**YOUR LOGO HERE**

**Digital Forensics and Incident Response**

**Technical Manual**

**DOCUMENT CONTROL #**

**CLASSIFICATION LEVEL HERE**

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) exemption number and category: **7, Law Enforcement**

**Department of Name of Agency review required before public release**

Name/Org: Your name/org Date:

Guidance (if applicable):

**Record of Changes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Pages Affected | Description | Author/Editor |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**TABLE OF CONTENTS**

[1. Purpose](#Purpose)5

[2. Scope](#Scope)5

[3. Roles and Responsibilities](#Roles_and_Responsibilities)5

[4. Requirements](#Requirements)6

[Forensic Sterilization of Loose Media Procedure](#Forensic_Steriliziation_of_Loose_Media)7

[Forensic Sterilization of Active Files Procedure](#Forensic_Steriliziation_of_Active_Files)9

[Target Drive Preparation Procedure – Loose Media](#Target_Drive_Preparation_Loose_Media)10

[Target Drive Preparation Procedure – Network Storage](#Target_Drive_Preparation_Network_Storage)12

[Hard Drive Removal Procedure](#Hard_Drive_Removal_Procedure)13

[Forensic Imaging Procedure – Windows Based](#Forensic_Imaging_Procedure)15

[Forensic Imaging Procedure – Linux Based (Using a Forensic Computer)](#Forensic_Imaging_Procedure_Linux_NH)17

[Forensic Imaging Procedure – Linux Based (Using the Original Host)](#Forensic_Imaging_Procedure_Linux_H)19

[Forensic Preview Procedure – Windows](#Forensic_Preview_Procedure_Windows)21

[Forensic Preview Procedure – Linux](#Forensic_Preview_Procedure_Linux)23

[Evidence Search Procedure](#Evidence_Search_Procedure)25

[Acquisition of Live Memory (RAM) – Non Network Acquisition Procedure](#Acquisition_of_RAM_non_network)28

[Acquisition of Live Memory (RAM) – Network Acquisition Procedure using Encase](#Acquisition_of_RAM_network)30

[Acquiring a Logical Forensic Image of a Running System – Non Network Procedure](#Acquiring_logical_image_of_sys_non_ntwk)33

[Acquiring a Logical Forensic Image of a Running System – Network Procedure using Encase](#Acquiring_logical_image_of_system_ntwk) 35

[Mounting a Forensic Image File as a Logical Drive using FTK Imager Procedure](#Mounting_forensic_image_ftkimager)38

[Acquiring a Logical Forensic Image of a Network Resource Procedure](#logical_image_of_network_resource)40

[Checking the Basic Input / Output System (BIOS) Procedure](#checking_bios)42

[Investigating Malicious Code Procedure](#Investigating_Malicious_Code)44

[Live Response Procedure](#Live_response)47

[Imaging a Mac Computer Using Target Disk Mode Procedure](#mac_imaging_TDM)49

[Acquiring an Image of a Virtual Machine Procedure](#Acquiring_vm)51

[Incident Response Daily Duties](#IR_daily_duties)53

[Log Review Daily Duties](#Log_review_duties)55

[Standard Naming Conventions](#standard_naming_conventions)57

[Spillage Remediation](#spillage_remediation)73

**1. Purpose**

The purpose of the Cyber Incident Response Team (CIRT) Technical Manual is to provide Cyber Security Office personnel with desktop instructions on how to perform common technical procedures during cyber security investigations. This manual also ensures that all Cyber Security personnel with CIRT responsibilities are consistently performing their duties the same way and using industry standard techniques.

**2. Scope**

This document is applicable to all Cyber Security personnel who have CIRT responsibilities including, but not limited to; collection and preservation of digital evidence, incident response, cyber investigations, fraud, waste, and abuse investigations, or the forensic analysis of digital evidence. The individuals most impacted by this technical manual are those assigned to the [Agency Name] Monitor and Control Team, although other Cyber Security personnel may find themselves assisting with digital investigations and should be familiar with the presence of this document.

This document is not a validation manual and is generally not vendor or tool specific, unless there is only one tool at [Agency Name]’s disposal that will accomplish the task. This document applies to the methodology and steps for commonly taken actions in a CIRT incident. Forensic tool validations are documented separately.

**3. Roles and Responsibilities**

|  |  |
| --- | --- |
| Key Role / Position Title | Responsibility |
| Cyber Security Personnel assigned to CIRT | * Apply the instructions detailed in this manual in the course of investigations and/or analysis of digital evidence. * Provide input into making updates or changes to this manual as needed. |
| CIRT Supervisor | * Maintain document control, including revision tracking. * Ensure the document is reviewed at least annually to account for technological changes. * Incorporate changes requested by CIRT personnel. * Provide input as necessary to document. |
| Cyber Security Manager | * Ensure document meets all legal, technical, and administrative requirements. * Final approval of document. * Provide input as necessary to document. |

**4. Requirements**

[Agency Name] CIRT personnel shall utilize the technical procedures in this manual when conducting investigations as defined in section 2 of this document “Scope”. It should be noted, however that investigations involving digital evidence are rarely the same and can present many challenges due to differences in hardware, software, and investigative need. The CIRT personnel will use the techniques in this manual whenever possible with the understanding that in rare circumstances a variance may be required to accomplish a critical task. In the event a variance is necessary, CIRT personnel shall document in a separate memorandum the reason why a variance was required and notify the .CIRT Supervisor and the Cyber Security Manager. The CIRT Supervisor will review the action taken and make a determination if this document is in need of updating, or if the issue was so isolated that the variance was acceptable and no document update is required.

|  |
| --- |
| **Forensic Sterilization of Loose Media Procedure** |

**1. Purpose**

The purpose of this procedure is to provide direction to the CIRT personnel when forensically sterilizing (wiping) loose media. Forensically sterilizing media has a number of purposes and may include overwriting a single file, multiple files, a removable drive, or an entire physical disk. Forensically sterilizing media may be indicated when the media is needed to store digital evidence (e.g., a forensic image of host under investigation) or may be used when cleaning up a spillage event to ensure information is irretrievable in the future.

**2. Equipment Needed**

1. Approved software or hardware for forensically sterilizing data.
2. Loose media to be forensically sterilized.
3. Computer or other device capable of running sterilizing program.

**3. Calibration**

All hardware and software used in this protocol shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Prepare the computer or hardware device (e.g., Logicube Talon) by turning on the device and ensuring it boots properly.
2. Attach media to be sterilized.
3. Launch forensic sterilizing utility.
4. Using approved software or hardware device, begin overwriting all data within the physical disk space with a known character (pre-determined in the validation study). Ensure at least one pass of overwriting occurs.
5. If desired, format the loose media with the file system of choice.
6. Return the media if necessary, or if staying with Cyber Security, label the media as being sterilized and store it appropriately.

**5. Important Notes**

None.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| **Forensic Sterilization of Active Files Procedure** |

**1. Purpose**

The purpose of this protocol is to provide direction to the CIRT personnel when forensically sterilizing (wiping) active files. Forensically sterilizing active files may be indicated when an entire physical disk does not need to be sterilized, however a file(s) need to be securely removed, (e.g., a spillage cleanup).

**2. Equipment Needed**

1. Approved software for forensically sterilizing data.
2. Access to physical or logical device that the active files reside upon.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Access the physical device that contains the unwanted files, or have logical access to the files (e.g., a MicroSD card from a mobile device, or access to a shared directory on a network device with sufficient privileges to remove the files securely).
2. Ensure the unwanted files are present on the device.
3. Re-confirm the files to be removed.
4. Install and/or run the sterilization utility (e.g., Microsoft SDelete).
5. Overwrite unwanted files securely using approved sterilization utility.
6. Uninstall sterilization utility if necessary.
7. Confirm unwanted files are no longer accessible.

**5. Important Notes**

None.

**6. References**

1. Validation manual

|  |
| --- |
| **Target Drive Preparation Procedure – Loose Media** |

**1. Purpose**

The purpose of this procedure is to provide direction to the CIRT personnel when preparing loose media (e.g., hard drive) to store forensic images or other digital evidence.

**2. Equipment Needed**

1. Approved software or hardware for forensically sterilizing data.
2. Loose media to be forensically sterilized.
3. Computer or other device capable of running sterilizing program.
4. Computer capable of formatting loose media to appropriate file system.

**3. Calibration**

All hardware and software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Forensically sterilize the loose media as specified in this document if it is not already sterilized.
2. If media appears to be sterilized, confirm the attached label indicates the drive has been sterilized.
3. Connect the loose media to a designated forensic computer and initialize and format the drive (if necessary) to the appropriate file system for the investigation.
4. Create a volume label on any partition that may hold evidence. Label each volume with the [Agency Name] case number and unique evidence item number for the case (e.g., 13-0001, Item #1).
5. Create any necessary directories and name them in accordance with the naming convention specified in the administrative manual.
6. Label the external media appropriately, indicating the case number, date, examiner name, and what evidence is stored on the device.
7. Secure the device in accordance with evidence handling procedures outlined in the administrative manual.

**5. Important Notes**

None.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| **Target Drive Preparation Procedure – Network Storage** |

**1. Purpose**

The purpose of this procedure is to provide direction to the CIRT personnel when preparing network storage (e.g., Storage Area Network (SAN) or Network Attached Storage (NAS)) to store forensic images or other digital evidence.

**2. Equipment Needed**

1. Computer with network access to the network storage device.
2. Sufficient network privileges to create and modify data on the network storage device.

**3. Calibration**

All hardware and software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Identify the network resource which will contain the evidence.
2. Create the necessary directory structure using proper naming conventions outlined in the administrative manual.

**5. Important Notes**

None.

**6. References**

1. Administrative manual

|  |
| --- |
| **Hard Drive Removal Procedure** |

**1. Purpose**

The purpose of this procedure is to describe the steps necessary when removing a hard drive from a computer system.

**2. Equipment Needed**

1. Tools.
2. Camera (optional).
3. Permanent Marker.
4. Labels (optional).

**3. Calibration**

None.

**4. Procedures**

1. Photograph the computer in its current condition prior to beginning work. Remove the computer from evidence packaging, photograph all sides of the computer[[1]](#footnote-1).
2. Open the case on the computer to access the hard drive, or if a laptop, locate what components must be removed to access the hard drive.
3. Photograph the internal components of the computer1.
4. Remove the hard drive from the computer.
5. If there are multiple hard drives in the computer, use a permanent marker to label to distinguish the drives.
6. Record information from the drive(s) on the examiner’s notes including; make, model, serial number, size, etc.
7. Take appropriate measures to protect the drive from contamination, static discharge, and misplacement. The hard drive should be labeled with the [Agency Name] case number and the unique evidence item number.

**5. Important Notes**

This procedure is for standard desktop and laptop computers. It is understood that there are some computers in which the removal of the hard drive is not advisable. This could include laptop computers with solid state or flash memory hard drives, Apple computers where the hard drives may be extremely difficult to access, or technical reasons why removing the hard drive may not be the best action. In these situations, examiners should still complete steps A through D above and select a different method for acquiring data from the hard drive.

**6. References**

1. None.

|  |
| --- |
| **Forensic Imaging Procedure – Windows Based** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when forensically imaging media using a Windows based tool.

**2. Equipment Needed**

1. Tools.
2. Camera (optional).
3. Permanent marker.
4. Labels (optional).
5. Forensic computer.
6. Approved forensic imaging software.
7. Physical write-blocking device.

**3. Calibration**

All hardware and software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Ensure the media to be acquired is properly labeled and protected from damage, contamination, or misplacement.
2. Ensure all nomenclature from the hard drive has been properly recorded in the examiner’s notes.
3. Connect the media to be acquired to a hardware write blocker.
4. Connect the write blocker to the forensic computer.
5. Power on the write blocker and ensure the write protection light is illuminated.
6. Ensure the forensic computer recognizes the hard drive.
7. Ready the target media per protocols in this manual. Either place the image onto loose media (e.g., external hard drive), or place the image on the network. Ensure all naming conventions are proper and in conformance with the administrative manual.
8. Launch the forensic imaging tool of choice and hash the original media (or logical container to be imaged) using at least the MD5 algorithm and preferably SHA1.
9. After the original hash is obtained, utilize the forensic imaging software to create an image of the media (should be the same as what was hashed in the previous step).
10. Begin the forensic imaging process using the image format of the examiners choice.
11. At the completion of the imaging process, compare the hash value of the original media with that of the forensic image and ensure they are the same.
12. If the hash values between the original media and the forensic image do not match, the examiner should attempt to determine why. The examiner may choose to re-hash the original evidence and attempt to create another forensic image in the event an error was made in the imaging process. If the examiner is still unable to obtain a matching hash between the original evidence and the forensic image, this mismatch must be noted in the report and the examiner should render an opinion as to why the values will not match.
13. If the forensic imaging tool provides the option of generating an imaging report, the examiner should save the imaging report within the electronic case file.
14. At the conclusion of the imaging, the examiner should repackage the original media as evidence and store it per the administrative manual.

**5. Important Notes**

This procedure is specific for imaging hard drives and removable media that can be accessed and connected to a physical write blocking device. For devices that cannot be connected to a write blocking device, see additional procedures in this manual.

There are times when hash values may not match between the original media being imaged and the forensic image created, even when write protection is used. One example would be the imaging of some solid state hard drives. A mismatched hash value may also be caused by the original media failing and/or certain portions of the media not being accessible during the hashing or imaging process. A mismatched hash should be investigated, but is not necessarily a critical finding if the examiner can articulate their opinion as to the cause.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Forensic Imaging Procedure – Linux Based (Using a Forensic Computer)** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when forensically imaging media using a Linux based tool.

**2. Equipment Needed**

1. Tools.
2. Camera (optional).
3. Permanent marker.
4. Labels (optional).
5. Forensic computer.
6. Approved forensic imaging software.

**3. Calibration**

All hardware and software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Ensure the media to be acquired is properly labeled and protected from damage, contamination, or misplacement.
2. Ensure all nomenclature from the hard drive has been properly recorded in the examiner’s notes.
3. Boot forensic computer using bootable Linux CD, USB, Virtual Machine (VM), or other bootable device.
4. Ensure Linux operating system boots properly.
5. Attach media to be imaged to the forensic computer.
6. Ensure the Linux operating system recognizes the media to be imaged.
7. Create a hash of the original media to be imaged (at least MD5, but preferably SHA1).
8. Connect the target media to the forensic computer (either local drive, external drive, or network location).
9. Remove write protection of target drive so image can be written to the target location.
10. Launch the imaging utility (either through the Graphical User Interface (GUI) or the Command Line Interface (CLI)).
11. Image the original media to the target media using the format of the examiners choice.
12. At the completion of the imaging process, compare the hash value of the original media with that of the forensic image and ensure they are the same.
13. If the hash values between the original media and the forensic image do not match, the examiner should attempt to determine why. The examiner may choose to re-hash the original evidence and attempt to create another forensic image in the event an error was made in the imaging process. If the examiner is still unable to obtain a matching hash between the original evidence and the forensic image, this mismatch must be noted in the report and the examiner should render an opinion as to why the values will not match.
14. If the forensic imaging tool provides the option of generating an imaging report, the examiner should save the imaging report within the electronic case file.
15. At the conclusion of the imaging, the examiner should repackage the original media as evidence and store it per the administrative manual.

**5. Important Notes**

This procedure is specific for imaging hard drives and removable media that can be accessed and connected to a forensic computer. For devices that cannot be connected to a computer, see additional procedures in this manual.

There are times when hash values may not match between the original media being imaged and the forensic image created, even when write protection is used. One example would be the imaging of some solid state hard drives. A mismatched hash value may also be caused by the original media failing and/or certain portions of the hard drive not being accessible during the hashing or imaging process. A mismatched hash should be investigated, but is not necessarily a critical finding if the examiner can articulate their opinion as to the cause.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Forensic Imaging Procedure – Linux Based (Using the Original Host)** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when forensically imaging media using a Linux based tool on the original host machine. At times an examiner may need to use the original host machine to create an image of its own hard drive. Examples may include instances when the removal of the hard drive is not possible or inadvisable.

**2. Equipment Needed**

1. Tools.
2. Camera (optional).
3. Approved forensic imaging software.
4. Target disk to store forensic image.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Document the current state (power on or off, running programs, presence of encryption tools, etc.) of the original evidence computer.
2. Get the Linux distribution bootable media prepared (CD, DVD, USB, etc.).
3. Power down the original evidence computer.
4. IF USB device, Insert the bootable Linux distribution into the computer.
5. IF optical media, power on the computer and quickly open the optical drive tray and insert the optical disc.
6. Boot the computer into the boot menu (this may be performed by booting into the Basic Input/Output System (BIOS), or temporary boot menu of a Windows based computer, or by holding the “Option” key on a Mac based computer.
7. Select to boot the computer from the known good Linux utility.
8. Ensure the computer boots properly to the Linux distribution.
9. Plug in the target media and ensure it is ready to receive the forensic image from the host (properly formatted and write protection turned off for that volume).
10. Perform a hash of the original evidence media (at least MD5, but preferably SHA1).
11. Record the hash value(s) of the original evidence media.
12. Launch the imaging utility (either through the Graphical User Interface (GUI) or the Command Line Interface (CLI)).
13. Image the original media to the target media using the format of the examiners choice.
14. At the completion of the imaging process, compare the hash value of the original media with that of the forensic image and ensure they are the same.
15. If the hash values between the original media and the forensic image do not match, the examiner should attempt to determine why. The examiner may choose to re-hash the original evidence and attempt to create another forensic image in the event an error was made in the imaging process. If the examiner is still unable to obtain a matching hash between the original evidence and the forensic image, this mismatch must be noted in the report and the examiner should render an opinion as to why the values will not match.
16. If the forensic imaging tool provides the option of generating an imaging report, the examiner should save the imaging report within the electronic case file.
17. At the conclusion of the imaging, the examiner may package the entire computer as evidence, or may leave the computer in production depending on the specifics of the investigation.

**5. Important Notes**

This procedure is specific for imaging hard drives installed in a computer that either cannot be removed or it is inadvisable to remove them.

There are times when hash values may not match between the original media being imaged and the forensic image created, even when write protection is used. One example would be the imaging of some solid state hard drives. A mismatched hash value may also be caused by the original media failing and/or certain portions of the hard drive not being accessible during the hashing or imaging process. A mismatched hash should be investigated, but is not necessarily a critical finding if the examiner can articulate their opinion as to the cause.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Forensic Preview Procedure – Windows** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when forensically previewing digital evidence using a Windows based forensic machine. There are situations in which an examiner may not need to acquire an entire image of a piece of media, however the active files on the media need to be reviewed in a forensically sound manner.

**2. Equipment Needed**

1. Tools.
2. Hardware write blocker.
3. Forensic computer.
4. Approved forensic software.

**3. Calibration**

All software and hardware used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Ensure the media to be previewed is properly labeled and protected from damage, contamination, or misplacement.
2. Ensure all nomenclature from the media has been properly recorded in the examiner’s notes.
3. Connect the media to a hardware write blocker.
4. Connect the hardware write blocker to the forensic computer.
5. Power on the hardware write blocker.
6. Ensure the write protection light is illuminated.
7. Ensure the forensic computer recognizes the new device.
8. Launch the forensic software tool of choice to review the contents on the media (note, at times an examiner may simply use Windows’ built-in explorer function).
9. At the conclusion of the preview, eject the media and repackage it if necessary, following evidence handling procedures within the administrative manual.

**5. Important Notes**

None.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Forensic Preview Procedure – Linux** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when forensically previewing digital evidence using a Linux forensic tool. There are situations in which an examiner may not need to acquire an entire image of a piece of media, however the active files on the media need to be reviewed in a forensically sound manner.

**2. Equipment Needed**

1. Approved forensic software.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Ensure the media to be previewed is properly labeled and protected from damage, contamination, or misplacement.
2. Ensure all nomenclature from the media has been properly recorded in the examiner’s notes.
3. Get the Linux distribution bootable media prepared (CD, DVD, USB, etc.).
4. Power down the original evidence computer.
5. IF USB device, Insert the bootable Linux distribution into the computer.
6. IF optical media, power on the computer and quickly open the optical drive tray and insert the optical disc.
7. Boot the computer into the boot menu (this may be performed by booting into the Basic Input/Output System (BIOS) of a Windows based computer, or by holding the “Option” key on a Mac based computer.
8. Select to boot the computer from the known good Linux utility.
9. Ensure the computer boots properly to the Linux distribution.
10. Begin previewing the files on the computer as necessary for the investigation.
11. At the conclusion of the preview, eject the media and repackage it if necessary, following evidence handling procedures within the administrative manual.

**5. Important Notes**

None.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Evidence Search Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners with a systematic means of searching digital evidence submitted for forensic analysis.

**2. Equipment Needed**

1. Forensic computer.
2. Forensic software.

**3. Calibration**

All hardware and software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Review the following:
   1. Authority to conduct investigation.
   2. Details involving the investigation.
   3. Ensure incident and related information is in case management system.
2. System hardware examination:
   1. Photograph the evidence, including all sides of the evidence[[2]](#footnote-2).
   2. If possible, open the case and photograph internal components of the evidence2.
   3. If possible, remove any hard drive(s).
   4. If applicable, document hard drive(s) label and jumper settings (if present).
3. Case folder creation:
   1. Create main electronic case folder using proper naming conventions as detailed in the administrative manual.
4. Forensic imaging:
   1. If the device is to be imaged, image the device according to procedures detailed in this manual.
   2. Place the image on a forensically sterilized piece of media or on a network device.
   3. Ensure naming conventions are used according to administrative manual to prevent cross-contamination or mislabeling of evidence.
   4. Document pre-hash and post-hash of original evidence if applicable.
5. Time settings:
   1. If the examination is on a computer, the examiner should confirm the settings of the internal clock (generally by checking the BIOS of a Windows machine, or using a boot utility for a Mac).
   2. If the examination is performed on a Windows based computer, the examiner should export, at a minimum, the HKLM\System registry hive and confirm the time zone settings of the evidence computer.
   3. The examiner should ensure their forensic machine’s clock and time zone settings mirror that of the original evidence computer.
   4. Document all of these findings in the examiner’s notes for this case.
6. Malware scan:
   1. The examiner shall perform an independent malware scan of any media that will be examined. The examiner may use a number of approved anti-malware software tools available to them for this scan. Any malware located or other abnormalities will be documented in the forensic report and researched by the examiner.
7. Forensic processing:
   1. Depending on the needs of the investigation and the examiner’s preferences, the amount of processing done may vary greatly. For example, an examiner may choose to data carve, conduct entropy tests, full text indexing, and hashing of all files in one case, but on another case may not do any up-front processing and just begin to look at the evidence from the forensic image.
8. Reporting:
   1. The examiner shall document their actions and findings in accordance with the administrative manual.

**5. Important Notes**

This procedure is a guideline and it is understood that a number of factors may change how an examiner performs an examination. This procedure does not dictate specific tools that an examiner must use, other than the tools used must be approved and validated.

None.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Acquisition of Live Memory (RAM) – Non Network Acquisition Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when acquiring live memory (RAM) of a computer. This procedure is to be used when the examiner has physical access to the computer and does not cover the acquisition of RAM over a network environment. RAM can contain a large amount of evidentiary value including, but not limited to; passwords, webpages, documents, images, text, websites visited, clipboard contents, and more.

**2. Equipment Needed**

1. Approved forensic software.
2. Portable storage device.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Ensure the USB device containing the forensic software tool to acquire RAM is ready.
2. Ensure an external storage device (generally a USB drive or other external drive, or may be a partition on the software USB device) is forensically sterilized and ready to accept the RAM dump.
3. Insert the USB device containing the forensic software tool of choice into the running computer.
4. Document the exact date and time the USB device was introduced into the computer.
5. Navigate to the executable file on the USB device and select to acquire the RAM of the local computer and place the RAM dump onto the USB target drive.
6. If the USB target drive is different than the forensic tool drive, introduce this into the running computer. Document the exact date and time this drive was introduced as well.
7. Begin the RAM dump process.
8. When the software tool advises the RAM dump has finished, close the forensic software tool and eject any USB devices introduced by the forensic examiner.
9. Handle the USB device containing the RAM dump with care. If the device is going to hold RAM dumps from multiple hosts, ensure proper naming conventions are used to eliminate the cross-contamination of digital information. Each RAM dump shall be placed in a unique directory and the directory will be named with the case number and either the item number of the host (if there is one) or the machine name the RAM was pulled from. For example 13-0089 ITEM #1 or 13-0089 B034575.
10. Transport the device to the laboratory for further analysis if needed.
11. If not done automatically by the forensic software used to create the RAM dump, create a MD5 and/or SHA1 hash value of the RAM dump and document the results.

**5. Important Notes**

Random Access Memory (RAM) is volatile. If a computer system is turned “off” when the examiner arrives, there is no need to turn on the computer to acquire the RAM. RAM acquisitions should only be done on running live systems.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Acquisition of Live Memory (RAM) – Network Acquisition using Encase** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when acquiring live memory (RAM) of a computer. This procedure refers specifically to using Encase Enterprise to acquire RAM of computers connected to the [Agency Name] network. RAM can contain a large amount of evidentiary value including, but not limited to; passwords, webpages, documents, images, text, websites visited, clipboard contents, and more.

**2. Equipment Needed**

1. Encase Enterprise.
2. Storage device to hold evidence.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Determine the IP address or computer name of the suspect device to acquire from.
2. Launch Encase Enterprise.
3. Login to the Encase Server.
4. Click “Add a device”.
5. Click “Physical Memory” to acquire just RAM. If running processes are also desired, click “Process Memory” as well.
6. Click “Next”.
7. Enter the computer name or IP address of the suspect machine to acquire from.
8. Select “Memory”.
9. Click “Next”.
10. Click “Finish” if all settings are correct.
11. On the right side of the screen where it shows the available devices, right click the small red triangle under the suspect computer.
12. Click “Acquire” from the menu that is presented.
13. Click “Add to case” if you want the physical image of the memory added to the case on the left side of the screen. Click “Replace source device” if you would like to eliminate the preview of the device and just have the physical image available for review.
14. Click “Next”.
15. In the next wizard window, complete the fields as follows:
    1. Name – Enter the [Agency Name] CIRT case number (e.g., 13-0001)
    2. Evidence Number – Enter the unique evidence items number if one has been assigned (e.g., Item 1). If no item number has been assigned, use the default information (host name and IP address).
    3. Notes – This is optional and may be completed by the examiner as necessary. Some items to consider would be the forensic workstation asset ID or any other special circumstances.
16. Select compression ratio.
17. Select at least MD5 hashing, however SHA1 is recommended.
18. Select the output path based upon naming conventions described in the administrative manual.
19. Click “Finish”.
20. Handle the device containing the RAM image with care. If the device is going to hold RAM dumps from multiple hosts, ensure proper naming conventions are used to eliminate the cross-contamination of digital information. Each RAM dump shall be placed in a unique directory and the directory will be named with the case number and either the item number of the host (if there is one) or the machine name the image was pulled from. For example 13-0089 ITEM #1 or 13-0089 B034575.
21. If the device containing the image is going to considered evidence, the device shall be sealed within an evidence bag and stored within the secure evidence area. Consider making two copies of a drive when it will become evidence (such as a fraud, waste, and abuse case) with one drive being the evidence drive and the other being a working copy for analysis.

**5. Important Notes**

Random Access Memory (RAM) is volatile. If a computer system is turned “off” when the examiner arrives, there is no need to turn on the computer to acquire the RAM. RAM acquisitions should only be done on running live systems.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Acquiring a Logical Image of a Running System – Non Network Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when acquiring a logical disk image of a live machine (also referred to as live acquisition).

**2. Equipment Needed**

1. Approved forensic software.
2. Portable storage device.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Determine the physical machine that has access to the information desired.
2. Access the machine and document information about the machine (serial number, current state, etc.).
3. Ensure the USB drive containing the forensic software tool of choice is available.
4. Introduce the USB drive into the running system. Note the exact date and time.
5. Launch the forensic tool that will create the logical image.
6. Ensure a forensically sterilized target drive is available to place the logical image onto, or if using a network location, ensure it is prepared in accordance with this manual and the administrative manual.
7. Using the forensic tool, select the logical drive, directories, or files that are to be imaged.
8. Give proper names to the file and include the case number of the investigation.
9. Provide the file path of where the image is to be placed.
10. Create the forensic image (image format is up to the examiner’s discretion) and ensure the image container is hashed by at least the MD5 algorithm, preferably the SHA1 algorithm as well.
11. Properly eject all introduced USB devices at the conclusion of the imaging process.
12. Handle the device containing the forensic image with care. If the device is going to hold images from multiple hosts, ensure proper naming conventions are used to eliminate the cross-contamination of digital information. Each image shall be placed in a unique directory and the directory will be named with the case number and either the item number of the host (if there is one) or the machine name the image was pulled from. For example 13-0089 ITEM #1 or 13-0089 B034575.
13. If the device containing the image is going to considered evidence, the device shall be sealed within an evidence bag and stored within the secure evidence area. Consider making two copies of a drive when it will become evidence (such as a fraud, waste, and abuse case) with one drive being the evidence drive and the other being a working copy for analysis.
14. Transport the device to the laboratory for further analysis if needed.

**5. Important Notes**

Acquiring a logical image of a running system may be required in certain circumstances when powering down a system to obtain a traditional physical image is contraindicated. An example would be obtaining a network share folder of an employee in a fraud, waste, or abuse case, or obtaining system files from a running production server where taking the server offline is not an option. It is also important to note that since acquiring data in a live environment is dynamic and files may change after the acquisition by end-users or the system itself, the state of the system at the moment of the acquisition can never be replicated exactly again. The data that is acquired through forensically sound methods should be saved in an image container and the entire container hashed, so the data can be validated and integrity checked at a later date.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Acquiring a Logical Image of a Running System – Network Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when acquiring a logical disk image of a live machine over the network using Encase.

**2. Equipment Needed**

1. Encase Enterprise.
2. Storage area for image.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Determine the IP address or computer name of the suspect device to acquire from.
2. Launch Encase Enterprise.
3. Login to the Encase Server.
4. Click “Add a device”.
5. Click “Local Drives” option.
6. Click “Next”.
7. Enter the computer name or IP address of the suspect machine to acquire from.
8. Select “Local Drive”.
9. Click “Next”.
10. Click “Finish” if all settings are correct.
11. On the right side of the screen where it shows the available devices, right click the small red triangle under the suspect computer.
12. Expand the selection to view the logical drive, directories, or files you want to acquire and select those.
13. Click “Acquire” from the menu that is presented.
14. Click “Add to case” if you want the physical image of the memory added to the case on the left side of the screen. Click “Replace source device” if you would like to eliminate the preview of the device and just have the physical image available for review.
15. Click “Next”.
16. In the next wizard window, complete the fields as follows:
    1. Name – Enter the [Agency Name] CIRT case number (e.g., 13-0001)
    2. Evidence Number – Enter the unique evidence items number if one has been assigned (e.g., Item 1). If no item number has been assigned, use the default information (host name and IP address).
    3. Notes – This is optional and may be completed by the examiner as necessary. Some items to consider would be the forensic workstation asset ID or any other special circumstances.
17. Select compression ratio.
18. Select at least MD5 hashing, however SHA1 is recommended.
19. Select the output path based upon naming conventions described in the administrative manual.
20. Click “Finish”.
21. Handle the device containing the forensic image with care. If the device is going to hold images from multiple hosts, ensure proper naming conventions are used to eliminate the cross-contamination of digital information. Each image shall be placed in a unique directory and the directory will be named with the case number and either the item number of the host (if there is one) or the machine name the image was pulled from. For example 13-0089 ITEM #1 or 13-0089 B034575.
22. If the device containing the image is going to considered evidence, the device shall be sealed within an evidence bag and stored within the secure evidence area. Consider making two copies of a drive when it will become evidence (such as a fraud, waste, and abuse case) with one drive being the evidence drive and the other being a working copy for analysis.

**5. Important Notes**

Acquiring a logical image of a running system may be required in certain circumstances when powering down a system to obtain a traditional physical image is contraindicated. An example would be obtaining a network share folder of an employee in a fraud, waste, or abuse case, or obtaining system files from a running production server where taking the server offline is not an option. It is also important to note that since acquiring data in a live environment is dynamic and files may change after the acquisition by end-users or the system itself, the state of the system at the moment of the acquisition can never be replicated exactly again. The data that is acquired through forensically sound methods should be saved in an image container and the entire container hashed, so the data can be validated and integrity checked at a later date.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Mounting a Forensic Image File as a Logical Drive Using FTK Imager** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when mounting a forensic image file as a logical drive.

**2. Equipment Needed**

1. FTK Imager.
2. Forensic computer.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Launch FTK Imager.
2. Ensure forensic image is accessible to forensic computer (e.g., network resource is available or image on removable drive is connected to forensic computer).
3. Click “File” and then select “Image Mounting”, or alternatively the small gray icon in the toolbar that represents this same command.
4. Click the ellipsis under the “Image File” dialog box and navigate to where the forensic image is currently stored and click “open”.
5. Select whether to mount this as a logical or physical drive.
6. Assign the drive letter.
7. Select File System / Read Only as the mount method.
8. Click “Mount”.
9. Go to “My Computer” and ensure the drive mounted appropriately (note, if the image had multiple partitions, you should see each partition mounted with its own drive letter).

**5. Important Notes**

It is sometimes necessary to mount a forensic image to do further testing. Some of these tests may include exporting data, running anti-malware scans against the mounted logical drives, or using other forensic tools against a forensic image.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Acquiring a Logical Image of a Network Resource using FTK Imager** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when acquiring a logical forensic image of a network resource. This procedure would commonly be used to forensically capture a network shared resource such as an employee’s “personal” drive or group directory.

**2. Equipment Needed**

1. FTK Imager.
2. Forensic computer.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Ensure the examiner has privileges sufficient to access the network resource.
2. Navigate to the network resource that is to be forensically acquired.
3. Select the directory to be imaged and map the network location as a local drive on the forensic computer. Do not open or access files within the directory.
4. Map the network location as a drive letter on the forensic machine. Make note of the drive letter used.
5. Launch FTK Imager.
6. Click “File” and “Create Disk Image” or alternatively, click on the disk image icon on the toolbar.
7. Select the source of the image in the dialog box as “Contents of a Folder”.
8. Click “Next”.
9. If a warning appears about the compatibility of logical image files, click “Yes” to continue.
10. Select the source of the evidence. Click “Browse” and then navigate to the mapped drive letter created for this network resource and click “Ok”.
11. Click “Finish”.
12. In the Create Image dialog box, ensure that the boxes for “verify images after they are created”, “precalculate progress statistics”, and create directory listings of all files in the image after they are created” are checked.
13. Click “Add”.
14. Enter [Agency Name] unique case number (mandatory), evidence number (mandatory), unique description (optional), examiner (mandatory), notes (optional).
15. Click “Next”.
16. Click “Browse” and select the destination for the forensic image. This should be placed on an appropriately prepared piece of media.
17. Provide the image file a name according to appropriate naming conventions.
18. Provide a fragment size.
19. Select the compression ratio.
20. Select whether or not to use AccessData (AD) encryption.
21. Click “Finish”.
22. The image process should begin and will end with a window showing the pre and post MD5 and SHA1 hash values of the network resource.
23. Handle the device containing the image with care. If the device is going to hold images from multiple hosts, ensure proper naming conventions are used to eliminate the cross-contamination of digital information. Each image shall be placed in a unique directory and the directory will be named with the case number and either the item number of the host (if there is one) or the machine name the image was pulled from. For example 13-0089 ITEM #1 or 13-0089 B034575.
24. If the device containing the image is going to considered evidence, the device shall be sealed within an evidence bag and stored within the secure evidence area. Consider making two copies of a drive when it will become evidence (such as a fraud, waste, and abuse case) with one drive being the evidence drive and the other being a working copy for analysis.

**5. Important Notes**

It should be noted that acquiring a logical image of a network resource will not include things such as certain metadata, unallocated space, or slack space.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Checking the Basic Input / Output System (BIOS) Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take checking the Basic Input / Output System (BIOS) of a computer.

**2. Equipment Needed**

1. Host computer.

**3. Calibration**

N/A.

**4. Procedures**

1. A computer must be booted into the BIOS before checking it. Prior to turning off the host computer, ensure that all live analysis has been completed (if applicable).
2. Power down the computer if it is turned on. Depending on the investigation this may be accomplished by doing a normal “shutdown”, or by pulling the plug from the back of the computer, or removing the battery and unplugging if it is a laptop.
3. Power on the computer and boot into the BIOS. Generally this is accomplished by pressing a function key, escape, delete, or some other button, depending on the BIOS manufacturer.
4. Once in the BIOS, navigate to the setting menu that shows the current date and time.
5. Compare the BIOS date and time with that of a trusted source (e.g., cellular phone clock set by the network). Document any discrepancies.
6. Shut down the computer.

**5. Important Notes**

At times a BIOS password may be in place. If a BIOS password is in place, examiners should attempt to identify what the password is by interviewing the computer owner or system administrator. If the BIOS password cannot be obtained, the examiner may consider booting the computer with a Linux forensic tool to check the date and time without accessing the BIOS. There are ways to bypass certain manufacturers BIOS passwords, however at times this may reset the clock and other setting information, so examiners should use care when considering this method.

**6. References**

None.

|  |
| --- |
| **Investigating Malicious Code Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when investigating malware. This procedure will cover both the static analysis (process that consists of collecting information about and from an executable file without running it) and dynamic analysis (launching an executable file in a controlled and monitored environment so that its affects on a system can be observed and documented).

**2. Equipment Needed**

1. Forensic computer.
2. Anti-malware detection software.
3. Forensic analysis software.
4. Hardware write blocker.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures – Static Analysis**

1. If the host machine is connected to the [Agency Name] domain, attempt to review log information from sources such as FireEye, firewall logs, and other sources of information in an attempt to identify if the malware was quarantined by the anti-virus (AV) software, what may have led to the machine being compromised (reviewing GET logs and other information), and if there is a presence of Internet Protocol (IP) traffic coming from the host to the outside. This information should also assist in establishing a timeline of activity.
2. Take note of where the malicious code is located on the host, including the full file path and MAC (Modified, Accessed, Created) times of the malicious file. Also take note of the operating system the file was located on.
3. Take note of who found the suspicious file and the time it was located.
4. Take note of any complaints from an end-user, administrator, or anyone else that may have been the result of malicious software.
5. Always attempt to perform a live response on the suspect host machine, obtaining volatile memory, running processes, network artifacts and connections, etc.
6. If a physical forensic image was obtained of the host machine, mount the forensic image using FTK Imager and scan the mounted drive with an AV engine again. If possible, scan with a different engine than what made the initial finding. Note any additional malware located.
7. If a physical forensic image is not possible to obtain (e.g., production server that cannot be taken off-line), than a logical forensic image should be obtained of at least the operating system (OS) partition of the host. If the malware appears to be located on a network storage device, that are should also be logically imaged.
8. If memory was obtained from the host system, perform an analysis of the memory of any indicators of compromise (IOC), and malware.
9. If the malware is not detected through all AV scans or any other alerting system at [Agency Name], consider scanning the system for malware by doing an entropy test or checking for packed files.
10. If the malicious file(s) has been identified and located, create a MD5 hash of the file(s).
11. Upload the MD5 hash to an online virus scanning tool such as Virus Total or ThreatExpert to identify additional information about the malware and if it has been previously identified.
12. Attempt to classify the file using a tool such as TRiD. Ensure the latest definitions are downloaded. Classifying the file should provide information about what type of file it is and possibly how it was written.
13. Use a tool such as strings.exe or bintext.exe to review the ASCII and Unicode strings in the suspicious file.
14. If there is a need to determine the dependencies required to run the malicious software, import the malicious software into a program such as DependencyWalker.
15. Examine the registry of the host computer for evidence of persistence, such as changes to autorun and run registry keys.
16. Consider examining prefetch files for evidence of launched executables and their associated files.
17. Consider creating a timeline of activity on the host machine to look for other activity at the time the malware was introduced to the system, or to determine what files are malicious based upon the known facts in the investigation.
18. Report the findings and take appropriate containment, eradication, and recovery efforts.

**5. Procedures – Dynamic Analysis**

1. The examiner must have a safe working environment to conduct dynamic analysis of malware. This includes a system that is not connected to the domain. It is recommended to use virtual machines for the dynamic analysis of malware.
2. Boot the virtual machine test environment.
3. Place the malware on the machine.
4. If checking for network connectivity, use software such as FakeDNS to control web traffic.
5. Launch the necessary tools for the testing. This may include tools such as Process Monitor, Wireshark, Filemon, Regmon, mailpot, etc.
6. Launch the malware and begin monitoring the effects of the malware.
7. Document the findings and use the information gained to further the investigation.
8. Continue with the remaining steps in the incident response process (e.g., containment, eradication, recovery).

**6. Important Notes**

These lists are quite exhaustive and may not always need to be done in each investigation. For example, in a case where an examiner is notified of malware being detected on a host computer and the enterprise AV software immediate caught the malware and quarantined it, less may need to be done. In this case the incident responder may review the AV logs and firewall logs to ensure no data was lost, do a preliminary examination of the host machine and request IT wipe the hard drive and re-image the device. If a root cause is determined of how the malware was able to get on the machine then that information should be provided to the necessary people to consider changes to blacklists and other security rules.

**7. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Live Response Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners with the proper steps to take when performing a live response of a host system. Live response refers to obtaining volatile information from a running system. Live response should not be confused with live acquisition, which refers to acquiring a logical image of a storage device while a system is running. Live acquisition may occur as part of live response, however is not synonymous. Whether or not to perform a live response depends on several factors including, but not limited to; the examiner’s experience, the type of investigation, the type of host system, and the resources available to the examiner. Live analysis collects volatile information on a system that would otherwise be lost if the traditional “pull the plug” approach were taken with the computer system.

**2. Equipment Needed**

1. Host computer.
2. Forensic software tools.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Make the determination that live response is needed.
2. Identify the host machine.
3. Prepare live response tools.
4. Prepare a target drive to collect data onto.
5. Document all actions taken on the machine, including dates and times.
6. Be mindful of the order of volatility. Consider obtaining data that is more volatile first, such as:
   * Obtaining the RAM
   * System time
   * Logged-on user(s)
   * Open files
   * Network information
   * Network connections
   * Process information
   * Process-to-port mapping
   * Process memory
   * Network status
   * Clipboard contents
   * Service/driver information
   * Command history
   * Mapped drives
   * Shares
7. Remove the target drive containing data acquired during the live response.
8. Consider the target drive as containing potential evidence and handle it appropriately. Each acquired drive shall be placed in a unique directory and the directory will be named with the case number and either the item number of the host (if there is one) or the machine name the data was acquired from. For example 13-0089 ITEM #1 or 13-0089 B034575.
9. Make a determination if the system will be shut down or left running.
10. If conducting this via the network, this information may be obtained without physically accessing the host.
11. Tools such as Encase, already has a presence on many hosts in the [Agency Name] environment and may be used to collect the above information without introducing new hardware into the host.
12. If Encase is utilized over the network, the examiner should still document their procedures and ensure they have a properly dedicated target location (either disk or network space) that has the naming conventions required in the administrative manual.

**5. Important Notes**

Performing live response will make system changes on the host machine. These changes can easily be determined during a forensic analysis if the examiner properly documents their actions. It is important that examiners understand that this process will make changes and what some of those changes may be.

**6. References**

1. Administrative manual
2. Validation manual

|  |
| --- |
| **Imaging a Mac Computer using Target Disk Mode Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners direction when forensically imaging a Mac computer using Target Disk Mode.

**2. Equipment Needed**

1. Forensic computer.
2. Host (suspect) computer.
3. Firewire cables.
4. Firewire hardware write blocker.
5. Approved forensic imaging software for Mac.
6. Target drive to place image on.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Identify the host Mac computer to be imaged.
2. Note the host system serial number, asset tag number, or any other distinguishing numbers or nomenclature on the system.
3. Prepare a forensic Mac computer by ensuring it is powered on, is not connected to the Internet, and has the appropriate Mac forensic imaging software installed.
4. Prepare a Firewire hardware write blocker and Firewire cables (preferably Firewire 800).
5. If the host (suspect) Mac is powered on, consider any live response needs prior to turning it off.
6. Once the above is done, power off the host Mac.
7. Connect the Firewire cable to the host Mac and then to the Firewire hardware write blocker.
8. Connect the other end of the Firewire hardware write blocker to the forensic Mac computer.
9. Power on the host Mac while holding down the “T” key on the keyboard.
10. The Mac should boot into Target Disk Mode and a Firewire symbol should appear on the screen of the computer.
11. The forensic computer should soon recognize the host computer’s hard drive as an externally attached hard drive.
12. The forensic examiner could choose to preview the contents of the logical files on the host machine as this is a forensically sound preview and/or they may physically image the hard drive from the host computer.
13. To forensically image the host computer, ensure a forensically sterilized target drive is prepared and connected to the forensic computer, or that a network connection to a lab network storage device is prepared.
14. Launch the forensic imaging application of choice and select the host computer’s hard drive as the drive to be imaged.
15. Create at least a MD5 and preferably a SHA1 hash of the original host hard drive and document the results.
16. Select the target drive as the destination drive.
17. Begin forensically imaging the host hard drive onto the destination hard drive.
18. At the conclusion of the imaging process, compare the MD5 and SHA1 hash values from the original drive to that of the forensic image.
19. Power down the host machine.
20. Disconnect all equipment.

**5. Important Notes**

None.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| **Acquiring an Image of a Virtual Machine Procedure** |

**1. Purpose**

The purpose of this procedure is to provide examiners direction when investigating a virtual machine (VM) and how to forensically image a VM.

**2. Equipment Needed**

1. Forensic computer.
2. Forensic imaging software.
3. Forensic software capable of mounting a .VMDK file as a logical drive.
4. Target drive to store forensic image on.

**3. Calibration**

All software used in this procedure shall be validated and the validation documented within the [Agency Name] CIRT Validation Manual.

**4. Procedures**

1. Identify the VDI that is the subject of the investigation.
2. Contact the IT staff of [Agency Name] and request that the VDI either be copied or cloned to another target location.
3. Be aware that some agency’s may utilize folder redirection for much of the stored for VDI users. That data may also need to be captured and reviewed, depending on the nature of the investigation.
4. Since a .VMDK file is encapsulated much like a forensic image file, the file itself is protected from data being injected or removed from the .VMDK file until the point it is booted.
5. Ensure the .VMDK file it placed on a target location that is accessible from a forensic computer.
6. Launch a forensic software tool that is capable of opening a .VMDK file (e.g., FTK Imager).
   1. Note – in FTK Imager this can be done by adding an evidence item and clicking “Image File”, then selecting the .VMDK file.
7. Once the .VMDK file is open, create an original hash (at least MD5 but preferably SHA1 of that .VMDK with the forensic software.
8. Create a forensic image of the .VMDK file and store the image on a target disk.
9. Match the hash values of the original mounted .VMDK file with the forensic image.
10. Process the forensic image with the forensic software tools of choice.

**5. Important Notes**

[Agency Name] currently deploys multiple Virtual Desktop Interfaces (VDI)’s throughout the environment. It may become necessary to obtain a VM to conduct a forensic analysis of that machine. VM’s are stored within the [Agency Name] data center and each VDI has a corresponding .VMDK file that can be obtained by contacting IT.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| **Incident Response Daily Duties** |

**1. Purpose**

The purpose of this procedure is to provide direction to the [Agency Name] CIRT (Cyber Incident Response Team) personnel who are assigned to respond to various emails and alerts generated by systems within the enterprise.

**2. Equipment Needed**

1. Computer connected to the [Agency Name] network.
2. Access to all systems that generate logs / alerts.
3. An Enterprise Email account.
4. Access to Remedy.

**3. Procedures**

1. Each week, a different member of the CIRT is the primary member accountable for responding to security events that may have been reported by a user or security appliance. These events should be reviewed as early as possible during the CIRT member’s shift.
2. It is the responsibility of the CIRT member to ensure that all cases identified during the week of their assigned Incident Response duty is addressed and responded to in the appropriate time frames.
3. When an event is reviewed that needs further investigation, the CIRT member assigned to incident response will notify the CIRT member responsible for log review for that week in order to deconflict the log/alert.
4. If the event or anomaly is determined to be worthy of an investigation, it shall be triaged accordingly and investigated.
5. If additional resources are needed, it is the responsibility of the CIRT member on duty to request assistance from other CIRT members when necessary.

**4. Daily Operations**

The following events will be examined daily or as they are generated:

Federal Intelligence Alerts

Symantec Endpoint Protection Notifications

FireEye Events

PII Notifications

Classified Spills

Phishing Notifications

Splunk Alerts

|  |
| --- |
| **Log Review Daily Duties** |

**1. Purpose**

The purpose of this procedure is to provide direction to the CIRT (Cyber Incident Response Team) personnel who are assigned to review the various logs and alerts generated by systems within the enterprise.

**2. Equipment Needed**

1. Computer connected to the [Agency Name] network.
2. Access to all systems that generate logs / alerts.

**3. Procedures**

Each week, a different member of the CIRT is accountable for reviewing the system logs and alerts generated by the enterprise. These logs should be reviewed as early as possible during the CIRT member’s shift. Alerts that are generated in real-time should be reviewed as soon as possible.

When a log or alert is reviewed that needs further investigation, the CIRT member assigned to log review will notify the CIRT member responsible for incident response (IR) for that week in order to deconflict the log/alert.

If the alert or log anomaly is determined to be worthy of an investigation, it shall be triaged accordingly and investigated.

**4. Daily Operations**

The following logs and alerts will be examined daily:

DNS logs

DHCP logs

VPN logon summary

RSA log summary

GETLOG summary

Maldomain query match alert

Splunk Alerts

Foreign downloads alert

SNORT report

Firewall reports

TriGeo reports

CERT documents

|  |
| --- |
| **Standardized Naming Conventions** |

**1. Purpose**

The purpose of this document is to create strict naming conventions and ensure standardization between CIRT members during the storing of digital files, including digital evidence. The use of standard, organized naming conventions is critical to eliminate the possibility of the cross-contamination of digital information.

**2. Equipment Needed**

1. Computer.
2. Access to media which contains digital information and/or digital evidence.

**3. Procedures**

1. Prior to storing any digital information on a storage device, the CIRT member must ensure it is ready to receive information. This includes ensuring the storage device has been forensically sterilized and then formatted in a compatible file system.
2. Within the root of the storage device, a directory shall be created with the [Agency Name] case number. Example: F:\13-0001.
3. Any digital information collected by CIRT shall have the first part of the file name contain the unique case number and that item’s unique evidence item number or asset ID if no evidence item number has been assigned. For example, if a CIRT member obtains a physical image of a computer, the name of that image file should begin with the case number and unique item ID. Example: 13-0001 ITEM1 Image.001, or 13-0001 B324231 Image.E01.
4. Every subdirectory entry made to the main case number directory shall have the case number and item number (or asset ID) precede any other directory name. If a subdirectory was accidentally transferred out of the main directory, just by looking at the directory name it should be immediately apparent what case number it belongs to. Example: F:\13-0001\13-0001 ITEM1 RAM Dump\13-0001 ITEM1 Ram Dump.img.

**4. Naming Convention Examples**

**5. Important Notes**

None.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| **Spillage Remediation** |

**1. Purpose**

The purpose of this document is to provide information on how to properly remediate a classified spillage incident.

**2. Equipment Needed**

1. Computer.
2. Connection to network.
3. Access to Encase Enterprise, Dameware, MANDIANT, and Remedy.

**3. Email Cleanup**

1. If the number of users is limited, the investigator may go to the users’ location to examine the systems, have the systems brought to a central location, or use Dameware DWMRCC to remote the users’ systems. However the access is obtained, a search of the system to clean out the known emails will be performed. This approach will be needed for anyone who uses local PST or archive files. To remove the files, the investigator will select the file and use the <SHIFT><DELETE> key combination to delete the file without moving it to the “Deleted Items” folder.
2. The investigator will collect the date, the time, the sender, the recipients, and the subject of the emails identified as case-related. This information will be compiled on the secure network to create a master list of emails. The investigator will use this list to compare with the known case-relate individuals to identify individuals who were not previously identified as having been involved in the case. The investigator is reminded that the data collected about the emails is to be handled in a manner consistent with classified material.

3.1 Larger spillage where the total number of emails or users is unknown

1. Large spills with the possibility that there are emails that have not been identified yet will require the assistance from IT. Submit a Remedy ticket for “Email Cleanup”. For the description, refer the reader to the Cyber lead and refer to the Cyber Incident Response case number. Assign the call to IT. Provide the IT member with the case details within a limited area, do not put this information into Remedy. IT searches work best with some combination of sender address, recipient addresses, date and time, and subject. Searching for attachment names is less reliable. Attachments are hidden when the emails are encrypted. Limited Areas (LA) must be used to discuss classified information related to the case.
2. The IT member will supply a log of emails, which match the search criteria. The Cyber investigator will instruct the IT member which messages are to be deleted. The IT member will provide a second log of those actions. These shall be kept with the case notes on the secure network. The Cyber investigator will use the logs to confirm that there are no previously unidentified individuals in the logs. If so, their systems will need to be searched for case-related files.

**4. Blackberry Cleanup**

1. Blackberries belonging to users who sent or received case-related classified emails, will have to have their Blackberries wiped with a kill command. This requires coordination with the IT Telecommunications group and the IT service desk. Provide the Telecommunications group with a list of users, known to have generated or received the case-related emails, and ask them to verify which personnel have Blackberries. Do not correlate the list back to the case. Service desk assistance is requested through a Remedy ticket. Again do not provide details. Simply call it Blackberry cleanup and refer to the Cyber IR case number. Provide the list of Blackberry-holding users to the individual executing the Remedy ticket. The users will have to be warned their Blackberries will be reset. The procedure for resetting the Blackberries after receiving the “kill” command can be performed by the user, as long as the service desk provided an account and password to the user. If the user had the Blackberry setup for Entrusted email, they will have to coordinate with the service desk to get the encryption re-enabled.

**5. File Cleanup**

5.1 Desktop Cleanups.

1. If the full extent of the spill is known, collect the names of the individuals and identify their systems. If the scope is a limited number of users, the investigator has the option of using Encase Enterprise to examine the systems and locate case-related files, to map the users drive partitions and conduct the search, or to remote the system with the user and search. The user must be questioned about flash drives and other removable media.
2. If the full extent of the spillage is not known, searches of the [Agency Name] will need to be performed. If the full filenames are classified, a sweep with the full name cannot be performed. Use the MD5 hashes or partial filenames to perform the search for contaminated end-user systems. Use Encase Enterprise and/or Mandiant to perform the enclave search.

**6. Search identified drives for case-related files.**

1. The methods utilized for searching the drives of the identified systems will vary with the needs of the investigator. Manual searches of individual system is best accomplished by running a directory search and writing the results to a text file (use the target system’s hostname as the filename). This file will serve as an artifact to prove a search was made of the system. The file does need to be treated as classified, burned to CDROM, the investigating system must be cleared of the artifacts, and the files loaded on the secure network. If the user has a VDI or has an IT-maintained system, it is highly likely the system will be configured with Roaming Profiles. These directories are not available on the target system when the user is not logged in. It will take assistance from the System Admins to search this space. See Section 6.2 for Network Drives and Shared Resources.

**7. To remote a user’s desktop with an interactive user**

1. The investigator will need the Dameware DWMRCC installed on their workstation.
2. Call the user and confirm they will have the time to work with you. Do not discuss classified topics over the phone. Launch the DWMRCC and supply the system name to connect with the remote system.
3. Search the system for case-related files. The options available are by DOS commands, PowerShell commands, or with Windows Explorer. See “DOS Commands” or “PowerShell Commands” below for the proper syntax. Confirm matches by filenames or hashes.
4. Refer to “Clearing or Purging a drive” below to perform the cleanup.

**8. To map the remote system’s drive partitions**

1. In order to map drives from the target system, the investigator will need to know what partitions are in use by that system. This information will be obtained from an interview with the system’s custodian, from a Drive Report from the Microsoft System Center Configuration Manager (SCCM), or from having previewed the system previously with Encase. There are two command line methods of obtaining directory listings of a drive. These are using the standard DOS “Command Prompt” and PowerShell. The PowerShell method will provide a more concise list with full pathnames. For the purposes of the below commands, the following information will be used: The term “{UserID\_ir}” represents the investigator’s IR account, the term “{T:}” will represent the local drive letter used to mount the remote drive on, the term “{system}” will represent the investigation system’s hostname, and “{c$}” will represent the remote drive partition to be mounted. Refer to “Clearing or Purging a drive” below to clean the investigating system.

DOS Commands

Mount the remote drive partition

net use {T:} \\{system}\{c$}

Change to the mounted drive as the active drive.

{T:}

Confirm the current path is looking at the root level of the drive

cd \

Execute the directory search

dir /s > c:\temp\{system}.txt

Perform all searches against the text file to identify the case-related files.

findstr /i “{pattern} c:\temp\{system}.txt

Change the active drive back to the local system

c:

Unmount the mapped partition

net use /delete {T:}

PowerShell Commands

Mount the remote drive partition

New-PSDrive –Name {T} –PSProvider filesystem –Root \\{system}\{c$} //Note: no colon after the drive letter T that the drive is to be mounted to

Change to the mounted drive as the active drive.

{T:}

Confirm the current path is looking at the root level of the drive

cd \

Execute the directory search

Get-ChildItem –Recurse –Force –Name | Out-File –FilePath

c:\temp\{system}.txt –Encoding ASCII

Perform all searches against the text file to identify the case-related files.

Select-String -Path {system}.txt –Pattern {pattern}

//Note: quote the {pattern} if there are strings present.

Change the active drive back to the local system

c:

Unmount the mapped partition

Remove-PSDrive –name T

**9. To perform an enterprise sweep with Encase Enterprise**

1. Launch Encase Enterprise and log into the Safe.
2. Start a new case to keep the record of the findings.
3. In the Enterprise folder under the Enscript tab, launch the “Sweep Enterprise” applet.
4. Confirm the case options are set correctly and select the “Next” button.
5. Key in the target systems under machines or use the “Network Tree” button to select systems or ranges from the Encase known systems.
6. Under the “Module List” select the type search to perform. The module for filename or hash value searches is under “Custodian Search”. Verify only the “Custodian Search” is checked and double-click on the entry to enter the configuration menus.
7. Verify the search type desired is checked and double-click the entry to configure the settings.
8. After configuring and accepting search parameters, select “Okay” and the the “Next” button.
9. Use the “Sweep Options” button to verify the settings are as needed. Under the “Schedule” tab, conform the “Sweep Mode” is “Once” and that “”Retry until successful” is checked. Select “Okay” when satisfied with the options settings.
10. Select “Finish” to start the sweep.

**10. To use Encase to provide a file listing**

1. Launch Encase Enterprise and log into the Safe.
2. Start a new case to keep the record of the findings.
3. Use the “Add Device” to add the system under investigation
4. Check all logical drives shown as in use by the system and select the “Next” button.
5. Confirm all of the logical drives selected are shown and select the “Finish” button.
6. After Encase completes the parsing of the drives’ Master File Table (MFT), click on the pentagon in front of the partitions to be listed (the process known as “homeplating”) in the tree pane (left). Right click on any filename in the table pane (right). It is recommended the investigator use separate files to list each partition. Select the “Export” menu item.
7. There are a number of options in the “Export” popup window which need to be set. Set the output file type to “TEXT”. Check the field “Full Path” and certify no other options under Fields are checked. Do not check the “Only Checked Rows” option. The “Stop” option should contain a large number representing the number of objects to be written. Verify the output file is in the directory path you desire and that the file name contains only the hostname of the system, or the hostname with partition information. Do not relate this file to the case, or else a cleanup of the server will be required.
8. Select the “Finish” button.
9. Save the case, if desired, and close Encase.
10. Search the resultant files and identify systems to be cleaned.

**11. Clearing or Purging a drive**

1. The factor used to determine if the media (memory card, flash drive, or drive partition) can be cleared or should be purged is total space occupied by the known classified material in relation to the total media capacity. If less than 0.01% of the unclassified media contains classified material, use Microsoft’s SDelete tool with three passes (sdelete -p 3 {filename}) to remove the files (it will require mapping the drive to a drive letter for SDelete to work or transferring the SDelete tool to the remote system and using Dameware to remote the system.). After performing the SDelete on each file, the investigator must run the SDelete program with the ”zero free space” option (-z) along with the “three pass” option (sdelete –z –p 3) from the root level of the drive to be cleaned. Running SDelete from the investigator’s system against a mapped drive will take much longer than running it against an equivalent size local drive.
2. If in excess of 0.01% is contaminated, the system must be sanitized using an authorized tool, such as DBAN v1.6 or the Tableau TD2 Forensics 1:2 Duplicator.

**12. Network Drives and Other Shared Resources**

1. Identify shared resources and network drives utilized in the spill
2. If the full extent of the spill is known, identify shared resources (network) drives used by the known contaminated set of users.
3. If the full extent of the spill cannot be readily identified, a search of all [agency name] drives will be necessary.

**13. Search of Shared Resources for case-related files:**

1. As with the desktop drives, the determining factor for clearing or purging the media is the percentage of total space occupied by the classified information in relation to the total capacity of the media. If less than 0.01% of shared drive contains classified, use Microsoft’s SDelete tool with three passes to remove the files (it will require mapping the drive to a drive letter for SDelete to work. If access permissions do not allow the investigator to remove a file with SDelete, the investigator must notify the CIRT Supervisor of the issue. Create a Remedy ticket to get assistance from the System Administrators to properly clear the file. If this fails and the CIRT Supervisor approves, the file will be simply deleted.
2. If in excess of 0.01% of shared drive is contaminated, the media should be sanitized using an authorized tool, such as DBAN v1.6 or the Tableau TD2 Forensic 1:2 Duplicator. The CIRT Supervisor must be notified before any action is taken. If the shared resource is a large capacity network attached storage system or a source of operation impacting documents, impacts may dictate a review by IT management and the DAA. The CIRT Supervisor is responsible for coordinating this effort. The management decision will determine how the investigator will clean the shared resource.

**14. Server Cleanup**

14.1 Identify applications and servers which spillage related information was processed on.

1. Locations may include, but are not limited to, the following: WEB servers, application servers, and SharePoint servers. The applications will need to be traced to the servers that they operate from. Identify if there are Development, Stage, or Production servers for the application, or if there a single instance of the application.

14.2 Identify how the data is stored on the server.

1. This may require working with the IT Engineering/Applications group or an application owner group to get answers. Determine if the data is in a database, a flat file, or a combination of the two.
2. If the contamination is in flat files and is less than 0.01% of the media, use the Microsoft SDelete utility with three passes (-p 3) to clear the files. After clearing all case-related files, use the SDelete utility to zero the free space (-z option).
3. If the contamination is in flat files and exceeds 0.01%, the server will require purging. Before any action is taken, contact the CIRT Supervisor and advise concerning the issue. The CIRT Supervisor is responsible for coordinating efforts with the Cyber Security Manager, IT Management and with the DAA, if necessary. The investigator will follow the direction from the CIRT Supervisor to complete the sanitization of the server.

14.3 Was the spillage in a SQL database

1. If the classified material is in a SQL database, the CIRT Supervisor will be informed of the issue. The investigator will work with the IT Database team to identify actions to be taken and notify the CIRT Supervisor of the recommendations. The CIRT Supervisor and Cyber Security Manager will work with IT and/or the system owner to determine the best course of action. Options available for investigator include copying the unclassified portions of the table to a new table followed by deletion of the old table, deleting the classified records from a table, compacting the database after the cleanup of the tables, and finishing up by using the “-z” option in SDelete to zero out the drive free space.

**15. Backup Tape Cleanup**

15.1 Build the list of known contamination

1. Collect the identified locations for case-related files from the shared resources, applications, and servers.

15.2 Request assistance from the IT Data Center Operation (DCO) group

1. Open a Remedy ticket for “Backup Tape Cleanup”. Refer the reader to the Cyber lead and the case number instead of providing details. Assign the case to the IT DCO group. Use a limited area to provide the DCO personnel with the details of the case.

15.3 Collect the backup tapes

Once the DCO group identifies the tapes, the investigator will work with the group to collect these tapes, establish a chain of custody, and transport them to the [agency name] Facility. Procedures for hand-carrying classified material from one facility to another facility will be followed. These steps are as follows:

1. The investigator will notify his supervisor that they will accompany the DCO representative to the site to take custody of the backup tapes of interest.
2. The investigator will accompany the DCO representative to the site to take custody of the tapes.
3. Upon receiving the tapes, a Chain of Custody document will be started. The tapes will bagged in an opaque bag or envelope. Tape all seams with brown fiber tape or tamper-proof evidence tape. This envelope will be marked with the Classified Mailing Address, the level and category of the material, and any special caveats.
4. Place this bag/envelope inside another bag/envelope, tape all seams with brown fiber tape or tamper-proof evidence tape, and mark the bag/envelope with the Classified Mail Address.
5. The investigator will take the bagged material and proceed directly to the [agency name] facility and will deliver the items to the Safeguards and Security. The investigator will not make any stops along the way.

15.4 Surrender of the backup tapes to Safeguards and Security

1. Once back at the [agency name] Campus, the tapes will be surrendered to the Safeguards and Security Inquiry Officer for retention as case-related records. The Chain of Custody document will be signed over with the tapes.

**16. Offsite Cleanup**

1. Upon determining case-related information has left the site, the [Agency Name] CIRT Supervisor, the Cyber Security manager, and the [Agency Name] ISSM must be notified.
2. The DAA and ISOM need to be notified and assistance requested to contact the other agencies involved.
3. Once the other agencies have been briefed, remain in contact to obtain an ongoing status. The case cannot be closed until the external agencies have completed their cleanup.

**17. After Action Report**

17.1 Event Records and Notes

1. Investigators on the case are responsible for keeping a log with the dates and times actions were taken. This information when gathered in one location, provides a picture of the spilled information and as such is classified at the level and category of the spill until reviewed by a Derivative Classifier. These records must be kept on the secure network.

17.2 Generating the AAR

1. Once the cleanup is complete, a report of the actions taken must be generated and submitted to the Safeguards and Security Inquiry official. If the incident was generated at [Agency Name], a finalized incident report shall be filed with HQ.
2. The declassified reports must be reviewed and approved by the CIRT Supervisor prior to distribution to anyone outside of Cyber Security.

**18. Important Notes**

None.

**19. References**

1. Validation manual
2. Administrative manual

**20. References**

**[removed]**

**APPENDIX A – KNOWN NETWORK DRIVES AND SHARED LOCATIONS**

|  |  |
| --- | --- |
| **Description** | **Location** |
|  |  |
|  |  |
|  |  |
|  |  |

**Appendix B – Known Server locations**

[Removed]

**Appendix C – Known contacts for coordination**

|  |  |  |
| --- | --- | --- |
| **Name** | **Unclassified Telephone** | **Email** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**KNOWN INFORMATION FOR OTHER SITES**

|  |  |  |
| --- | --- | --- |
| **Name** | **Telephone** | **Email** |
|  |  |  |
|  |  |  |

**[Agency Name] Safeguards and Security Incident Contact List**

|  |  |  |  |
| --- | --- | --- | --- |
| **Position** | **Name** | **Telephone** | **Mobile Phone** |
|  |  |  |  |
|  | | | |
|  |  |  |  |
|  |  |  |  |

1. Photography may not always be possible or advisable depending on the type and sensitivity of the investigation. The decision to use photography in an investigation is left to the discretion of the investigator and clarification can be sought from the CIRT Supervisor. [↑](#footnote-ref-1)
2. Photography may not always be possible or advisable depending on the type and sensitivity of the investigation. The decision to use photography in an investigation is left to the discretion of the investigator and clarification can be sought from the CIRT Supervisor. [↑](#footnote-ref-2)