First Responder Guide

Published by	Portcullis Computer Security Limited
	The Grange Barn, Pike's End Pinner, Middlesex, HA5 2EX
Tel	+44 (0) 20 88 68 00 98
Fax	+44 (0) 20 88 68 00 17
Web	www.portcullis-security.com
Email	enquiries@portcullis-security.com

CONTENTS

Disclaimer

Whilst Portcullis Computer Security Limited has taken great care in the preparation of this document and the advice contained in it is informed by intelligence of the threat. Portcullis Computer Security Limited does not provide any warranty as to the accuracy or completeness of the document and accept no liability for any financial loss or damage arising from the use of this document or the advice it contains.

1 Introduction

Portcullis provides a comprehensive end-to-end incident response service and is ideally placed to fully manage any security incident. In addition to taking the lead on incidents, Portcullis can integrate with existing client incident response teams to provide skills, expertise and man-power, even at short notice. The purpose of this document is to provide guidance on both a technical and practical level to those employees or individuals likely to act as the First Responder in the event of a security incident. Much of this guidance draws on the Portcullis Cyber Threat Analysis and Detection Service (CTADS) incident response methodology.

This document focuses on providing suggested initial actions to be taken in response to any IT security incident to ensure that:

- No evidence, or potential evidence, is contaminated
- The incident is contained
- The impact of the incident on the business is minimised
- Further infection of the network or networks is prevented
- The organisation's reputation is preserved

In the event of a security incident it is important that the First Responder considers the need to maintain the availability and integrity of evidence. Due consideration should be given to how planned actions or system changes may impact this.

Associated Documentation

This document is intended to complement existing internal documentation relating to security incident investigations; these documents can be recorded below:

Document Name	Description	Location	Owned By
Example: *IT security incident response plan*	*Document detailing the process for handling IT security incidents*	*Electronic: \\network drive\incident response* *Hard copy: Room 7.1, filing cabinet C*	*A. N. Other* *Security Manager*

2 Preparation

"Forensic Readiness is the achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse Digital Evidence so that this evidence can be affectively used in any legal matters, in disciplinary matter, in an employment tribunal or in a court of law."

CESG, Good Practise Guide No. 18, Forensic Readiness 2011

Planning and fully preparing for the occurrence of security incidents is vitally important if organisations wish to handle such events efficiently and effectively. Organisations that handle security incidents well find the impact of such events much reduced compared to the lesser prepared organisation. Portcullis offers a security incident response planning service, specifically tailored to lead an organisation through the incident response process. This section outlines the necessary technical and practical considerations that should be considered in advance of an incident response engagement, as well as guidance for the First Responder on the applicable legal aspects, practical tool sets, process and procedures.

2.1 Appointing an IT Security First Responder Team

A First Responder Team should include individuals with specific skill sets or roles, as outlined below. It should be noted that it is not uncommon for both of these defined roles to be assigned to one individual.

2.1.1 Incident Coordinator

An incident will often impact a number of internal departments and sometimes external parties as well (supply chain, business partners, etc). To ensure that the incident response is correctly managed across multiple parties, it is vital to appoint an incident coordinator. The incident coordinator is responsible for ensuring that all parties are communicating effectively and that each is sufficiently informed to enable them to perform his/her role successfully.

The incident coordinator will, based on the initial characteristics of the incident, classify the type of incident (detailed in section 2.4) that has occurred and decide the actions required from the First Responder Team. He/she will also decide at what point assistance from specialist external suppliers is required.

2.1.2 First Responder

Once a security incident has been reported to the security team, members of the First Responder Team should be tasked with expediting the technical activities required, as outlined in later sections of this document. It is vital that these individuals possess the necessary knowledge and training to enable them to contain the incident and secure the relevant data sources in an evidentially sound manner (ensuring that the integrity of each data source is protected in order that it can be produced as evidence later).

2.2 Law

All members of the First Responder Team should be familiar with the relevant legislation in advance of participating in any incident response. This includes, but is not limited to, materials referenced in the Association of Chief Police Officers (ACPO) Guidelines on Computer Evidence:

Regulation of Investigatory Powers 2000 (RIPA)

http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

Official Secrets Act 1989

http://www.opsi.gov.uk/acts/acts1989/ukpga_19890006_en_1

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Computer Misuse Act 1990

http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.opsi.gov.uk/si/si2000/20002699.htm

2.3 Handling Computer Investigations and Electronic Evidence – ACPO Guidelines

All members of the First Responder Team must adhere to and be aware of the ACPO guidelines cited below:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In exceptional 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 give evidence explaining the relevance and the implications of their actions.

Principle 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.

Principle 4: The incident coordinator has overall responsibility for ensuring that the law and these principles are adhered to.

Principle Explanations

In a legal sense, computer-based electronic evidence is no different to text contained within a document and for this reason is subject to the same laws applicable to documentary evidence. The doctrine of the integrity of documentary evidence may be explained thus: *The onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of police.*

2.3.1 Adhering to ACPO Guidelines

In order to comply with the principles of computer-based electronic evidence, wherever practicable, a forensic image should be made of the target device in its entirety. Partial or selective file imaging may be considered as an alternative in certain circumstances (for example when the amount of data to be imaged renders this impractical), however, forensic principles must be adhered to whenever and wherever possible and forensic software, such as 'FTK Imager' or 'EnCase Portable', should be used.

Note: In a minority of cases it may not be possible to obtain an image using a recognised imaging device and in such circumstances it may become necessary for the original machine to be accessed to recover the evidence. In such a scenario it is essential that an impartial specialist is engaged to complete this activity and he/she must also be prepared to give evidence in a court of law regarding their activities. Such an expert would be expected to demonstrate objectively to a court both continuity and integrity of evidence, including significant detail on how the evidence was recovered. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result.

2.4 Incident Categories

It is recommended that an internal risk assessment classification matrix of assets is created and correlated with the incident categories specified below.

The category classification (rating) assigned to any security incident should dictate the internal (and potentially external) resources to be coordinated, the communication channels and escalation procedures that the incident coordinator will manage during the incident response. The following categories defined by CESG are useful as a point of reference:

Rating	Description
Critical	These incidents will usually cause the degradation of vital service(s) for a large number of users, involve a serious breach of network security, affect mission-critical equipment or services, or damage public confidence in the organisation. E.g. targeted attacks or loss of publicly available online service.
Significant	Less serious events are likely to impact a smaller group of users, disrupt non-essential services and breaches of network security policy. E.g. website defacement or damaging unauthorised changes to a system.
Minor	Many types of incident can be capably handled by internal IT support and security. All events should be reported back to the information security team who will track all occurrences of similar events. This will further the understanding of the IT security challenges and may raise awareness of new attacks. E.g. unsuccessful denial-of-service attack or the majority of network monitoring alerts.
Negligible	It is not necessary to report on incidents of limited impact or those affecting only a few users. This sort of event would include receipt of isolated spam or anti-virus alerts, minor computer hardware failure, loss of network connectivity to a peripheral device such as a printer, or loss of access to an external non-essential service. In general these would be considered to be part of normal IT support operations or can be dealt with by local installed intrusion prevention systems. E.g. isolated anti-virus alert or spam email.

2.5 Communication and Escalation Policies

During the initial stages of any response the incident coordinator will be responsible for reporting the incident to appropriate parties and maintaining contact. Based on the classification of the incident the appropriate escalation policies will be predefined. The First Responder must, therefore, have access to the following:

- Details of external agencies and resources to contact
- An overview of roles and responsibilities including a 'call tree' of contact details
- A list of escalation procedures appropriate to the type of incident and timescales

2.6 Devices - Overview and Considerations

Having a thorough understanding of the IT equipment likely to be compromised and, therefore, included in an investigation is extremely important at the planning stage. A comprehensive checklist should be created to assist in determining the 'computers of interest' including technical and business related information relating to those servers.

A First Responder should identify the type or types of computer systems most likely to be encountered within the environment that their planning relates to. They will also need to plan for the types of digital media they will encounter (CD/DVD, USB memory stick, memory card, external hard drive, etc). Note that devices such as iPods and satellite navigation devices can also store data so may also require forensic imaging and examination.

In large organisations and government departments combinations of laptops, desktops, tower and rack mount systems are used, often comprising numerous makes and models. Operating systems tend to be Microsoft Windows and / or Linux (or other UNIX derivatives). Thorough and detailed planning is imperative in such scenarios as a rack of computer systems can contain a huge number of individual components and drives.

Other considerations at the planning stage include the possible existence of 'RAID' arrays, which will need to be reconstructed after the image has been obtained before a proper analysis can be carried out. It should also be noted that in most cases 'live' imaging (detailed in 3.2.9) will be necessary to minimise the impact on client business operations.

2.6.1 First Responder Tool Kit

This kit is a collection of tools that must be available to the First Responder when a security incident occurs. The first stages of an engagement are the most important and time critical and it is vital that time is lost in setting up and finding the required tools. The following items are required:

Essentials:

- Logbook and pen
- Imaging laptops
- Live imaging tools (EnCase Portable, FTK, Helix, Raptor, Linen, etc)
- Cross-over cable
- Disks for image storage (encrypted)
- Evidence labels (tie-on and adhesive)

- Evidence bags
- Anti-static bags and bubble-wrap
- Digital camera / video
- List of experts, suppliers and legal resources
- Emergency telephone numbers and mobile phone
- Contact details for 3rd party specialist resources
- Contact details for internal specialist resources

Additional equipment:

- Property / evidence register
- Indelible markers
- Mobile phone evidence boxes
- Evidence tape
- Packaging material and boxes
- Gloves
- Torch
- Unused media (CDs, DVDs, floppy disks)
- Cable tags
- Faraday bags
- Cable ties

Tool kit:

- Anti-static mat and attached wristband
- Screwdrivers (flat blade, Phillips and torx)
- Allen keys / hex-nut screwdrivers
- Needle-nose and standard pliers
- A screwdriver for tamper-proof screws
- Tweezers and wire-cutters
- Specialised screwdrivers (manufacturer specific)

Write Blockers (as minimum):

- SATA
- PATA
- SCSI – All variants
- ZIF
- Compact Flash and all other digital media
- USB bridge

2.7 Logging

In order to successfully detect and track security incidents in any organisation the following audit types are strongly recommended:

- Detailed firewall/router logs
- Detailed logs for all proxy servers
- Detailed DNS logs
- DHCP logs covering all devices
- Detailed access logs for all critical servers
- Detailed email logs
- Web server logs (if applicable)

Note: It is recommended that logs are kept for as long as possible and at least for a minimum of 6 months. During an investigation these logs will provide valuable information and are often requested by third parties. Failure to ensure that the above logging is in place may have a detrimental effect on the investigation.

3 First Response

This section covers the hands-on initial response to a security incident and presumes that the organisation has been alerted to its existence either via an internal investigation or a trusted service provider. The information provided at the time of the alert should be passed to the First Responder Team who will begin to coordinate their approach. Several initial questions should be answered to ensure that the correct approach is be taken:

Q. Do we have the necessary skill set to deal with this incident?

A. Refer to section 3.2.2 Resources

Q. Is it likely this incident will escalate to a legal court case?

A. Refer to section 3.2.2 Resources

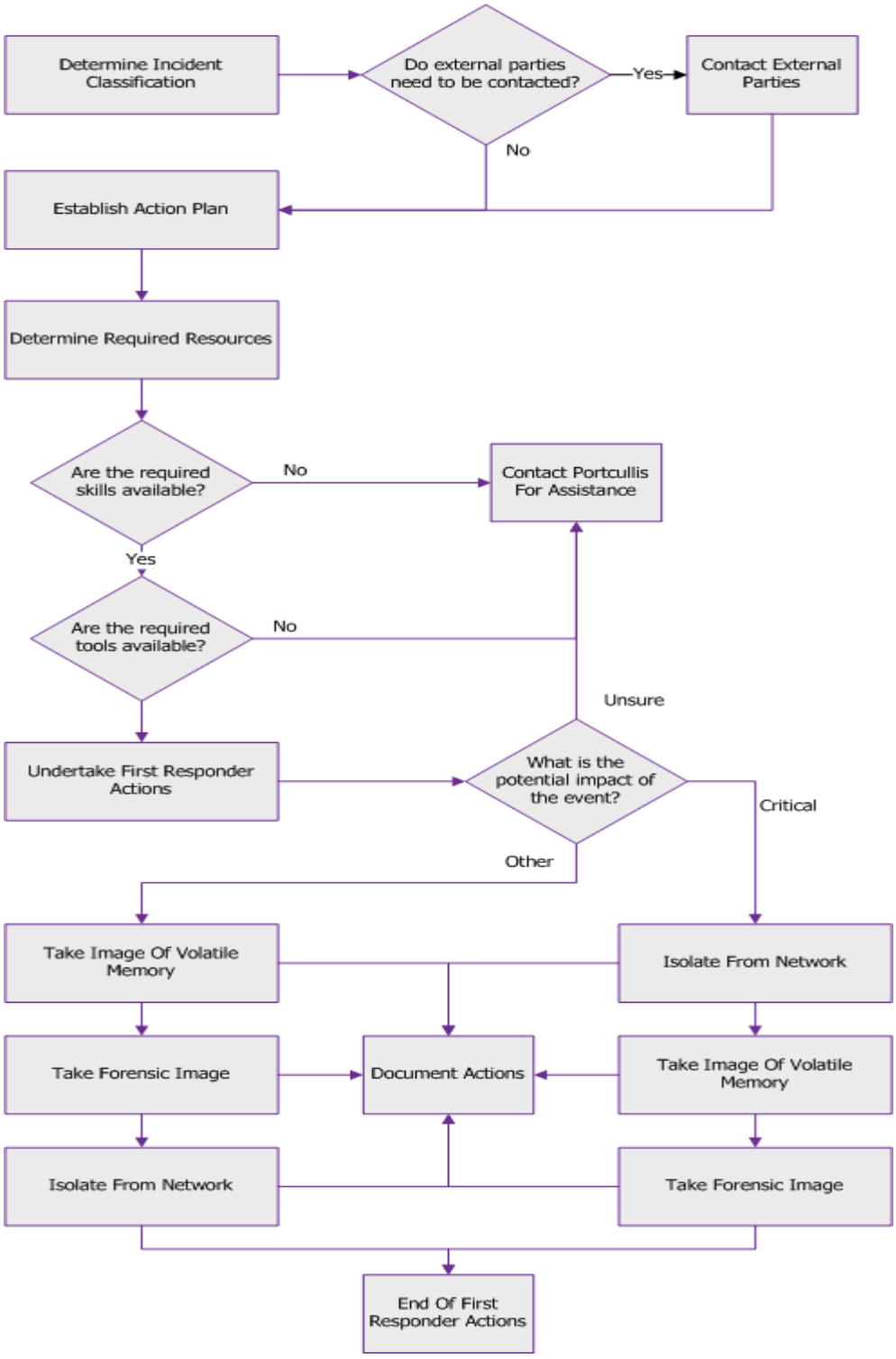
Q. Do we have the necessary equipment to deal with this incident?

A. Refer to section 3.2.3 Tools

Portcullis is able to provide specialist, end-to-end incident response and incident management services in the event that the answer to any of the above questions is 'No'.

3.1 Overview

The flowchart below provides a visual representation of the steps applicable to First Response and how they interrelate.



3.2 First Response Action Plan

Based on the security incident classification (see earlier) a First Responder will address the incident and establish the required tool kit.

3.2.1 Verification of Ownership

The First Responder should ensure that ownership of the target device(s) is established. Prior written authorisation or confirmation that the client owns the device(s) and is authorised to permit access to them is required from a duly-appointed representative prior to any interaction with the device or devices in question.

3.2.2 Resources

Upon categorisation of the security incident (2.4), it is important to ensure that the appropriate resources are made available, as discussed below. Relevant contact details for example should be readily available in the response tool kit.

Specialist Resources

The First Responder Team should determine whether any specialist resources will be required (contact details should be part of the response toolkit) either during or after the investigation, which may include:

- Technology forensics specialists
- Technology analysts (for example, database experts)
- Information analysts (for example, accountants)
- Legal support
- Psychological support
- On-site police support

Internal Resources

The First Responder Team should determine how many internal resources will be required by considering the following factors:

- Whether equipment is to be seized and reviewed remotely or whether work will be conducted in situ
- How much equipment will be seized
- Evaluate the number of staff that will be required to handle the incident
- Whether staff will be required as back-up or witnesses
- Whether resources have the requisite skills / qualifications or are appropriate to the task
- The physical location and health-and-safety aspects of the job
- Will each resource be required and / or available for the entirety of the project?

Should the internal resources fall short of the requirements for handling the incident, Portcullis can assist in all area and stages of the handling of an incident.

3.2.3 Tools

Determining whether specialist tools will be required during the investigation is also important and can be ascertained via the following considerations:

- If specialist equipment or the use of a sub-contractor is required, will this impact the investigation timescales?
- Are the resources available within the first response tool kit sufficient or will they need to be supplemented?
- Will there be sufficient usable resources available during the investigation?
- Are tools such as videos, cameras and phones working and fully charged and do they have sufficient storage?

3.2.4 Documentation

The first response handlers will need to keep a written record of every action undertaken as part of the investigation, which should be saved with the case file on a server and alongside any evidence files. The advantage of this methodical process is that clear and precise evidence can be referred to at a later date and the sequence of events and actions taken by the analyst can be repeated by opposition experts if required. Once the investigation is complete, or upon the handover to the investigation team, offsite back-up of all electronic files pertaining to the investigation is recommended.

Note: Media and System Imaging forms are included in this document and should be completed for each item submitted or imaged. Live imaging details should be recorded on the Live Imaging form.

3.2.5 Golden Rules

The First Responder Team may well encounter stressful situations during which it may seem appropriate to forego certain established procedures or predefined guidelines. However, such short-cuts can have considerable consequences later in the engagement and all efforts should be taken to follow the defined process. Portcullis strongly recommend adhering to the following guidance above all others:

- Ensure contemporaneous notes (either electronic or paper) are kept of all decisions made and actions taken
- If any system under investigation is still 'powered up' DO NOT turn it off until an expert decision on the risk of doing so has been made
- DO NOT perform analysis on a live system under investigation before a forensically safe image has been taken
- Ongoing consideration should be given to the need to use external resources; such as a security specialist, law enforcement agent or legal advisor

3.2.6 Forensic Image Acquisition Process

This phase of the assessment is to an extent governed by the classification of the incident and internal decisions regarding the nature of the investigation required. However, Portcullis' normal approach is to perform a forensic memory acquisition as well as an online acquisition of the underlying system, as this provides a snapshot of the system as it was at the time the incident was initially responded to. Offline forensic analysis is the least preferred option as evidence from running processes may be lost.

Where dealing with advanced malware, it should be noted that making changes to the filesystem or network will often trigger a fail-safe within the malware, which will in turn remove itself together with the evidence of infection.

In the event of there being insufficient time to acquire a full system image, Portcullis would recommend that as a minimum, the following files and folders should be forensically imaged:

- System folder (e.g. C:\windows)
- Users home directory (e.g. C:\Documents and Settings\, C:\Users\)
- Temporary files
- Pagefile

3.2.7 Evidence Handling

It is imperative that a chain of evidence is established. All exhibits should be identified with a unique exhibit number and, where possible, tagged and sealed in a dedicated, labelled, evidence bag. The format for exhibit numbering should adhere to the following conventions:

- First three letters of the project or client name (e.g. 'Project Flash' = FLA)
- First three letters of the imaging location (e.g. London = LON)
- Unique numbering starting logically at '001'

So, for example, the exhibits for 'Project Flash' imaged in London will be marked: FLA-LON-001, 002, etc. Should further exhibits for 'Project Flash' be seized or imaged at a different location (for example, Slough), then the exhibits will be marked: FLA-SLO-001, 002, etc.

Evidence bags should be used for all exhibits. The continuity panels on the bags should always be completed and all evidence stored in a secure, locked, location. When the evidence is handed over to the Investigation Team a Property Receipt Form should be completed.

To avoid any confusion, a record of all abbreviations used in the labelling system should be documented and kept in the investigation notes.

3.2.8 Forensically Imaging Volatile Memory

The processing of live memory images is vital in identifying malware. Given the relative ease of conducting this activity it should be completed for all engagements. It should also be conducted as the first imaging task, without any other changes being made to the underlying system or removal from its original network. Modern malware is sensitive to changes in system state and may delete all traces of itself, hence the requirement to take the live memory image at the first opportunity.

During the course of subsequent analysis the images taken from volatile memory will reveal vital information regarding the infection and the system at the time of the acquisition, including:

- Running processes
- Keyword matching
- System call tables (IDT, GDT, SSDT)
- API hooks in user and kernel mode (inline, IAT, EAT, NT syscall, winsock)
- List of all open network connections and open sockets (with associated process IDs)
- Open handles to all kernel/executive objects
- Memory maps of each process
- Root kit analysis

Note: The following suggested toolsets can act as independent software packages and do not require installation, keeping the changes to the memory and file system to a minimum.

Windows

Suggested software: FTK imager Lite

URL: http://www.accessdata.com/support/product-downloads

Filename: FTK Imager Lite version 2.9.0

Unix/Linux

Suggested software: dcfldd, sdd, dd_rescue, ddrescue, dccidd

3.2.9 Forensically Imaging The Underlying System

The image of the target hard drive and memory contents should be acquired as per the ACPO guidelines for computer-based electronic evidence. This requires all forensic examiners to produce electronic evidence that is the same as when it was first taken into the forensic examiner's possession (for example, the data was acquired securely using an accredited write-protecting device, or was acquired 'live' by using previously approved methods, namely EnCase portable, FTK Imager, Helix, etc).

No hard drive or digital media should be directly connected to a forensic workstation. The examiner must be prepared for every eventuality with regard to type and size of storage device, and considerations here include:

- Notation of target system
- Recording every step from disconnecting the system to its reconnection
- Recording details of the target device or devices, peripherals and attached cables and their respective locations
- Photographing or videoing the system in situ
- Recording the system type, model and serial number, and whether it has any distinguishing marks, features or security devices
- Identifying how many hard drives there are and their types and models
- Identifying the serial numbers and storage types
- Labelling and bagging (or tagging) upon acquisition
- Entering details into an exhibit log

Forensic Online Imaging

It is recommenced that, wherever possible, analysis of an infected machine is performed while it is running, after first creating both live memory and disk images.

Live analysis has a number of advantages over offline analysis:

> Active malware often unpacks many of its components for use and live host analysis permits access to these.
>
> Compared to offline analysis, it reduces the time necessary to reverse engineer the code.

Links to droppers (a program that is designed to install malware to a target system) and other useful indicators are often left intact whilst the code is resident; these attributes often reduce the time needed to understand the malware and greatly improve the reverse engineering process.

Note: Although there are techniques and toolsets available for booting up a forensic image into a virtual environment for further analysis, these techniques should not be relied on to work in every scenario and can be time consuming.

Forensic Offline Imaging

When imaging a hard disk that has been removed from the host system, the device must be attached to a forensically secure write-blocking device. Only imaging software or devices approved for this purpose (FTK Imager, EnCase, Helix, SOLO3, etc) should be used. Other software or devices must be thoroughly tested and verified against existing tools prior to use. Once the testing has been successfully carried out then a request for inclusion can be submitted to the incident coordinator. Once a decision is made to turn off a compromised machine, unplug the network lead or remove the battery, the only remaining options are to either remove the hard drive and mount it as read-only or make use of a software/hardware write-blocker in order to capture the image. The alternative is to boot up the affected machine with a forensically safe boot disk and create a forensically safe image with the installed tools on an external hard drive or in a network location.

3.3 Containment

One of the key activities during the initial incident response is the containment of the compromise. This should be a priority task in the process on the proviso that primary sources of evidence are not corrupted.

The containment phase will comprise a number of tactical short-term actions aimed at reducing the immediate impact of the incident, primarily by severing the threat actor's access to the client's network. On systems of low operational value, this can include rudimentary actions such as simply unplugging equipment, whereas on systems of a higher operational value it may be more appropriate to increase the security controls to pare back access to the bare minimum of services and increase monitoring. Such restrictions need only be in place until such time as it is possible to confidently restore services that are demonstrably clean and no longer vulnerable.

With the key aim of reducing the impact, this phase can be implemented before the threat of the incident has been fully verified. For example, if a system is of high operational value or contains sensitive data then it may be appropriate to contain it as a matter of course.

3.3.1 Isolating the device from network

Removing an affected device from the network is a critical first step and should be undertaken once forensic imaging of the memory contents is complete and the network capture has been performed (should this have been opted for).

- **Unplug the compromised device(s) from network**
  This can be achieved by unplugging the network cable(s) from the device(s).
- **Block and log offending traffic regarding the affected machine(s)**
  When an incident is reported, connections to known malicious IP addresses are often relevant. In dealing with a business-critical server that cannot be removed from the network, blocking and logging offending traffic streams in the access control list of an external firewall should be considered.
- **Block and log all traffic flows regarding the affected machine(s)**
  Blocking and dropping all traffic from the affected system is achieved by disabling the relevant port on the local switch. If this is not possible, for example due to virtualisation or routing equipment restrictions, dropping all traffic from the device IP Address is a suggested alternative.
- **Isolate affected machine(s) on separate network**
  A further solution is to create a separate private vlan, isolated from all other internal networks in order to prevent the malware from spreading.
- **Isolate in virtualised environments**
  When dealing with security incidents in virtual environments, isolation can be achieved by disconnecting or unplugging the network cable via the provided management software.

4 Analysis Form - Media Acquisition Details

Case Reference:		**Case Name:**			
Date:		**Image Ref No:**		**Imaging Location:**	
Media Information					
Make:		**Model:**			
Serial:		**Size on Label:**			
Device Type:		**Size In S/Ware:**			
No Sectors on Label:		**Size Match:** Yes/No			
No Sectors in S/Ware:					
Imaging Details					
Software/Method Used:		**Software Version:**			
Time Started:		**Time Finished:**			
Acquisition Hash:		**Verification Hash Match?**	Yes/No		
Image Path:					
Image Type:	Physical Device or Logical Evidence File etc:				
Other Info:					
Destination HDD Information					
Disk1	**File System***	**FAT**	**FAT32**	**NTFS**	**Other:**
Make:		**Model:**			
Serial:		**Size:**			
Form Completion			**QA**		
Name:			**Name:**		
Signature:			**Signature:**		
Date/Time:			**Date/Time:**		

5 Analysis Form – System

Case Reference:		Case Name:	

Date:		Custodian Name:	
Location of Acquisition/Discovery			
System Details			
Type: *	Server	Laptop	Desktop	Other:
Make:		**Model:**	
Serial:		**Additional Info:**	

RAID Config?	Level		Stripe Size:	

BIOS:	Date:		Time:		Reference:	
Daylight Saving:	Yes/No*	**Local Time Diff to GMT:**	+/_ Hours:			

Evidence Bags Signed?	YES / NO*	Seal No:	

Any Passwords or Encryption Used?	YES / NO*
(if yes then please state Type/passwords and how used.)	
Was The Equipment Switched on at Time of Acquisition?	**YES / NO***
Graceful Shutdown Power Pulled Time: Date: (If Yes Then Please State How Equipment Was Switched Off and Secured)	

Has The Equipment Been Switched on After Acquisition?	YES / NO*
(If Yes Then Please State Reason & Details of The Person)	
Photographs:	Yes No

Form Completion
Name:
Signature:
Date:

QA
Name:
Signature:
Date:

6 Live Acquisition Form

Case Name:		**Image Reference:**	
Date:		**Custodian Name:**	
Location of Acquisition/Discovery			
System Details			
Type: *	Server	Laptop	Desktop	Other:
Make:		**Model:**	
Serial:		**Additional Info:**	
Media Details			
Make:		**Model:**		**Serial:**	
Size on Label:		**LBA (Sectors):**		**Size Match in Software?**	**y/n**
Physical or Logical Image?		**If Physical: Disk Size**		**Logical: Partition Size**	
Acquisition Details					
Acquisition Started:		**Acquisition Completed:**	
Acquisition Hash:		**Values Match:**	**Yes/No**
Software used:	EnCase FTK Helix Other :				
Version used:		**Compression Level:**		**Acquisition Path:**	

Destination Drive			
Ser No:		**Name:**	
Size:		**File System:**	
Other Notes			
(Encryption etc)			
Evidence Bag seal No:			

Form Completion	**QA**
Name:	**Name:**
Signature:	**Signature:**
Date/Time:	**Date/Time:**

7 Evidence Movement Log

Case Number:		**Case Name:**	
Date:		**Time:**	
Released By:	(Name)	(Signature)	
Received By:	(Name)	(Signature)	
Purpose of Change of Custody			
Date:		**Time:**	
Released By:	(Name)	(Signature)	
Received By:	(Name)	(Signature)	
Purpose of Change of Custody			
Date:		**Time:**	
Released By:	(Name)	(Signature)	
Received By:	(Name)	(Signature)	
Purpose of Change of Custody			
Page		**OF**	

8 Property Receipt Form

A. Description of Items

Description	Seal Number

B. Statement of Receipt

I acknowledge receipt on behalf of _____ that the above items were received from _____ on _____

C. Delivery Signatures

Person Receiving Item	
Signed:	
Print Name:	
Company:	
Position:	
Date:	
Time:	

Person Releasing Items	
Signed:	
Print Name:	
Company:	
Position:	
Date:	
Time:	