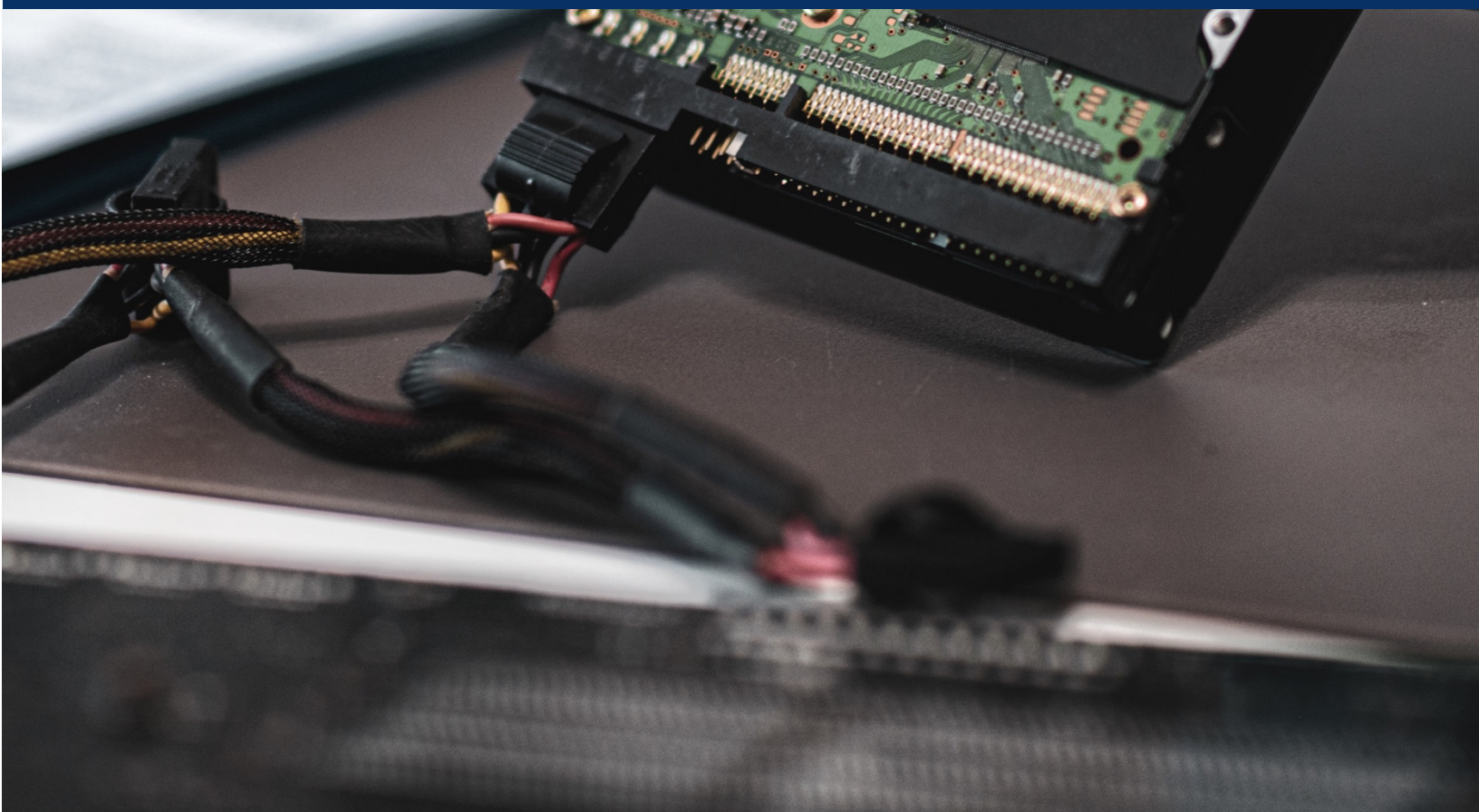
CyFIR DIGITAL EVIDENCE

POLICIES AND PROCEDURES MANUAL



Contents

INTRODUCTION

Purpose

The purpose of this manual is to give CyFIR personnel a resource that will serve as a starting point for the policies and procedures for the collection, handling, and processing of digital evidence.

Discussion

As society embraces technology and the use of mobile devices increases, a growing number of technological devices are being used in crimes and then seized by law enforcement as evidence. These devices are used by criminals to communicate, store data, and facilitate crimes. Computers, cellphones, GPS devices, digital cameras, and other devices that contain digital evidence must be properly collected, handled, and processed.

The volatile nature of the data on these devices requires proper seizure to preserve the integrity of the data and ensure their evidentiary value in legal proceedings.

Devices must also be processed properly, whether the data they contain are incriminating or exculpatory. It is equally important that these devices are stored in a manner that will preserve the data in their original state for examination by the plaintiff or defense and for the introduction of the original item into court when necessary.

Proper documentation for each device — tracking it from initial submission through storage, processing, the release of any information related to the data on the device, and the return of the device back to the originating individual or entity — will ensure the admissibility of the item and the resulting data in any judicial proceeding.

POLICIES AND PROCEDURES MANUAL

Purpose

Thorough documentation is key to every aspect of the legal process. Comprehensive policies and procedures are critical components of that documentation. The purpose of this manual is to give CyFIR personnel a starting point for the development of their own policies and procedures addressing the collection, handling, and processing of digital evidence. This document may and should be edited to suit an agency's specific needs in developing its own policies and procedures.

Discussion

Defining a series of policies and procedures can be a daunting task, especially if the author has no experience and no sample policies and procedures upon which to base their drafts. This manual provides a base to work from and build on. The policies and procedures drafted and adopted by an agency should be regarded as a living document and periodically reviewed and updated to remain current and valid. Once a solid foundation for the policies and procedures is established, the process of updating them will become a much more manageable task.

Adherence to the processes and procedures in this manual will ensure the technical admissibility of digital evidence handled by CyFIR personnel into the United States legal system.

Policy

ADMINISTRATIVE STATEMENT

(1) The CyFIR Policies and Procedures Manual will contain the current policies, procedures, rules, and guidelines for all forensic personnel employed and/or assigned to the CyFIR digital forensics team.

(2) All prior and existing manuals, standard operating procedures,orders, and regulations issued prior to this Policies and Procedures Manual shall be rescinded and replaced.

RESPONSIBILITIES OF PERSONNEL

The contents and revisions of this manual are the responsibility of the forensic director or appointed designee. The forensic director may issue interim directives as needed, which will remain in effect until such time as they are approved and made a permanent part of this Policies and Procedures Manual. All forensic personnel are expected to read and understand the contents of this manual and will be required to sign a document acknowledging they have received a copy of this manual, along with any interim directives, and have read and understood the contents of this manual. The forensic director will maintain the original of thisdocument, and a copy will be provided to each individual employed by or assigned to the digital forensic lab.

DISTRIBUTION

Copies of this Policies and Procedures Manual will be distributed to the following:

(1) Forensics director

(2) All forensic personnel

(3) CyFIR reference material library

This Policies and Procedures Manual will also be available in portable document format(.pdf) on the lab's file server or on another device in a manner accessible by the forensic personnel as deemed necessary and appropriate.

CASE ASSIGNMENT AND PRIORITIZATION

Purpose

This section outlines how cases involving digital evidence are received, prioritized, and assigned for forensic analysis.

Discussion

A system must be established to assign cases to lab personnel. Criteria for assignment include priority, case circumstances, examiner skill set, and forensic discipline. This policy will establish the criteria for case assignment and prioritization and the authority to make an exception in case assignment or priority.

Policy

CASE ASSIGNMENT

The forensic director or designee will assign all incoming cases. It is possible that a case may be assigned by forensic discipline based on the expertise or current caseload of the examinersor on the needs of the case itself. Unless the submitting agency indicates a need for expedited processing, all cases will be assigned in the order received.

CASE PRIORITIZATION

The forensic director or designee will be responsible for identifying cases with a higher priority than others. Priority level will be determined based on the facts known about each case when it is submitted to the digital forensic lab and will be updated as relevant information affecting the priority becomes available.

In collaboration with the investigator, submitting agency, and prosecuting attorney, the forensic director will be responsible for identifying cases that may be eligible for early case assessment (ECA). ECA may enable the digital forensic examiners to perform a forensic examination of the submitted digital evidence only to the extent authorized by the legal proceedings and authorities.

Additionally, cases may be triaged for specific information of investigative value to a case, such as contraband images in a child exploitation case. ECA and triage provide the forensic director and staff a way of improving the efficiency of justice and enable examiners to devote more time to more complex cases and cases that contain large volumes of digital evidence.

AN EXAMPLE OF CASE PRIORITIZATION

(1) Terrorism or any case where the loss of life is imminent

(2) Violent crimes such as murder, rape, and assault

(3) A child at immediate risk of exploitation or abuse

(4) Child pornography and solicitation

(5) Theft or destruction of intellectual property

(6) Public corruption

(7) Financial crimes

(8) Internet crimes, including network intrusion and unauthorized access

(9) Identity theft(10)Fraud

EXCEPTIONS AND MODIFICATIONS TO CASE PRIORITIZATION

All exceptions and/or modifications to case prioritization shall be made by the forensic director, or with the approval of the forensic director, and include all documentation relevant to the change in case priority.

EQUIPMENT TESTING, VALIDATION, AND UPDATES

Purpose

All equipment and software used by digital forensic personnel must first be tested and validated to confirm that it is operating as designed and producing accurate, valid results. Testing and validation must be repeated each time the equipment, firmware, and software are upgraded, reinstalled, or modified. The results of all testing and validation will be recorded and kept on file in order to document that all equipment being used inthe collection and processing of digital evidence is functioning within the manufacturer's specifications and the examiner's expectations based on training and experience.

Discussion

In order to determine if hardware or software is working properly, it must be tested by the user and found to perform consistently over time and deliver repeatable results in line with a known dataset each time it is used. This section addresses the need to test and validate each item that is used within the lab and to document the results. Testing steps will be clearly detailed and should be followed in order. It is recommended that as each step in the testing and validation is completed, the person performing the testing and validation should acknowledge completion of the step in writing with initials or another identifiable mark.

Policy

CONDUCTING VALIDATION TESTING

Validation testing will be conducted by all examiners who use any of the collection and processing hardware or software, in any fashion or to any degree, to collect or process digital evidence in the digital forensic lab or at a crime scene.

VALIDATION PROCEDURES

1. No forensic equipment will be used in the digital forensic lab prior to being tested and validated by forensic personnel and approved by the forensic director.

2. Examiners will test each item of hardware and software in a manner consistent with the manufacturer's specifications of usage. Testing will be performed using the same datasets for standardization. All results and anomalies will be documented.

3. Examiners performing the validation testing on all forensic hardware and software will use a standardized testing and report form, including the date of validation, product name, version number, manufacturer, and cost. All of the validation reports for each item of hardware and software will be approved by the forensic director before those items are used in the lab, and all the reports will be maintained on the digital forensic lab server (if available) and also in paper format in a binder maintained within the lab.

4. All hardware and software will be registered in the company's name. If the registration must be to an individual, approval from the forensic director will be obtained in a memo format,with a copy of the memo maintained on the lab server (if available) and in the lab validation report binder.

MAINTAINING VALIDATIONS

When a piece of equipment becomes damaged or is showing signs of wear or age, it should be tested to verify that it is still operating within the manufacturer's specifications. It is the responsibility of the examiners using the forensic equipment or assigned the item to report such issues to the forensic director. The forensic director will decide whether to replace faulty, damaged, or worn equipment.

After the initial validation of a piece of software, subsequent validations will be done whenever an update to the software is installed on the lab equipment — including the computers used to examine digital evidence (examination machines) or an item that is considered to be portable. Subsequent hardware validations will be performed each time existing hardware is updated, including firmware updates or installing a new or replacement item, such as a write-blocker. Any hardware upgrades done to an examiner's computer, however minor, should be documented and tested to ensure that they do not affect the performance of the forensic software installed on the computer.

SOFTWARE UPDATES

Updates, patches, or operating system service packs should be installed to the examiner's computer as necessary. The updates, patches, or service packs should be downloaded using a system connected to the internet but isolated from the examination machine and the forensic network. After performing any updates to forensic software, the hard disk drive may be imaged and the image may be maintained for future use in restoring the examiner's computer.

EVIDENCE AND PROPERTY HANDLING

Purpose

The digital forensic lab will receive digital evidence from investigations being conducted by CyFIR, LLC and may receive evidence from law enforcement agencies, legal firms or individuals. This policy will cover the proper handling of all digital evidence and property submitted to the digital forensic lab.

Discussion

In order for devices that contain digital evidence to be properly introduced in any judicial proceeding, the devices must be tracked from the time they enter the custody of the lab through their release to the submitting entity. There must be a complete, documented chain of custody from intake to release of each device.

Policy

FORENSIC PERSONNEL RESPONSIBILITIES

The chief responsibilities of all forensic personnel when receiving digital evidence or property are maintaining the chain of custody for and ensuring the security of the evidence of property stored in the secure evidence/property room of the digital forensic lab.

RECEIVING DIGITAL EVIDENCE

Only forensic personnel on duty at the time the evidence is brought to the digital forensic lab and authorized to receive evidence should accept and document the incoming evidence. When digital evidence is delivered to the digital forensic lab by an investigator or other law enforcement officer, the following steps will be taken:

(1) Forensic personnel will ensure all needed documentation is signed and on file. This documentation will include the signed engagement letter or contract and will detail the services requested as part of the statement of work.

(2) A copy of the seizure authority, such as a subpoena, search warrant, consent, or other judicial or administrative order, will be included in the case file. In those matters involving probation or parole, the case file will include a copy of the agreement whereby the defendant waives the right to consent before a search or agrees as a condition of probation or parole to a warrantless search by the Department of Probation and Parole. In all matters, there will be no examination started without ensuring that there is authorization for CyFIR to examine the evidence.

(3) Evidence intake personnel will list each item of evidence on an inventory document with a unique evidence

number, description, the date received and the individual that received the evidence. Any digital evidence examined or removed from a given device will have a unique derivative evidence ID number and all sides of the digital evidence photographed. The derivative ID number will begin with the unique evidence ID followed by a sequential numeration of the derivative evidence. Each evidence item will be marked with the number or letter to readily associate the item with the entry on the inventory document. Subsequent inventories of the evidence will indicate that each entry on the inventory document has been checked and matched to the corresponding evidence item.

(4) The lab intake personnel will sign for the evidence, fill out all required paperwork, upload the evidence photographs to case storage, open a new lab case as appropriate, and enter the evidence into the evidence storage facility.

(5) Derivative evidence is common in digital forensics. One computer, for example, may have multiple hard drives or internal devices that shall be considered unique derivative evidence items. In the event that a piece of digital evidence shall have derivative components that are evaluated as part of an investigation, each device shall have a separate CyFIR Digital Forensic Chain of Custody form filled out and a derivative evidence ID assigned. The derivative evidence ID shall begin with the parent evidence ID number followed by a dash and an iterative number indicating the subcomponent removal sequence. Example, BEtron-A-001-1, where BEtron-A0001 is the parent evidence ID and -1 is the component derivative sequence.

(6) If forensic personnel receive additional evidence from a case already opened, they will submit the necessary documentation identified above, along with an updated inventory document. The examiner who is processing the case will be notified that additional evidence has been received.

(7) A sample intake document is included to this policy as Attachment A – Evidence Intake Form

LABELING

A label will be placed on each item of submitted evidence. The label will at a minimum contain the case number and the unique evidence ID. The label may also contain the originating investigator or agency, lab number, date and time received, and any other information deemed necessary as the situation allows. In the event that a label may not be appropriate due to the surface composition (e.g., the label won't stick) or other factors the examiner may use a permanent marker to indicate the evidence number.

HANDLING EVIDENCE IN THE DIGITAL FORENSIC LAB

All evidence contained in the evidence/property room shall be secured by restricted access and properly guarded upon intake and remain secure until it is removed for examination.

a. REMOVING EVIDENCE FROM THE SECURE EVIDENCE/PROPERTY ROOM

No evidence will be removed without a legitimate, investigative purpose. When evidence is removed from the evidence/property room the examiner will disclose the purpose to the evidence room technician and then , an evidence tracking formwill be filled out and kept up to date. Each evidence tracking form will be kept with the case folder. The forensic personnel filling out the form will note the date and time, give their name and have the evidence room custodian countersign the tracking document. When the evidence is resealed and placed back in the evidence/propertyroom, the date, time, person's name, and location will be updated on the evidence tracking form and the evidence room technician will countersign the document accepting the evidence back into the secure storage.

b. EXAMINATION OF SEALED EVIDENCE BAGS OR CONTAINERS

Sealed evidence bags or containers will only be unsealed and opened during inventory or in thecourse of the digital forensic examination. When unsealing evidence containers or bags, care should be taken to leave the original seal on the packaging, if possible, and createa new opening in a different location. When the inventory is complete or the examiner is finished with the original evidence, it will be resealed with the examiner's name and initials across the new seal, along with the date and time.

c. EVIDENCE RELEASE PROCEDURE

The forensic director will approve all releases of evidence. In the event that evidence is seized by consent and the person to whom the property legally belongs revokes consent, arrangements will be made as soon as possible to return the evidence. Evidence will only be released to the originating entity. In the event that the items being released are forfeited, a copy of the court order declaring the condemnation or awarding the forfeiture will be included in the case file.

d. RELEASE OF EVIDENCE CONTAINING CONTRABAND MATERIAL

Evidence that contains contraband material, such as child pornographic images, will be clearly marked with a label stating, "Do Not Release — Contains Contraband." If evidence of this nature will be released to the originating entity, the media will be either:

i. Wiped with an approved wiping method to render the data on the mediaunrecoverable, or

ii. Accompanied by a form, signed by the ruling authority and included in the casefolder, acknowledging that there is contraband contained in the evidence and authorizing its release.

When evidence containing contraband is released to the originating agency, the evidence will be sealed and marked with the date, time, reason for release, name of the forensics staff member who released the evidence, and his or her initials over the seal.

e. EVIDENCE DESTRUCTION

The digital forensic lab may from time to time be requested to wipe media, removing all data contained on the media and rendering it unrecoverable. No evidence will be wiped unless a court order is issued or the owner consents in writing. The forensic director will first approve all evidence destruction and will maintain a copy of the court order or a signed consent by the owner in the case file. The lab will use an approved wiping method that has been validated and found to render unrecoverable any data contained on the hard drive or other digital media.

f. AUDITS

To maintain the integrity of the evidence/property room in the digital forensic lab, all property contained in the evidence/property room will be inventoried or audited twice a year. Forensic personnel designated by the forensic director will perform the audit. When the audit is complete, the results will be forwarded in an audit report to the forensic director, who will address any anomalies at that time. The audit report will identify each anomaly and its resolution. The forensic director will maintain an audit log, along with a list of any anomalies noted or observed.

SEARCH AND SEIZURE

Purpose

This policy provides basic guidelines that may assist forensic personnel involved in on-site support to subpoena and/or search warrant executions. The specific exceptions to the Fourth Amendment's warrant requirement — e.g., plain view,[1] consent,[2] and exigent circumstances[3] — should be handled according to current training and applicable law.

Further, the purpose of this policy is to:

a. Process and safeguard digital evidence coming into the custody of CyFIR.

b. Provide a standardized procedure for the collection and submission of computers and digital evidence for examination and analysis.

c. Document the chain of custody of evidence.

NOTE: This section is intended as a guide and is not meant to supersede any state or local laws in the governing jurisdiction. Prior to implementing any information provided in this section, state and local laws regarding search and seizure must be considered. Additionally, information implemented from this section should be approved by supervising attorney associated with the case.

Discussion

Everyone is protected from unreasonable searches and seizures under the Fourth Amendment to the U.S. Constitution, and forensic personnel will never conduct a search or seize evidence without a valid search warrant, subpoena or consent of the owner, except when in direct support to law enforcement and exigent circumstances exist. This section addresses the general procedures for documenting the execution of a search warrant or seizure by consent as they apply to digital evidence. This section is not intended to address the entire crime scene, but only digital evidence.

[1] The plain view doctrine is an exception to the Fourth Amendment's warrant requirement that allows an officer to seize evidence and contraband that are found in plain view during a lawful observation.

[2] A warrantless search may be lawful, if a law enforcement officer has asked for and is given consent to search.

[3] Exigent circumstances are those that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts **(**see United States v. McConney, Ninth Circuit, 728 F.2d 1195**)**.

Policy

EXECUTION OF SEARCHES

(1) During the execution of a subpoena or search warrant, all forensic personnel will always act in a professional manner, with the safety of all persons being considered first and foremost.

(2) The area containing the digital evidence will be photographed both before and after the search/seizure.

(3) When searching a person believed to have on their person any type of media or devices containing digital evidence, such as mobile phones and USB flash drives, forensic personnel or law enforcement of the same sex will conduct the search of that person.

(4) When a search/seizure is concluded, the area searched will be returned to pre-search condition, if possible, and exit photographs will be taken.

SEIZING EVIDENCE

(1) Maintaining the chain of custody is a critically important part of any subpoena or search warrant execution. When acquiring evidence, the forensic personnel conducting the search and acquisition will record where each item was found and its condition at the time of seizure.

(2) When possible, all evidence found will be photographed prior to being moved.

(3) All evidence will be recorded and stored in a proper container IAW the new evidence documentation procedures outlined in the Evidence Handling section of this policy.

(4) All evidence will be turned over to the lab staff member assigned as the evidence custodian, or to the person assigned to fill out and maintain the inventory sheet.

(5) A copy of the completed and signed inventory sheet will be left with the owner of the property acquired. If the owner is not available, it will be left at the property in accordance with the subpoena instructions and/or applicable governing law.

(6) The evidence will be taken to the digital forensic lab, inventoried, and labeled according to established procedures.

(7) All evidence will then be secured in the digital forensic lab property/evidence room.

STORAGE AND RETENTION OF EVIDENCE

Purpose

This policy outlines the storage of digital evidence and its retention period in the CyFIR digital forensic lab.

Discussion

This policy is intended to address the need for the storage of all digital evidence, irrespective of the originating entity

Policy

a. CREATION OF NEW CASES

When a case is assigned to a forensic examiner and it requires the creation of an image of the digital evidence, a folder will be created on an approved CyFIR forensic analysis server or workstation using a uniform naming convention. It is recommended that the assigned case number be used as the name of the folder. Additional folders will be created within the main case folder for the storage of the original evidence image(s). If there is more than one piece of digital evidence to be imaged and examined, there will be subfolderslabeled with the evidence number assigned to each.

b. ACCESS TO CASE STORAGE

Forensic examiners and the forensic director will be the only forensic personnel who have accessto the case data storage area. Only the forensic director will be able to delete files and folders.

c. EVIDENCE AND RETENTION

All processed evidence from each case will be kept in the case folder created by the examiner during the initial setup for examination. This will include any reports of digital forensic examination, exported files, files generated by the forensic softwareused, and any other supporting files that belong to the case.

(1) Copies of the reports and supporting files will also be given to the agency or investigator requesting the forensic examination.

(2) All submitted items for a particular case — such as computers, hard drives, external hard drives, mobile phones, and USB flash drives — will be released to the owning entity or originating organization once requested after the digital examination is complete and a final report is produced.

(3) A copy of the document releasing the evidence for backup, whether in email formator by letter, will be maintained by the forensic director in the case folder.

(4) The forensic director or designee will be responsible for removing the case folder from the case file area on the file server (or other storage media) after it has been backedup. The forensic director or designee will be responsible for maintaining a record of where the backup is stored.

(5) All output from examination, processed files, and image files will be considered evidence, and the corresponding level of security will be applied and maintained.

(6) In the event that an outside entity has submitted a large number of cases for processing, a single case with a large number of items to be processed, or a number of devices that collectively contain a large amount of data to be processed, that agency may be required to provide the digital forensic lab with its own data storage ofsufficient size to back up the case data after it has been processed and removed from the digital forensic lab's file server.

(7) When forensic imaging is required for a piece of digital evidence forensic examiners will utilize an approved write block device to ensure that no changes are made to the original evidence. In the event that a specific piece of digital evidence is not supported by write block technology, with the approval of the lab director and following successful training on the technique, forensic examiners may use alternate boot technologies that mount digital evidence in a read only mode that prevents changes to the original evidence to image the device.

REPORTS

Purpose

This policy ensures that all forensic personnel are aware that a comprehensive final report is a major part of the job of all personnel who examine digital evidence in a case.

Discussion

When a report is well written and organized, it can be interpreted and presented in court so that the judge, jury, and defense will understand the circumstances of the case, the evidence that was found, and how the evidence was found. Additionally, the report should document the acquisition of the forensic image file(s) of the digital evidence, the evidence found as a result of the examination as it pertains to the scope of work, and the status or disposition of the digital evidence.

Policy

Forensic personnel are required to create a report for each case number in CyFIR's case management system. Reports will contain the basic information about the incident, the information requested based on the request for service, all information as to what actions the forensic personnel took, as well as their observations, conclusions, and, if necessary, any opinions of theforensic examiners.

a. REPORT DOCUMENTS

At a minimum, a CyFIR report will contain:

(1) Case number

(2) Originating Entity

(3) Case Number

(4) Point of Contact Information

(5) Complete list of evidence submitted and location of evidence

(6) Date and time of evidence intake

(7) What information is being sought (emails, images, etc.)

(8) Short summary of the case and any attachments given by the originating entity

The final report will include all the above with the addition of:

(1) Examinations conducted (if more than one)

(2) Summary of results and conclusions or opinions

(3) Complete report details

(4) Disposition of evidence

(5) Signature of examiner (digital or handwritten)

b. APPROVAL OF REPORTS

All reports created and edited by forensic personnel will be forwarded to the forensic director for review and approval. No reports will be released without the approval of the forensic director.

c. REVIEWS

All reports submitted to the forensic director will go through two reviews, one technical and one administrative.

The technical review will ensure all documents are clearly labeled, all examinations have been conducted, and the examiner's findings are supported by evidence.

(1) The administrative review will then be performed to ensure any technical issues have been resolved, to find any grammatical errors, and to verify that all the documentation is present and complete.

d. REVIEW DOCUMENTATION

The reviews detailed in section d above will be documented in the review section of the report or on the last page of the report.

e. REPORTS CONTAINING CONTRABAND EVIDENCE

(1) Reports containing images of child exploitation, abuse or other sensitive materials will be duplicated without the actual sensitive images in the report. A copy will be provided to the attorney's for providing discovery to opposing counsel.

(2) In the event the attorney requests a copy of the report with the contraband images, a contraband acknowledgment document will be signed by the requesting investigator or prosecuting attorney.

(3) At no time will any reports containing images of child exploitation or abuse leave the digital forensic lab unless there is a court order to supply the images opposing counsel or an opposing expert. The opposing counsel or opposing expert will be required to sign a receipt to acknowledge they are in possession of child exploitation or abuse materials and will be required to return the report(s) back to the attorney when the case is disposed of.

f. REPORT STORAGE

All reports in the case folder(s) generated by the examiner and by the digital forensic lab will be saved on the digital forensic lab's servers or accessible storage devices. All handwritten documents or other hard copy documents will be scanned and stored in the case folder on the lab's servers or accessible storage devices.

g. AMENDMENTS TO REPORT

If a mistake or discrepancy is found in a report that has already been issued, that report will be corrected, and an amended copy will be forwarded to the originating investigator or originating agency and to the prosecuting attorney's office as soon as possible. The forensic director will be notified immediately, and the report will then be marked "Amended Report."

(1) In the event a report needs an amendment or a supplemental report, it will besubmitted to the forensic director for review and approval prior to release.

(2) The amended report or supplemental report will then be added to the final report by the forensic director.

MATERIALS AND SUPPLIES

Purpose

All materials and supplies used in the digital forensic lab, including consumables, will be approved by the forensic director. The content of this policy includes what supplies will be used, who will be responsible for purchasing and maintaining them, and how forensic personnel will report deficient or faulty supplies and request additional supplies.

Discussion

In the course of the day-to-day operations of the digital forensic lab, office supplies will be used and expended. These office supplies include, but are not limited to, paper and ink used for printed forms and reports; CDs, DVDs, and Blu-ray discs, if still in use; and file folders and labels.

Policy

a. SUPPLY SELECTION AND PURCHASING

(1) It is the responsibility of the forensic director to decide what supplies will be used in the digital forensic lab.

(2) All forensic personnel are encouraged to give constructive suggestions as to new supplies,vendors, or changes to the existing supplies used within the digital forensic lab.

(3) All supplies, forensic and non-forensic, will be purchased at the direction of the forensic director or with the forensic director's approval.

(4) All supply purchasing will be made according to purchasing procedures currently in place at CyFIR, LLC

b. REPORTING FAULTY SUPPLIES

Forensic personnel who find supplies or equipment that are deficient, faulty, do not perform as expected, or do not meet their intended specifications will notify the forensic director by email or memo. Supplies of this nature will be removed from use until the forensic director takes action.

c. SUPPLY STOCKING AND INVENTORY CONTROL

Requests for new supplies will be sent to the forensic director for approval.

DIGITAL FORENSIC LAB ACCESS

Purpose

The digital forensic lab processes and holds evidence from both internal and external entities. The evidence that is entrusted to the digital forensic lab contains extremely sensitive data — information or images that are highly confidential in nature. The security of the digital forensic lab and of the data contained therein is essentialin maintaining the integrity and chain of custody of the evidence.

Discussion

In order to promote and maintain the highest level of confidence in the examiners, theirwork product, and their ability to testify in any judicial proceeding, the integrity of the lab as a whole must be guarded at all times. By limiting access to only those individuals who require access, the lab's integrity is maintained at the highest level possible.

Policy

a. LAB DESIGNATION

Due to Covid-19 and other exigent circumstances, CyFIR may allow the designation of digital forensic labs within a forensic examiner's quarters providing that the following conditions are met:

(1) The designated lab area must have the ability to be secured with either a keyed or combination lock when not occupied or under the direct supervision of the forensic examiner.

(2) Must have a safe or other evidence storage device that is not transportable by two men.

(3) Must have an alarm for unoccupied time periods.

(4) Must be climate controlled.

(5) Must be used exclusively for digital forensic activities.

b. LAB PERSONNEL

All personnel assigned to or employed by the digital forensic lab are responsible for the safety and security of the lab. Every effort must be made to maintain the security of the lab at all times and ensure that no unauthorized persons enter the lab at any time.

c. ACCESS TO LAB

(1) All personnel assigned to or employed by the lab will be issued credentials for gaining access to the lab.

(2) Only designated personnel will be allowed to open the lab if secured. This authorization shall be at the sole discretion of the forensic lab director.

(3) At no time will any forensic personnel share their credentials and/or keys or allow anyone to use them. Violations will result in the possibility of loss of access, assignment to a different division or sector within the agency, or disciplinary action, including but not limited to suspension and/or termination.

(4) If the digital forensic lab is equipped with an alarm system, forensic personnel who require 24/7 access will be provided with the code for the alarm system. Whenever the digital forensic lab is not within the immediate observation and control of authorized lab personnel, the alarm will be activated.

(5) Access to any area of the digital forensic lab will be limited to authorized personnel only, unless otherwise approved by the forensic director.

(6) Law enforcement officers, parole/probation officers, and district attorneys/assistant district attorneys will be granted access to the lab in their official capacity without needing the permission of the forensic director, provided each individual signs the entry log and agrees to be escorted at all times.

(7) All non-law enforcement visitors will be required to obtain the permission of the forensic director prior to any visit. All visitors will sign in and remain escorted at all times. Visitors may be denied access at CyFIR's sole discretion.

(8) If the lab is equipped with a warning system (such as a flashing blue light) to let all of the personnel in the lab know that non-law enforcement visitors are in the lab, this system will be activated prior to the entry of any non-law enforcement visitors. When the system is active, all examiners will minimize all programs on their monitor screens to prevent the visitors from observing any case-related data.

(9) Opposing counsel will not be allowed access to the lab under any circumstances.

(10) Maintenance and cleaning personnel will not enter the digital forensic lab unless escorted by forensic personnel and will be required to sign the visitor's log.

RELEASE OF INFORMATION TO THE MEDIA

Purpose

This policy regulates and provides guidance regarding the release of information to the news media and media access to the digital forensic lab.

Discussion

When an investigation is being conducted, especially in high visibility cases, the public will have a need for information. There must be a sole point for the release of informationon cases that impact the community as a whole. However, the digital forensic lab facilitates the processing of evidence and thus cannot be responsible for the release of information to the media.

Policy

a. RELEASE OF INFORMATION

It shall be the policy of CyFIR, LLC that no member of the forensic team shall provide statements or releases of any kind unless directed to do so by the retaining client or authority. Furthermore, it is the policy of CyFIR to not comment in any shape or form concerning any client or CyFIR engagement in specific situations to any entity outside of CyFIR and the retaining client.

b. REQUESTS BY NEWS MEDIA

(1) Any request for information received by CyFIR, LLC from the media will be forwardedto the forensic director, who will refer the inquiry to the retaining entity of the case in question.

(2) Any other requests by the news media for information regarding any current investigations, or for access to the digital forensic lab, will be referred to the retaining entity.

QUALITY ASSURANCE POLICY AND PROCESS

Purpose

Quality assurance ensures that the digital forensic lab is meeting the needs and expectations of CyFIR, LLC, as well as the needs and expectations of any outside organizations and entities that submit digital evidence to the lab.

Quality assurance refers to the planned and systematic activities implemented to ensure that the quality requirements identified for and expected of a product or service are met. It encompasses evaluation, measurement, comparison with standards, monitoring of processes, and feedback that identifies the existence or absence of errors in the results.

Discussion

The digital forensic lab has an ongoing quality assurance program that is designed to monitor the quality of the examination process and provide for continual assessment of and improvements on this process. Quality assurance applies both to the hardware and software employed in the lab and to the work products from each lab examiner. Lab staff will identify and rectify any problems that may affect the lab's performance, the investigative process, or the prosecution of offenders.

Policy

a. OBJECTIVE

The purpose of this quality assurance policy is to:

(1) Build, maintain, support, and document an ongoing quality assurance programthat includes effective and organized processes for monitoring, collecting, and evaluating all critical information about important aspects of lab performance in order to identify those areas that have identifiable room for improvement.

(2) Assist in the improvement of each examiner's work processes and work products by focusing on identifying (through the use of continuous evaluations), correcting, and following up on any issues or problems that affect the overall performance of the digital forensic lab.

(3) Implement corrective action when problems or improvement opportunities are identified.

(4) Follow up on identified problems to ensure improvements have been made or corrective actions taken and to ensure a timely resolution with complete documentation of the corrective actions or

improvements.

b. INDICATORS OF QUALITY ASSURANCE

Indicators of quality assurance are actively evaluated to maintain an established standard of lab performance. Data from each indicator area will be collected, recorded, and analyzed. The findings will be evaluated to detect any deficiencies andany areas of the process that could be improved upon. When required, appropriate corrective action will be implemented and documented.

Post-corrective monitoring will ensure that the action taken was appropriate andresulted in the proper resolution of any problems or issues found.

c. PROFICIENCY TESTING

(a) Proficiency programs are designed to ensure that examiners are proficient and efficient. The lab will participate in external proficiency examinations,such as the International Association of Computer Investigative Specialists' certification and recertification programs, as well as the lab's own internal proficiency examinations.

(b) The lab supervisor or designee will review the final results of all proficiencytesting and discuss those results with the employee.

(c) If there are any noted deficiencies in either the internal or external proficiency examinations, those deficiencies will be investigated by the lab manager. A deficiency report will be created, and the forensic director willinclude an explanation of the likely cause(s) of the deficiency along with appropriate corrective action that will be taken.

d. COMPLAINTS

Complaints received by the lab are monitored for response, corrective action, and follow-up. The forensic director or designee will respond to any written or oral complaint deemed significant that concerns the lab's quality of service or work product. The timeline for responding to complaints will follow [YOUR AGENCY]'s policy. Responses to complaints will be maintained by the forensic director for review and any additional recommendations of appropriate action.

(1) TRAINING FOR NEW EMPLOYEES

Lab-specific job descriptions detailing the duties of each employee will be kept on hand in the individual personnel files. Each employee will read, understand, and sign an acknowledgment of their particular job description. Each employee will receive specific training on the skills for which they are responsible. Specific projects may have project specific training as required.

(2) NEW PROCEDURES AND NEW EQUIPMENT

Each employee will be trained on new procedures and new equipment.

(3) CONTINUING EDUCATION AND TRAINING

Continuing education provides personnel an opportunity to review and expand their knowledge of the digital forensic lab and its processes, facilitating successful lab operations. Each lab examiner is required to

complete a minimum of 10 hours of continuing education per year through training conferences, seminars, workshops, and vendor-specific training. It is strongly suggested that each employee keep a record of his or her continuing education. Additionally, each forensic examiner is required to maintain the proficiency and training requirements relevant to forensic and industry certifications that they possess.

e. MANAGEMENT REVIEW

The objectives of management review are:

(1) To establish that the quality assurance program is achieving the expected results, meeting the digital forensic lab's requirements, continuing to meet customers' needs and expectations, and functioning in accordance with theestablished policies and procedures.

(2) To expose deficiencies or defects in the workflow of the lab, identify weaknesses,and evaluate possible improvements.

(3) To review the effectiveness of previous corrective actions, and to ensure that theestablished quality assurance program is meeting the current needs of the lab and will meet the lab's needs in the future.

(4) To review any complaints received, identify the cause, and recommendcorrective action if required.

(5) To review the findings of internal and external audits and identify any area(s) for possible improvements.