

Tiger Digital Forensics – Certified Incident Handler

Title	Tiger Digital Forensics – Certified Incident Handler
Version	1.1
Status	Public Release
Date	21 st Oct 2011
Author	Professor Andrew Blyth (Tiger Technical Panel)
Review Date	1 st Aug 2011

Version	Date	Author	Changes and Comments
0.0	20/09/2010	Prof Andrew Blyth	Draft Version
1.0	21/06/2011	Prof Andrew Blyth	Final Release V1.0
1.1	21/10/2011	Prof Andrew Blyth	Final Release V1.1

Table of Contents

1. Introduction.....	3
1.1 Aims and Objectives.....	3
2 Legal, Management, Ethics and Compliance.....	6
2.1 Understand Requirements.....	6
2.2 Defining Scope.....	6
2.3 Legal Issues.....	6
2.4 Planning and Management.....	7
2.5 Managing risk.....	7
2.5 Testing Methodology.....	8
2.6 Testing Platform.....	8
3.0 Technical Expertise.....	10
3.1 Forensic Technology.....	10
3.2 Scene of Crime Management.....	10
3.3 File System and File Systems Artefacts.....	11
3.4 Identification and Analysis of the Operating System.....	12
3.5 Identification and Analysis of Applications and Software Artefacts....	12
3.6 Identification and Analysis of Internet Activity.....	13
3.7 Identification and Analysis of Audit Data.....	14
4 Deliverables.....	16
4.1 Management Presentation of Results.....	16
4.2 Technical Presentation of Results.....	16

1. Introduction

1.1 Aims and Objectives

- 1.1.1 This document is intended to define the base-line technical standards for the TIGER Digital Forensics – Certified Incident Handler this is based upon the advanced TIGER Digital Forensics – Certified Forensic Investigator level. It also reflects where possible the emerging ISO27037 standard
- 1.1.2 The “Incident Handler” expected to possess and have the ability to demonstrate a range of skills and knowledge associated with the first response and the need to seize of computer evidence, including imaging of main stream desktop and laptop equipment, as well specify works to recover digital evidence from more complex systems such as RAID, mobile or other devices.
- 1.1.3 The nature of the assessment for a the TIGER Digital Forensics – Certified Incident Handler is a structured assessment whereby the candidate is expected to discuss numerous aspects of a first response scenario and subsequently to demonstrate technical capability to obtain an image.
- 1.1.4 The objective of the assault course is to evaluate the candidate in an environment that mimics a typical real-world scenario as much as possible.
- 1.1.5 The areas of expertise that are to be assessed at the TIGER Digital Forensics – Certified Incident Handler level consist of three overall aspects categorised as follows:
 - **Legal, Management, Ethics & Compliance:** Demonstration of knowledge and capability in areas such as legal knowledge, understanding customer requirements, the scoping of forensic investigation, the planning and management of engagements, risk management throughout engagements, the use of a suitable forensic investigation platform and compliance with current best practice guidance.
 - **Technical Expertise:** Demonstration of knowledge of, and ability to perform imaging of drives. and an understanding of case limitations.
 - **Deliverables:** Demonstration of capability in the preparation and ability to acquire an image of main stream computer equipment, to maintain chain of custody and standards and scope/advise on larger scale works, finally to brief to both non-technical and technical audiences. In both instances the results will be documented providing a summary of the issue.

- 1.1.6 Aspects have been chosen in an attempt to ensure that the forensic investigation requirements and concerns of industry are incorporated into the individual candidate evaluation process.
- 1.1.7 The assessment for a the TIGER Digital Forensics – Certified Incident Handler consists of tree parts:
- A multiple choice assessment (1 Hour)
 - A written examination (2 Hours)
 - A practical assessment (3 Hours)
- 1.1.8 The pass marks for each element of the TIGER Digital Forensics – Certified Incident Handler assessment is 60% and a successful candidate must pass all components of assessment.

1.1.9 Summary of TIGER Scheme Forensic Investigator Requirements

Area	Skill-set	Skills Requirement Summary
Legal, Management, Ethics & Compliance	Understanding requirements	Demonstrate the ability to understand customer requirements and set customer expectations for a given incident scenario.
	Defining scope	Demonstrate the ability to define a scope of a computer forensic investigation given customer requirements, timeframes and any constraints.
	Legal issues	Demonstrate an appropriate knowledge of UK law and best practice potentially relevant to forensic investigation in a variety of situations.
	Planning and Management	Demonstrate the ability to develop a project plan for a given forensic investigation requirement and defined scope. Demonstrate an understanding of engagement management issues such as customer and supplier liaison, arranging access to facilities, secure storage of customer data and contingency planning.
	Managing risk	Demonstrate the ability to enforce procedures and liaise with the customer and other relevant parties to reduce the likelihood or impact of any unwanted issues arising from forensic investigations such as disruption to service.
Technical Expertise	Forensic Technology	Demonstrate awareness of existing and emerging computer forensic technologies likely to have relevance to a forensic investigation. In particular tools that are fit for purpose and defensible in a court of law.
	Scene of Crime Management	Demonstrate the ability to perform scene of crime management and the identification and handling of potential evidence sources.
	Identification and Analysis of the Operating System	Demonstrate the ability to identify the host operating system, and artefacts specific to the host operating system.
	May be able to Identify Applications and Software Artefacts	Demonstrate the ability to identify and analyse various software applications and artefacts specific to the software applications.
	May be able to Identify Internet Activity	Demonstrate the ability to identify and analyse internet activity relating to various clients and servers. In particular, the ability to identify and analyse Internet Activity relating to various web browsers and web servers.
May be able to Identify and location of Audit Data	Demonstrate the ability to identify, extract and document audit data that has been generated by a variety of operating systems and applications/services.	
Deliverables	Management presentation of results	Demonstrate the ability to produce a written and verbal summary of the computer forensic investigation results to a non-technical audience, such as a jury in the Crown Court.
	Technical presentation of results	Demonstrate the ability to document and explain identified forensic issues. Identifying the issue, impact, risk and suitable recommendations.

2 Legal, Management, Ethics and Compliance

2.1 Understand Requirements

Demonstrate the ability to understand customer requirements and set customer expectations for a given forensic incident scenario.

ID	Description
A1	The candidate MUST liaise effectively with the assessor who will provide a list of requirements and constraints for the forensic incident scenario.

2.2 Defining Scope

Demonstrate the ability to define a scope of testing given certain customer requirements, timeframes and any constraints.

ID	Description
B1	The candidate MUST be able to discuss with the assessor the benefits and disadvantages of particular approaches and how the requirements will or will not be met by the proposed scope.
B2	The candidate MUST demonstrate an understanding that a forensic investigation of digital evidence is commonly employed as a post event response to a serious information security incident or computer related crime. In fact there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs.
B3	The candidate MUST demonstrate an understanding that forensic readiness is introduced as the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation.

2.3 Legal Issues

Demonstrate an appropriate knowledge of UK law potentially relevant to forensic investigations in a variety of situations.

ID	Description
C1	The candidate MUST be able to demonstrate an understanding of the relevance UK laws and the requirement for a letter of authorisation prior to the commencement of a forensic case.
C2	The candidate SHOULD also demonstrate awareness of the need to inform and obtain permission from third parties in certain situations.

2.4 Planning and Management

Demonstrate the ability to develop a project plan for a given forensic investigation requirement and defined scope. Demonstrate an understanding of engagement management issues such as customer and supplier liaison, arranging access to facilities; secure storage of customer data and contingency planning.

ID	Description
D1	The candidate MUST be able to demonstrate awareness of the requirement for suitable system access.
D2	The candidate MUST be able to demonstrate awareness of requirement for authority documents to have been signed by all relevant parties including any third party hosting company or service providers
D3	The candidate MUST be able to demonstrate awareness of the requirement for physical access and escorts in a timely fashion.
D4	The candidate MUST be able to demonstrate awareness of the availability of key customer staff for specific elements of the forensic incident assessment.
D6	The candidate MAY be able to demonstrate awareness of the agreements with regard to delivery of the draft and final reports.

2.5 Managing risk

Demonstrate the ability to follow risk reduction procedures and liaise with the customer and other relevant parties to reduce the likelihood or impact of any unwanted issues arising from forensic investigations such as disruption to service.

ID	Description
E1	The candidate MUST demonstrate awareness of the risks associated with forensic investigations that can impact on customer systems; these may include unintentional disruption to network devices and links through bandwidth consumption.
E2	The candidate MUST demonstrate awareness of the risks associated with forensic investigations that can impact on customer systems', these may include unintentional disruption to systems and applications.
E3	The candidate MUST demonstrate awareness of the risks associated with forensic investigations that can impact on customer systems. These may include disruption to user access through the

	lockout of user and application accounts.
E4	The candidate MUST demonstrate awareness of the risks associated with forensic investigations that can impact on customer systems; these may include disruption to audit and monitoring functions.
E5	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the forensic investigation, these would be expected to include ensuring that both the investigation team and the customer have established point of contact for emergencies.
E6	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the investigation, these would be expected to include ensuring that the customer has an operational backup/restore procedure in place in the event of unintended data or system corruption.
E7	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the investigation, these would be expected to include ensuring that the customer is aware of the potential for computer equipment being held off the customers site, especially in criminal proceedings.
E8	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the test.

2.5 Testing Methodology

Demonstrate understanding of and adherence to a stated forensic incident investigations methodology for a given forensic investigation requirement and defined scope.

ID	Description
F2	The candidate MUST , when asked throughout the imaging assault course; show how any activities performed or tools used are supported directly by their chosen methodology.

2.6 Testing Platform

Demonstrate possession and use of a suitable well-maintained and configured forensic investigations platform.

ID	Description
G2	The candidate MUST be in possession of a system that is suitable for performing imaging. The system may be configured with any choice of

	<p>software and operating system(s) however the following conditions must be met:</p> <ul style="list-style-type: none">• All commercial software MUST be suitably licensed <p>Anti-virus software SHOULD be installed and configured in such a way so as to not disrupt the analysis process.</p>
--	--

3.0 Technical Expertise

3.1 Forensic Technology

Demonstrate awareness of existing and emerging forensic technologies likely to have relevance to a forensic investigation.

ID	Description
H2	<p>The candidate MUST understand the operation and role of the following forensic technologies and controls:</p> <ul style="list-style-type: none">• Relevant ACPO Guidance• Forensic Imaging <p>The candidate Should have a broad working understanding of the following</p> <ul style="list-style-type: none">• Data Carving Techniques• Virtual Environments• Audit Logs• Malware Artefacts• Live Memory Analysis• Write Blocking• Logical / Physical Acquisition• File Analysis• Operating System Differences

3.2 Scene of Crime Management

Demonstrate the ability to perform scene of crime management and the identification, collection, acquisition and handling/preservation of forensic artefacts.

ID	Description
I1	<p>The candidate MUST understand the issues relating to scheme of crime management, such as:</p> <ul style="list-style-type: none">• Handling and storage of forensic artefacts• Physical Security• Security vetting of staff• Network Considerations
I2	<p>The candidate MUST understand the legal and regulatory issues, such as:</p> <ul style="list-style-type: none">• Computer Misuse Act• ACPO GPG on E-Evidence• Data Protection Action• Police and Criminal Evidence Act• Regulations of Investigatory Power Act• Contract Law and the Theft Act• Copyright and IPR Law

13	The candidate MUST demonstrate knowledge of the impact of volatile and non-volatile evidence.
14	The candidate MUST demonstrate the ability to formulate and execute <ul style="list-style-type: none"> • The collection of evidence process. • Evidence records in relation to the chain of evidence
15	The candidate MUST demonstrate the ability to create and validate appropriate forensic images.
16	The candidate MAY demonstrate specialist analysis in relation to advanced audit data logs such as Intrusion Detection Systems and Router/Firewall Logs.
17	The candidate MAY demonstrate an understanding of password requirements prior to acquisition of evidence.
18	The candidate MAY demonstrate an awareness of the optimization of the evidence collection process and the identification of any constraints that may hinder the evidence collection process.

3.3 File System and File Systems Artefacts

Demonstrate an understanding of various file system types (NTFS, FAT16, FAT32, etc). Demonstrate an understanding of how various file system artefacts are created and managed at the physical and logical levels.

ID	Description
J1	The candidate MAY demonstrate the ability to identify the forensic target operating system type and various file system artefacts. In particular: <ul style="list-style-type: none"> • File Partitions • Master Boot Record and EFI • NTFS, FAT16, FAT32, HFS, EXT3 and EXT4 • RAID • Magic Numbers and File Types, such as: <ul style="list-style-type: none"> ○ Microsoft Office ○ Pictures (JPEG, TIFF, GIF, etc) ○ Postscript (PS) ○ Executable (COEFF and ELF), and Libraries (DLL and SO). ○ Movie (AVI and MPEG) ○ Web (HTML) ○ XML and SGML ○ Scripts and Batch Files ○ Command Files ○ Shortcuts (*.lnk etc) ○ Recycle Bin (INFO2 etc)

	<ul style="list-style-type: none"> • File Structures and Access Control Lists, including <ul style="list-style-type: none"> ○ Access Rights ○ Creation, modification and access times • Slack Space
--	--

3.4 Identification and Analysis of the Operating System

Demonstrate the ability to identify the host operating system, and operating artefacts.

ID	Description
K1	<p>The candidate MUST demonstrate the ability to identify the forensic target operating system. In particular:</p> <ul style="list-style-type: none"> • Host operating system and key operating system objects. • Hashing of disk and file system artefacts, in particular MD5/SHA1/SHA256.
K2	<p>The candidate MUST demonstrate an understanding of MS Windows and Unix operating system architectures. In particular:</p> <ul style="list-style-type: none"> • Key operating files • File Versioning and dependences • The MS Windows registry and key registry settings and access rights
K3	<p>The candidate MAY demonstrate an understanding of MS Windows and Unix networking architectures. In particular:</p> <ul style="list-style-type: none"> • Hostname and Host IP • Relationship between MAC address, Network Interface Card and IP Address • Subnet and routing information • Firewall configuration.
K5	<p>The candidate MAY demonstrate an understanding of alternate hashing methods.</p>
K6	<p>The candidate may demonstrate the ability to identify malicious software.</p>

3.5 Identification and Analysis of Applications and Software Artefacts

Demonstrate the ability to identify and analyse various software applications and associated artefacts.

ID	Description
L1	<p>The candidate MUST demonstrate the ability to identify software/applications located in the target system. In particular:</p>

	<ul style="list-style-type: none"> • Software/ Application configuration settings • Software/ Application Audit data • Software/ Application creation time • Software/ Application modified time • Software/ Application access time • Software licence keys • Pirated/illegal software
L2	<p>The candidate MUST demonstrate the ability to identify and analyse data from software/applications located in the target system relating to internet activity. In particular:</p> <ul style="list-style-type: none"> • Web browsers and their configuration • Web Servers and their configuration • Peer to Peer software and their configuration • Chat software and its configuration • VoIP software and its configuration • E-Mail systems (Web, IMAP, POP and SMTP) • Database Software • Office Applications (Word, PowerPoint etc). • Media Duplication (CD/DVD) • Video and Audio Applications • File/Application viewers

3.6 Identification and Analysis of Internet Activity

Demonstrate the ability to identify and analyse Internet activity relating to various clients and servers. In particular, the ability to identify and analyse Internet Activity relating to various web browsers and web servers.

ID	Description
M1	<p>The candidate MUST demonstrate the ability to identify software/applications located in the target system relating to internet activity. In particular:</p> <ul style="list-style-type: none"> • Web browsers and their configuration • Web Servers and their configuration • Peer to Peer software and their configuration • Chat software and its configuration • VoIP software and its configuration • E-Mail systems (Web, IMAP, POP and SMTP)
M2	The candidate MUST demonstrate the ability to identify and analyse internet history.
M3	The candidate MUST demonstrate the ability to identify and analyse data located in the target system relating to internet activity. In particular:

	<ul style="list-style-type: none"> • Web browsers and their configuration • Web Servers and their configuration • Peer to Peer software and their configuration • Chat software and its configuration • VoIP software and its configuration • E-Mail systems (Web, IMAP, POP and SMTP)
--	--

3.7 Identification and Analysis of Audit Data

Demonstrate the ability to identify, extract and document audit data that has been generated by a variety of operating systems and applications/services.

ID	Description
N1	<p>The candidate MUST demonstrate the ability to identify and analyse various generic audit data artefacts. In particular:</p> <ul style="list-style-type: none"> • Accounting information • System usage information (processes and files)
N5	<p>The candidate MAY demonstrate the ability to identify and analyse various MS Windows artefacts. In particular:</p> <ul style="list-style-type: none"> • TDI Monitoring • Network Monitoring • Registry Monitoring • File Access Monitoring • Object Access Monitoring
N6	<p>The candidate MUST demonstrate the ability to identify logs including email logs, web logs, etc.</p>
N8	<p>The candidate MUST demonstrate the ability to identify various MS Windows audit data artefacts. In particular:</p> <ul style="list-style-type: none"> • Application audit data such as service start and service termination. • System usage information such as process and user access (logon and logoff data) • Process creation and termination • File/Object access • DNS and replication audit data. • Service audit data such as ISS etc
N9	<p>The candidate MUST demonstrate the ability to identify Unix audit data artefacts. In particular:</p> <ul style="list-style-type: none"> • Application audit data • Relevant syslog data • Service audit data such as apache etc • User audit data such as logon/logoff

N10	The candidate MAY demonstrate the ability to monitor and analyse RAM using a variety of live memory tools.
-----	--

4 Deliverables

4.1 *Management Presentation of Results*

Demonstrate the ability to produce a written and verbal summary of security testing results to a non-technical audience.

ID	Description
O2	The candidate MUST be able to provide both a verbal and written summary of their actions, including problems encountered to people who are non-technical. Whilst it is appreciated that many forensic issues are by definition technical, the presentation of such information is often to non-technical individuals, such as a jury in the Crown Court.

4.2 *Technical Presentation of Results*

Demonstrate the ability to document and explain identified forensic issues identifying the issue, impact, risk and suitable recommendations.

ID	Description
P2	The candidate MUST be able to provide detailed information on images taken, or files obtained (such as logs). Such information is likely to include details of the issue, and recommended action(s) for remediation.