

# Tiger Digital Forensics - Certified Malware Analyst

<b>Title</b>	<b>Tiger Digital Forensics - Certified Malware Analyst</b>
<b>Version</b>	1.1
<b>Status</b>	Public Release
<b>Date</b>	21 <sup>st</sup> June 2011
<b>Author</b>	Professor Andrew Blyth (Tiger Technical Panel)
<b>Review Date</b>	1 <sup>st</sup> July 2012

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Changes and Comments</b>
0.1	10/09/10	Prof Andrew Blyth	Draft Version
0.2	20/09/10	Prof Andrew Blyth	Draft Version
1.0	22/10/10	Prof Andrew Blyth	Public Release
1.1	21/06/11	Prof Andrew Blyth	Public Release

## 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.....	6
2.5 Managing Risk.....	7
2.5 Malicious Software Analysis Methodology .....	8
2.6 Malicious Software Analysis Platform .....	8
3.0 Technical Expertise.....	10
3.1 Malicious Software Concepts.....	10
3.2 Operating Systems Concepts and Artefacts .....	10
3.3 File System and File Systems Artefacts.....	12
3.4 Networking and Network Analysis .....	12
3.5 Classification and Identification of Infection Strategies and Payloads	13
3.6 Classification and Identification of in-memory Infection Strategies ....	14
3.7 Defensive Techniques and Malicious Code Analysis.....	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 Malware Analyst (CMA)* level.
- 1.1.2 The Malware Analyst is expected to possess and have the ability to demonstrate a wide range of skills and knowledge associated with the analysis of malicious software.
- 1.1.3 The nature of the assessment for a Certified Malware Analyst is that of an assault course whereby the candidate is expected to discuss numerous aspects of a malware analysis and subsequently to demonstrate technical capability on a specially designed and maintained assault course.
- 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 Malware Analyst* 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 the analysis of malicious software, the planning and management of engagements, risk management throughout engagements, the use of a suitable analysis platform and compliance with current best practice guidance.
  - **Technical Expertise:** Demonstration of knowledge of, and ability to perform a certified malware analysis, including but not limited to physical considerations, analysis of artefacts and an understanding of the capabilities of operating systems and malicious software.
  - **Deliverables:** Demonstration of capability in the preparation and presentation of malware analytical results to both non-technical and technical audiences. In both instances the results will be documented providing a summary of the issue, an interpretation of the case along with relevant recommendations.
- 1.1.6 Aspects have been chosen in an attempt to ensure that the malware analysis requirements and concerns of industry are incorporated into the individual candidate evaluation process. The Certified Malware Analyst assault course is more than a simple assessment of technical skill and is designed to evaluate the candidate as a whole and their capabilities across the computer forensic spectrum.

1.1.7 The assessment for a Tiger Digital Forensics - *Certified Malware Analyst* (CMA) consists of four parts:

- A multiple choice assessment (1 Hour)
- A written examination (3 Hours)
- A practical assessment via an assault course (6 Hours)
- A viva (30 Minutes)

1.1.8 The Tiger Digital Forensics - *Certified Malware Analyst* (CMA) assault course is an assessment of technical skill and is designed to evaluate the candidate as a whole and their capabilities across the security-testing spectrum.

1.1.9 The pass marks for each element of the Tiger Digital Forensics - *Certified Malware Analyst* (CMA) assessment is 60% and a successful candidate must pass all components of assessment.

### 1.1.10 Summary of TIGER Scheme Malware Analyst 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 malware scenario.
	Defining scope	Demonstrate the ability to define a scope of a malicious software investigation given customer requirements, timeframes and any constraints.
	Legal issues	Demonstrate an appropriate knowledge of UK law and best practice potentially relevant to malware investigation in a variety of situations.
	Planning and Management	Demonstrate the ability to develop a project plan for a given malicious software 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 malware investigations such as disruption to service.
	Malicious Software Analysis Methodology	Demonstrate the adherence to a stated methodology for a given malicious software investigation requirement and defined scope.
	Malicious Software Analysis Platform	Demonstrate possession and use of a suitably well-maintained and configured investigation platform. Demonstrate awareness of existing and emerging technologies likely to have relevance to a malicious software investigation. In particular tools that are fit for purpose.
Technical Expertise	Malicious Software Concepts	Demonstrate understanding of how malicious software functions and the technologies/self-propagation-strategies upon which they rely.
	Operating Systems Concepts and Artefacts	Demonstrate understanding of operating architectures, structures and artefacts. Demonstrate an understanding of process and memory management.
	File System and File System Artefacts	Demonstrate an understanding of various files types (NTFS, FAT16, FAT32, etc). Demonstrate an understanding of how various file system artefacts are created and managed at the physical and logical levels. Demonstrate the ability to decode various file types and file structures such as EXE, ELF, DLL, SO, PDF etc.
	Networking and Network Analysis	Demonstrate the ability to capture and decode IPv4 and IPv6 network traffic so as to identify the activity of malicious software and reconstruction of documents and files sent across the network.
	Classification and Identification of Infection Strategies and Payload	Demonstrate the ability to identify various infection strategies and payloads. Demonstrate the ability to identify various techniques that an adversary might reasonably use to avoid detection. Demonstrate the ability to identify and reverse engineering a payload (e.g. packers)
	Classification and Identification of in-memory Infection Strategies	Demonstrate the ability capture and analyse live memory and process information. Demonstrate the ability to perform the classification and identification of in-memory infection.
	Defensive Techniques and Malicious Code Analysis	Demonstrate the ability to analyse malicious code with a view to the identification of defensive/mitigation strategies.
Deliverables	Management presentation of results	Demonstrate the ability to produce a written and verbal summary of the malicious software investigation results to a non-technical audience.
	Technical presentation of results	Demonstrate the ability to document and explain identified malware 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 malicious software scenario.

ID	Description
A1	The candidate MUST liaise effectively with the assessor who will provide a list of requirements and constraints for the malicious software 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 produce a suitable scope for the testing based on the requirements and constraints provided by the assessor during the 'understanding requirements' phase of the assault course.
B2	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.

### 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 of 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.
D5	The candidate MUST be able to demonstrate awareness of the agreements on any status update process throughout the forensic investigation (e.g. daily wash up meetings, immediate notification of high risk issues.)
D6	The candidate MUST 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 malicious software investigations such as disruption to service.

ID	Description
E1	The candidate MUST demonstrate awareness of the risks associated with malicious software investigations and the impact that they can have 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 malicious software investigations and the impact that they can have on customer systems; these may include unintentional disruption to systems and applications.
E3	The candidate MUST demonstrate awareness of the risks associated with malware 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 <b>MUST</b> 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 <b>MAY</b> 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 <b>MAY</b> 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 <b>MAY</b> 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 <b>MAY</b> demonstrate the ability to suggest strategies aimed at reducing risk throughout the test.

## 2.5 Malicious Software Analysis Methodology

Demonstrate understanding of and adherence to a stated malicious software analysis methodology for a given investigation requirement and defined scope.

ID	Description
F1	The candidate <b>MUST</b> , when asked throughout the malicious software investigation assault course; show how any activities performed or tools used are supported directly by their chosen methodology.

## 2.6 Malicious Software Analysis Platform

Demonstrate possession and use of a suitable well-maintained and configured malicious software analysis platform.

ID	Description
G1	The candidate <b>MUST</b> be in possession of a system that is suitable for performing malicious software analysis. The system may be configured

	<p>with any choice of software and operating system(s) however the following conditions must be met:</p>
--	--

- All commercial software **MUST** be suitably licensed
- Anti-virus software **SHOULD** be installed and configured in such a way so as to not disrupt the analysis process.
- Virtualisation software **SHOULD** be installed and configured in such a way so as to not contaminate non-virtual networks.

## 3.0 Technical Expertise

### 3.1 Malicious Software Concepts

Demonstrate an understanding of how malicious software functions and the technologies/self-propagation-strategies upon which they rely.

ID	Description
H1	The candidate MUST demonstrate an understanding of encryption and Hashing methods such as: <ul style="list-style-type: none"><li>• AES, DES and Triple DES</li><li>• MD5, SHA256 and SHA2</li></ul>
H2	The candidate MUST demonstrate an understanding of binders and file obfuscation and the role that they play in malicious software such as: <ul style="list-style-type: none"><li>• UPX, CEXE</li><li>• ASCrypt</li><li>• EXECryptor, Krypton, MEW</li><li>• PEBundle</li><li>• PECompact and PE Crypt 32</li><li>• PELOCK and PEpack</li><li>• PELite and SFX</li></ul>
H3	The candidate MUST demonstrate an understanding of exploits and the role they play in malicious software development.
H4	The candidate MUST demonstrate an understanding of the various common activities undertaken by malware, such as: <ul style="list-style-type: none"><li>• Beaconsing</li><li>• Downloading and executing further malicious code</li><li>• Capturing user data</li><li>• Data exfiltration</li><li>• Interactive sessions</li></ul>

### 3.2 Operating Systems Concepts and Artefacts

Demonstrate understanding of operating architectures, structures and artefacts. Demonstrate an understanding of process and memory management.

ID	Description
I1	The candidate MUST demonstrate an understanding of MS Windows and Unix operating system architectures. In particular: <ul style="list-style-type: none"><li>• Operating System Architectures</li><li>• Operating system file architecture and</li></ul>

	<p>structure</p> <ul style="list-style-type: none"> <li>• File Versioning and dependences</li> <li>• The Microsoft Windows registry and key registry settings and access rights.</li> <li>• Microsoft Windows Active directory, domains and LDAP.</li> </ul>
I2	<p>The candidate MAY demonstrate an understanding of MS Windows and Unix networking architectures. In particular:</p> <ul style="list-style-type: none"> <li>• Hostname and Host IP</li> <li>• Relationship between MAC address, Network Interface Card and IP Address</li> <li>• Subnet and routing information</li> <li>• Firewall configuration.</li> <li>• TCP Stack</li> </ul>
I3	<p>The candidate MAY demonstrate an understanding of key systems services such as:</p> <ul style="list-style-type: none"> <li>• HTTP, HTTPS and SSL/TLS</li> <li>• Windows Authentication and Password Systems</li> <li>• Telnet, FTP and SSH</li> <li>• NFS and SMB</li> <li>• WebDav and Enterprise Document Management Tools</li> <li>• LDAP and Active Directory</li> </ul>
I4	<p>The candidate MAY demonstrate the ability to identify and analyse various MS Windows/Unix artefacts. In particular:</p> <ul style="list-style-type: none"> <li>• TDI Monitoring</li> <li>• Network Monitoring</li> <li>• Registry Monitoring</li> <li>• File Access Monitoring</li> <li>• Object Access Monitoring</li> <li>• Process/Thread Creation/Destruction</li> <li>• Hooking</li> </ul>
I5	<p>The candidate MUST demonstrate the ability to identify and analyse various MS Windows/Unix audit data artefacts. In particular:</p> <ul style="list-style-type: none"> <li>• Application audit data such as service start and service termination.</li> <li>• System usage information such as process and user access (logon and logoff data)</li> <li>• Process creation and termination</li> <li>• File/Object access</li> <li>• DNS and replication audit data.</li> <li>• Service audit data such as ISS etc</li> </ul>

### 3.3 File System and File Systems Artefacts

Demonstrate an understanding of various files types (NTFS, FAT16, FAT32, etc). Demonstrate an understanding of how various file system artefacts are created and managed at the physical and logical levels. Demonstrate the ability to decode various file types and file structures such as EXE, ELF, DLL, SO, PDF etc.

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

### 3.4 Networking and Network Analysis

Demonstrate the ability to capture, decode and analyse IPV4 and IPV6 network traffic so as to identify the activity of malicious software.

ID	Description
K1	<p>The candidate MUST demonstrate an understanding of networking. In particular:</p> <ul style="list-style-type: none"><li>• The packet structure of IPV4 and IPV6 and the ability to decode/deconstruct IPV4 and IPV6</li><li>• Network Devices such as Routers and Firewalls, and their associated ACL.</li><li>• Packet capture tools and packet replay</li></ul>

	<p>tools</p> <ul style="list-style-type: none"> <li>• Networking security protocols such as IPSec, Kerberos, SSH, SSL and TLS.</li> <li>• Routing and routing protocols such as RIP, OSPF, EGP, BGP etc.</li> <li>• The ability to decode application level protocols such as HTTP, FTP and Telnet, etc.</li> <li>• The ability to decode context specific traffic (e.g. PDF files, e-mail reconstruction etc.)</li> </ul>
K2	<p>The candidate MUST demonstrate the ability to:</p> <ul style="list-style-type: none"> <li>• Monitor a TCP/IP network and filter/capture network traffic.</li> </ul>
K2	<p>The candidate MUST demonstrate the ability to derive and analyse payload data from captured network traffic so as to identify:</p> <ul style="list-style-type: none"> <li>• The communication/control methods used by malicious software;</li> <li>• The infection/replication methods used by malicious software;</li> <li>• Network layer indicators of compromised that could be used to identify malicious software elsewhere;</li> <li>• Systems that have been infected by malicious software.</li> </ul>

### **3.5 Classification and Identification of Infection Strategies and Payloads**

Demonstrate the ability to identify various infection strategies and payloads. Demonstrate the ability to identify various techniques that an adversary might reasonably use to avoid detection. Demonstrate the ability to identify and reverse engineer a payload.

<b>ID</b>	<b>Description</b>
L1	<p>The candidate MUST demonstrate the ability to identify and analyse various propagation methods. In particular:</p> <ul style="list-style-type: none"> <li>• Target locator</li> <li>• E-Mail and SMTP</li> <li>• Executable code based</li> <li>• HTML based</li> <li>• HTTP/S URL link based</li> <li>• Code injection</li> <li>• Shell-code based</li> </ul>
L2	<p>The candidate MUST demonstrate the ability to identify and analyse various payloads. In particular:</p> <ul style="list-style-type: none"> <li>• Destructive and non-destructive</li> </ul>

	<ul style="list-style-type: none"> <li>• DOS and Botnets</li> <li>• Data Stealers</li> </ul>
--	--

### 3.6 **Classification and Identification of in-memory Infection Strategies**

Demonstrate the ability capture and analyse live memory and process information. Demonstrate the ability to perform the classification and identification of in-memory infection.

ID	Description
M1	<p>The candidate MUST demonstrate the ability to capture and analyse live memory and process information. In particular:</p> <ul style="list-style-type: none"> <li>• Virtual address spaces and Virtual memory system</li> <li>• Memory scanning and capture methods</li> <li>• Memory scanning and paging</li> <li>• Memory disinfection</li> <li>• Memory scanning in kernel mode</li> </ul>
M2	<p>The candidate MUST demonstrate the ability to perform the classification and identification of in-memory infection. In particular:</p> <ul style="list-style-type: none"> <li>• Identification of memory structures in memory</li> <li>• Identification of process structures in memory</li> <li>• Identification of networking structures in memory</li> <li>• Identification of registry structures in memory</li> <li>• The ability to decode/reverse engineering the following: <ul style="list-style-type: none"> <li>○ Memory/page structures</li> <li>○ Process structures</li> <li>○ Networking structures</li> <li>○ Registry structures</li> <li>○ IDT and SST structures</li> <li>○ TDI structures</li> </ul> </li> </ul>

### 3.7 **Defensive Techniques and Malicious Code Analysis**

Demonstrate the ability to analyse malicious code with a view to the identification of defensive/mitigation strategies.

ID	Description
N1	<p>The candidate MUST demonstrate the ability to analyse malicious code with a view to the identification of defensive/mitigation strategies. In particular:</p>

	<ul style="list-style-type: none"> <li>• Network defensive strategies</li> <li>• Honey-pots</li> <li>• Process protection</li> <li>• Memory protection</li> <li>• Heuristic and Behavioural analysis</li> <li>• Simulation and Virtualisation</li> </ul>
N2	<p>The candidate MUST demonstrate the ability to reverse engineer malicious code. In particular:</p> <ul style="list-style-type: none"> <li>• Static Analysis</li> <li>• Text/String Analysis</li> <li>• Dynamic Analysis</li> <li>• Dependency Identify</li> <li>• Functional Analysis</li> <li>• File Type/Structure Analysis</li> <li>• Registry use analysis</li> <li>• Decrypting</li> <li>• Fuzzing</li> <li>• Dynamic analysis techniques</li> </ul>
N3	<p>The candidate MUST demonstrate the ability to identify when a machine has been infected and to recommend strategies for removal and techniques to mitigate future infection.</p>

## 4 Deliverables

### 4.1 *Management Presentation of Results*

Demonstrate the ability to produce a written and verbal summary of malicious software analysis results to a non-technical audience.

ID	Description
O1	The candidate <b>MUST</b> be able to provide both a verbal and written summary of a malware investigation to customers who are non-technical. Whilst it is appreciated that many malware issues are by definition technical, the presentation of such information is often to non-technical individuals.

### 4.2 *Technical Presentation of Results*

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

ID	Description
P1	The candidate <b>MUST</b> be able to provide detailed information on identified malware issues to the customers. Such information is likely to include a list of affected components, details of the malicious code, how it works, how to detect it and recommended action(s) for remediation.