey*, Ernst & Young (2009).
[www.ey.com/publication/vwLUAssets/12th_annual_GISS/\\$FILE/12th_annual_GISS.pdf](http://www.ey.com/publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf)

³ *Information Security Breaches Survey*, BERR (2008), Crown Copyright.
www.berr.gov.uk/files/file45714.pdf

1: The Role of Forensics within Organisations

- Global Internet Security Threat Report⁴ by Symantec – once a twice-yearly publication, the report is now published annually. This report differs from the previous three in that it does not rely upon people to report the findings. Instead, Symantec acquire the information from a variety of sensors and systems deployed throughout the world. The report therefore provides a far more statistically reliable picture on the nature and scale of the threat; however, it fails to illustrate what the consequences are of those threats and what efforts are being made to better secure systems.

Taking a snapshot of the most current surveys at the time of writing, it is clear that the nature and seriousness of the threat is considerable. Looking at the mainstay of cybercrime, malicious software (malware), it can be seen that they still provide a significant threat to systems. The CSI survey in 2008 reported that 50% of respondents experienced a virus incident (which includes other forms of malware). The BERR survey reports this as lower at 35% in 2008 overall; however, notably when analysing for Enterprise organisations only, this number shoots back up to 68%. This demonstrates at present, Enterprise organisations are a far larger target for attackers. Indeed, Symantec's report has identified that threats are increasingly being targeted to specific

⁴ Symantec Global Internet Security Threat Report: Trends for 2008, Symantec (2009).

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

1: The Role of Forensics within Organisations

organisations or individuals, and the CSI survey also reported that 27% of respondents had experienced targeted attacks within their organisation.

An underlying theme in this changing threat landscape is the move towards financial reward. Symantec reports that the underground economy is generating millions of dollars in revenue from cybercrime-related activity. Previously, financial reward was infrequently a key driver of cybercrime. Hackers would break into systems in order to demonstrate their technical ability over those administering the systems, and malware writers created viruses and worms that would maximise their infection and spread throughout the Internet. However, since the beginning of the millennium the surveys have shown an increasing focus being given towards threats that provide a financial reward to the attacker. Advanced-fee fraud and phishing or 419 scams are two examples of widespread threats aimed at providing financial reward. As awareness of these widespread threats increases, so the threat evolves towards more targeted threats, such as spear phishing.

Whilst the previous two trends are focused upon the threats that enter the system from outside the organisation, the surveys point to a considerable threat coming from inside. The CSI survey put this second to virus incidents at 44% of respondents, with the BERR survey at 21%. Moreover, the BERR survey in particular noticed a significant swing from external to internal threat, with over two-thirds of the worst incidents coming from inside misuse. Organisations, therefore, may face a considerable threat from their own employees.

1: The Role of Forensics within Organisations

This becomes more concerning when you appreciate that much of the traditional information security mechanisms are focused upon ensuring that attackers from outside the system cannot get in. Little consideration is frequently given to the attackers from within the system.

Whilst the nature of the threat has changed significantly, it is essential to realise that it is still evolving. Although it is difficult to predict what form the threat will take in the future – largely by doing so will itself ensure the threat evolves in a different direction – it is important to ensure information security is not simply a reactive system that deploys new countermeasures upon identification of new threats, but proactively seeks to develop controls, practices and policies to assist in their identification and prevention.

The discussion up to this point has focused upon cybercrime. However, it is also important to appreciate that information systems are not simply the target of crime but are frequently used as a tool for crime. Many forms of traditional crime, such as money laundering, fraud, blackmail, distribution of child pornography and illegal drug distribution, can all be facilitated by the use of computers. Indeed, given the ubiquitous nature of information systems and the efficiency gains achieved in using them for financial record keeping and communication, it is difficult to envisage many crimes of this nature not using computers. Within an organisational perspective, it is important to ensure you do not simply protect your systems from cybercrime threats, but also ensure they are not being used to facilitate traditional crime.

1: The Role of Forensics within Organisations

Digital forensics is a growing specialism that assists organisations in the identification of misuse. In comparison to many areas of traditional information security, such as authentication and access control, it is relatively new, born out of the need to be able to identify exploitation of electronic systems in a manner that would be deemed acceptable by the juridical system. Within digital forensics, a number of more specific sub-categories exist, such as computer, network and embedded forensics. Each in turn seeks to understand their specific technology platform to capitalise upon the evidence being captured. For instance, within computer forensics, tools, techniques and procedures have been developed to extract evidence from hard drive and volatile media. Significant time has been focused upon understanding the nature of file systems in order to ensure all artefacts are identified, and to appreciate the nature of the data. Within embedded forensics, such as mobile devices or game consoles, the nature of the underlying architecture means that different tools and procedures are required in order to extract relevant artefacts in a forensically sound manner.

A key driver to date for the use of computer forensics has been from law enforcement and the identification of traditional crime. This quickly moved on to cybercrime, but is still largely within the sphere of law enforcement and their need to analyse systems in a legally acceptable manner in order to bring the guilty to justice. However, although this driver has not changed, organisations are increasingly identifying the importance of establishing a computer forensics expertise. Whilst organisations might not always seek criminal or

1: The Role of Forensics within Organisations

civil compensation for the attacks against their systems, it has become accepted that the tools, techniques and procedures developed for digital forensics provides an effective and sound methodology for analysing systems. The primary motivation for using forensics is incident management and the ability to identify which files have been affected and how the malware has infected the system, with a view to closing the vulnerability. Forensics within the organisation can also be used to identify possible insider misuse of systems or information. An organisation equipped with a well-trained computer forensic capability is able to both reactively and proactively defend against attacks from both inside and outside the organisation.

The primary focus within the digital forensic industry has been on computer forensics and as such the focus of this pocket book will largely be on computer forensics. However, many of the processes and procedures documented within the forthcoming chapters are also appropriate for use within the other areas. In addition, a chapter has also been included to discuss specific aspects of network and embedded forensics as both of these are becoming increasingly important within a world where mobile devices are ubiquitous and anti-forensic techniques are more commonplace. The next three chapters focus upon the core procedural aspects of computer forensics: the proactive stance, acquisition and analysis.

CHAPTER 2: BE PREPARED – PROACTIVE FORENSICS

Within an organisation, undertaking forensics is not a simple task and involves a series of procedural and technical aspects that if not carried out correctly will affect the forensic value of the investigation and the resulting evidence. It is therefore essential that these are developed, implemented and tested prior to tackling an incident. Being proactive about the design of a forensic expertise within your organisation will ensure that your incident response team is able to respond effectively and efficiently. This chapter introduces the steps necessary to be proactive, and discusses the key procedural aspects that need to be followed during an investigation.

Being proactive is not simply about ensuring the correct procedures are in place for dealing with an incident, or about ensuring staff have the necessary training to forensically acquire and analyse machines running Windows®, Linux, Unix and Mac (plus many others). It is possible to go further in the forensic readiness and consider the organisational IT infrastructure. Optimising the IT infrastructure for use within incident analysis will enable more efficient analysis of systems whilst minimising the operational impact on systems. For instance, if an organisation has a file server that is critical to operations and is under a 24/7 service level agreement, then it would be difficult to take a system down for forensic acquisition of data – particularly as this can take some time when dealing with large storage volumes. Establishing

2: Be Prepared – Proactive Forensics

redundancy within the IT architecture would assist in ensuring critical systems remain operational yet provide a facility to provide incident analysis.

The most effective deployment of a forensics team is as an aspect of the organisation's Computer Security Incident Response Team (CSIRT) – more commonly referred to as Computer Emergency Response Team (CERT). Whilst no definitive standard exists to date, Carnegie Mellon University's CERT have compiled a handbook for the development, implementation and management of a CSIRT.⁵ The handbook provides a robust framework for the handling and assessment of incidents, and clearly defines the role for forensics as one belonging to incident analysis.

Whilst it is out of the scope of this text to describe the framework in detail, it is worth highlighting the specific aspects relating to setting up a forensics team. Computer forensics is a highly human-centric process, requiring trained specialists with the specific knowledge of operating systems and forensic software. This therefore places a large burden upon recruitment and training of staff. Furthermore, once trained, given that new operating systems function differently and frequently come equipped with new file systems, resources are required for continued training. The scope of training will depend upon the variety of systems an organisation is using; fewer file systems result in

⁵ *Handbook for Computer Security Incident Response Teams (CSIRTs)*, West-Brown, M et al, CERT Carnegie Mellon (2003).

www.cert.org/csirts

2: Be Prepared – Proactive Forensics

less training. The nature of undertaking forensics means you do not only need an individual with an excellent technical knowledge of systems, but you are also looking for someone who has an inquisitive mind, and is able to identify leads and follow them through the data. Given the complex nature of file systems and the large storage capacities of hard drive media, it simply is not cost effective to examine every aspect of the drive. It is therefore necessary to understand and appreciate the nature of the crime, the resulting evidence that might exist and where such evidence might reside on the media. The results and findings of the forensic investigation are very much down to the examiner and their ability to professionally analyse the data.

The actual process of computer forensics is inherently a reactive approach to the identification of misuse of systems, whether that is cyber or computer-assisted crime. But how do you know when to undertake a forensic investigation of a system? Because of the nature of forensics, specifically the time and resources required to investigate a system, routine investigation of systems is simply infeasible. An organisation will investigate a system based upon one or more factors causing concern to an administrator. Traditional security controls are frequently used for cyber-related activities, such as Intrusion Detection System (IDS) alarms, a system operating outside of normal parameters, unusual processes running on a system, log files containing spurious entries, network logs showing large volumes of traffic entering or leaving the network, or end-users reporting discrepancies.

2: Be Prepared – Proactive Forensics

Having established that something is amiss, forensics can now be utilised to identify what has happened. Whilst literature differs a little on the number of stages that a forensics procedure requires, all agree on the general principle of the process. Amongst the most robust and popular models proposed is the Digital Forensics Workshop⁶ model. It establishes seven key stages to the process:

- Identification – the initial identification that something is wrong and requires forensic investigation.
- Preservation – to ensure data is acquired in a forensically sound manner with an appropriate chain of custody being maintained.
- Collection – the use of approved software and hardware and appropriate legal authority where necessary in collecting the evidence.
- Examination – through the use of filtering and data extraction techniques identify artefacts of interest.
- Analysis – understand the chronology of events and link together artefacts in order to understand the complete picture.
- Presentation – document and present the findings in an appropriate manner.
- Decision – in a legal situation this would be whether sufficient evidence exists to proceed with a criminal case. Within an organisational environment, it could be the point at which a

⁶ DFRWS Technical Report: A Road Map for Digital Forensic Research, Palmer, G, DFRWS (2001).

www.dfrws.org/2001/dfrws-rm-final.pdf

2: Be Prepared – Proactive Forensics

decision is made to proceed with civil proceedings or an action is taken against an employee.

The core underlying principle within computer forensics is preservation of data. Therefore, during all stages of examination and analysis a forensic examiner will work on duplicates of the original evidence rather than the original. Should changes occur to the data, an additional duplicate of the original can be made. In order to facilitate the preservation of evidence, it is important to ensure an appropriate chain of custody throughout the forensic investigation, from the initial capture of the hardware through to collection, examination, analysis and presentation. At all stages, it should be clear who had been handling the data and when. At no time should the evidence remain unsupervised or freely accessible. In the UK, examiners adhere with the Association of Chief Police Officers (ACPO) guidelines.⁷ These comprise of four principles:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may be subsequently relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to

⁷ *Good Practice Guide for Computer-Based Electronic Evidence*, 7Safe, ACPO (2007).

www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

2: Be Prepared – Proactive Forensics

give evidence explaining the relevance and the implications of their actions.

3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Whilst the intention of the organisation in performing an investigation might not be one of involving the police or seeking compensation through civil actions, care should always be taken in following these principles in case such a decision is required at a later stage. For instance, in many investigations the true consequences of insider misuse might not be understood until after the investigation has taken place. If the investigation did not follow the guidelines and good forensic practice, the value of the evidence found would be in question.

In addition to the personnel requirements for establishing a forensics expertise, thought must also be given to the equipment required to perform such activities. The subsequent chapters provide an insight into the techniques and tools required to perform a forensic investigation, with the Resources section providing a reference. However, for the moment the dialogue will concentrate on the initial set-up requirements. In order to perform forensic analysis of systems, it is imperative that

2: Be Prepared – Proactive Forensics

the machine performing the analysis is a trusted one that has not been compromised. Typically this would involve having a stand-alone computer or, within a larger environment, a closed network with minimal network connections to essential services. A large role of the investigation will be to undertake string searches of the drive for specific keywords or file formats. With large storage devices this takes time, so having sufficient processing capacity and high-speed drives would assist in speeding up the process. A myriad of hardware and software components are then required to perform the actual investigation. Given the nature of the task, it is also important the investigation takes place in a restricted room with strict physical access control. Maintaining the integrity of the investigation is paramount if the organisation decides they wish to utilise the evidence for any formal civil or criminal proceedings.

It is worth highlighting that as computer forensics is a relatively new discipline, the speed of change regarding what is considered standard operating procedure is rapid. New developments within the area are pushing the envelope of what computer forensics is able to achieve. A decade ago, computer forensics involved the use of some elementary tools and hexadecimal editors that allowed you to view the actual data. Tools have since been developed that permit the extraction of files and whole file systems in a forensically sound manner. This has reduced the technical level of expertise required in many cases and has certainly speeded up dramatically the process of examination. The flip side to this is, unfortunately, that examiners now have to deal with far larger