CALIFORNIA STATE UNIVERSITY SAN MARCOS

PROJECT SIGNATURE PAGE

PROJECT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE

MASTER OF SCIENCE

IN

CYBERSECURITY

PROJECT TITLE: Cyber Forensics Investigation Tactical, Techniques, and Procedures (TTP)

AUTHOR: Mr. Jaja O'Neil

DATE OF SUCCESSFUL DEFENSE: May 1, 2017

THE PROJECT HAS BEEN ACCEPTED BY THE PROJECT COMMITTEE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN CYBERSECURITY.

Teresa Macklin, J.D.		May 1, 2017
PROJECT COMMITTEE CHAIR	SIGNATURE	DATE
Yi Sun, PhD		May 1, 2017
PROJECT COMMITTEE MEMBER	SIGNATURE	DATE
Darren Bennett		May 1, 2017
PROJECT COMMITTEE MEMBER	SIGNATURE	DATE

Cyber Forensics Investigation Tactics, Techniques, and Procedures (TTP)

Author: Jaja O'Neil

Date: May 1, 2017

Image @ http://computerforensiclabsinc.com/

Faculty Advisors

Project Chair: Teresa Macklin, J.D.

Committee Member: Darren Bennett

Committee Member: Yi Sun, PhD

Professional Science Masters

California State University, San Marcos

EFFORT

"A good plan, violently executed now, is better than a perfect plan next week."

"Good tactics can save even the worst strategy. Bad tactics will destroy even the best strategy."

-General George S. Patton, Jr. (USA)

Table of Contents

List of Figures……..4

Executive Summary…….5

Acknowledgements……..6

Introduction……..7

Chapter 1: Initial Communication……9

Chapter 2: Collection……...11

Chapter 3: Examination and Analysis……..26

Chapter 4: Reporting……..……...29

Glossary……31

References……34

Appendixes

A: Sample of Non-Disclosure Agreement (NDA)……35

B: Sample Authorization to Collect and Search Electronic Evidence…..38

C: Sample Chain of Custody Form……...39

D: Sample Cyber Forensics Investigation Final Report……41

LIST OF FIGURES

Figure 1. Sample of Cyber Forensics Investigation Communication Flow Chart……10

Figure 2. Sample Chain of Custody Flow Chart……...14

Figure 3. Sample labeling of computer and peripheral evidence……..19

Figure 4. Evidence / Chain of Possession Tags……19

Figure 5. Non-static bags……..20

Figure 6. Tamper Resistant Tape……..20

Figure 7. Controlled Space Log……21

EXECUTIVE SUMMARY

Cyber Forensics Investigation

Tactics, Techniques, and Procedures (TTP)

Author: Jaja O'Neil

Date: May 1, 2017

Professional Science Masters Degree Program

California State University San Marcos (CSUSM)

While pursuing the M.S. Cybersecurity degree at CSUSM and as part of the semester in residence (SiR) requirement, I opted to pursue a subject not previously performed in my professional life and has the potential of being a real benefit in the realm of cyber forensics. The idea of developing a cyber forensics investigation Tactics, Techniques, and Procedures (TTP) document was conceived from a real-world request to conduct a cyber forensics investigation on a person of interest (POI) who was believed to be transferring proprietary information to an unauthorized person.

The request was from a pharmaceutical company based in San Diego, CA, started by college friends who put together their own information technology (IT) infrastructure. As a cyber-security consultant, I sometimes rely on established methodologies to inform the work I do for my customers. Here, there was no published methodology and I reluctantly turned down the engagement, but it did spawn the question of where would I turn for a guide for conducting a cyber forensics investigation. The guide could be used within cybersecurity firms, cyber incident response teams (CIRT), or within other organizations whereby cyber forensics investigations are conducted.

Tactics, Techniques, and Procedures (TTPs) publications have been a tradition in United States military doctrine. The TTP model contains detailed processes which can be used by people with little, to no instruction from an educator, trainer, or supervisor. The use of TTPs in the U.S. military has been quite successful and another tool in the arsenal from which the civilian, commercial sector can take note and incorporate into its own processes.

Admittedly, during my time of working with my law enforcement committee member, Mr. Darren Bennett, I have learned that the law enforcement community develops TTPs solely to understand the behavior of the target / suspect / adversary! I kept the term "TTP", as this document is intended for a wide audience of organizations that may conduct a cyber forensics investigation.

ACKNOWLEDGEMENTS

I thank the following individuals for their contributions leading up to and / or during the development of this project:

- Teresa Macklin for being patient through tangential episodes of thoughts and ideas, readily sharing her wealth of cyber-related and legal knowledge, and for getting the M.S. Cybersecurity launched in the right direction.
- Darren Bennet for providing a general overview of Federal Bureau of Investigation (FBI) cyber processes, giving me a tour of FBI – San Diego offices, and consistently meeting with me in the evenings, after longs days of fighting crime or while on work travel.
- Dr. Yi Sun for being supportive of our efforts and being ready to extend support when needed.

As a direct result of your teaching, I have learned volumes developing this TTP.

SPECIAL THANKS

Special thanks for the professionalism and warmth of the following organizations at California State University – San Marcos (CSUSM):

- CSUSM College of Extended Learning (EL) and College of Science and Mathematics for starting the M.S. Cybersecurity Program.
- CSUSM Veterans' Center for assisting Veterans in a great transition to academic and professional success.
- CSUSM staff and faculty for making the on-campus college experience seem easy.

Your professionalism, customer service, and attention to detail is greatly appreciated.

Dedicated to:

My wonderful family and friends, near and far, who have admired my pursuit of the M.S. in Cybersecurity at CSUSM, and have waited patiently for the completion of the program.

The active and veteran men and women of our United States Armed Forces, the men and women of law enforcement, and those on the front lines of cybersecurity infrastructure who work for the greater good of a cyber-safe world. Keep up the good fight!

INTRODUCTION

ROLE OF TTP

This TTP is meant to be a reference of steps for investigators to follow when working with electronic equipment and associated evidence. This TTP is not specific to law enforcement, but is intended to support law enforcement efforts if a crime is discovered. The TTP is not the "end all, be all" for all things cyber forensics. Instead this TTP is a starting point in which to collect a series of practices for different situations.

Considering the many topics associated with cyber forensics, this TTP is but the first few chapters in the larger collection of information required to properly collect and store cyber forensics data. So, consider this TTP as the beginning of what should turn into a very large publication, one that will require regular reviews for relevance.

At some point in the future, and after this TTP proves to be quite voluminous. We hope the maturing of this TTP contributes to the genesis of working groups of expert cyber forensic investigators of various industries to validate, agree, revise, and approve the content as technologies, techniques, and laws change. The goal is to standardize the required steps in a cyber forensics investigation down to the task level.

The TTP will not address every cyber forensics scenario, nor should it be the sole reference from which you perform your cyber forensics analysis. In fact, you are highly encouraged to research evidence admissible techniques, precedence, laws, policies, and regulations within the affected jurisdictions as these will vary from jurisdiction to jurisdiction. Further, you are highly encouraged to make appendixes for technical steps to follow in specific situations associated with cyber forensics collection, examination, and analysis.

For this TTP, we are using a hypothetical situation in which a suspect or target / person of interest (POI) can move controlled, classified or unclassified, information from points of access (e.g. client laptop) to an external node. This TTP does not contain practices in identifying and collecting evidence associated with malware or unauthorized intrusion.

The format of the TTP conforms closely to the format used in military TTP publications and technical documents, but does not conform to the usual APA format.

This TTP is expected to be used as a frame of reference and provide depth in understanding of the cyber forensics investigation processes.

SCOPE

Audience.

The audiences for this TTP include cyber incident responders (e.g. Cyber (or Computer) Incident Response Teams (CIRT)), cyber investigators, and supervisors. Cyber incident responders will need to understand cyber forensics investigative techniques even though cyber forensics

investigations may not be their sole job within an organization. Cyber incident responders are usually employed by an organization in which they are expected to perform investigative tasks when there is a cyber-related incident within the employing organization.

There are organizations for hire that offer cyber incident services, for both ongoing, real-time and post-incident, delayed analysis. Real-time cyber incident response personnel work on-site with the client organization and monitor cyber related incidents as they happen and across the network(s). Delayed cyber incident response is addressing the cyber-related incident after the incident has occurred. Additionally, cyber incident responders may arrive while the incident remains active and should be prepared to gather as much e-evidence as possible for further examination and analysis.

This TTP was developed with task lines that start with an action word that is meant for the investigator to execute. This TTP can be a part of an incident responders and cyber forensic investigators toolkit as a reference, but a responder or investigator should be familiar enough with this TTP to determine which task items will be relevant to the investigation. Thoroughness in your processes and records (log) keeping will be the key to your success!

Frame of reference.

The chapter topics are based on the four basic phases (collection, examination, analysis, and reporting) of a cyber forensics investigation per National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response (See NIST SP 800-86[1]).

Content.

The first iteration of this TTP is to cover higher level topics of conducting a cyber forensic investigation. From the higher-level topics, details and a variety of situations and device considerations can be made for future versions of this document.

This TTP was developed for the purposes of determining the activities of an insider threat. Two circumstances were considered for employing this TTP:

1. The insider threat (person of interest – POI) is alleged to have committed acts on client organization information systems (IS) or networks (Nets) that were either criminal or against company (client organization) policy and is no longer with the company; or

2. The POI is alleged to have committed acts on client organization ISs or Nets that were either criminal or against client organization policy and remains with the company.

[1]*National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response* may be found at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

CYBER FORENSICS EVIDENCE COLLECTION TTP

1. Initial communication.

Per National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response, there are four basic phases to the forensics process: Collection, Examination, Analysis, and Reporting. We have added an additional phase at the front-end of the process called Initial Communication. Initial communication is important to establish communication boundaries and methodologies between the parties associated with or who may support the investigation. Communications concerning requests for information (RFI), requests for services (RFS), significant adjustments to agreements and facts concerning the case should be logged as the results may be part of future legal or disciplinary.

- Create an investigation log for the case and begin logging events.
    - The log may be a paper or electronic file formatted with date, time, and entry in the document body. Case number and investigator name fields are at the top of the log pages.
    - When not logging for the case, store the case log in a location with restricted and controlled access. Access to the log file must be recorded and access records retained for a length of time defined by the organization, or perhaps defined by contract.

NOTE: CONTINUE TO LOG EVERY STEP YOU TAKE INTO THE CASE LOG.

- Refer to an approved communications plan for communicating with the organization requesting the cyber forensics investigation services. If no communications plan is defined

for use, refer to National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide.

The following is a sample diagram of a cyber forensics investigation communication flow chart:

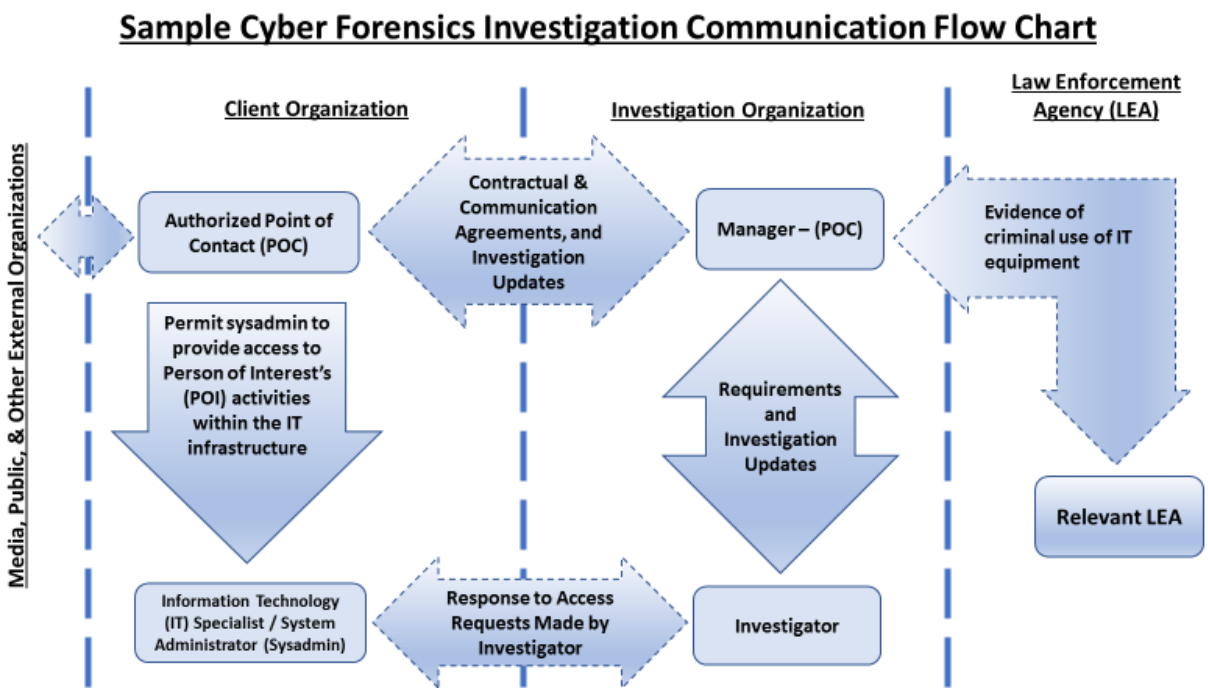


Figure 1. Sample Cyber Forensics Investigation Communication Flow Chart. This figure illustrates how communications might flow between investigators and clients while conducting a cyber forensics investigation.

- Know the terms of any non-disclosure agreement (NDA) (see example in Appendix A) and other agreements established between your own organization and the client organization.

- Affirmatively identify the client's POC for questions or assistance needed during the investigation.
- Provide the client POC an overview of investigation expectations and needs.

2. Collection.

NOTE: Before starting your collection steps, you must step through what you intend to do, what materials and tools you will need, and what controlled storage arrangements will be made for any evidence you collect.

- Identify what controlled storage space(s) will be used for keeping the evidence when the evidence is not being examine or analyzed.

NOTE: The client organization may want to keep the physical property on site while you conduct the investigation. The client organization should be prepared to meet standard of practice controls associated with evidence handling to ensure there is no tampering. Later, hashing of the hard drive is discussed as a requirement for ensuring e-evidence integrity.

- Obtain a copy of the client organization's Acceptable Use Policy (AUP), employee handbook or other material regarding terms and conditions of employee use of client organization's information systems (IS) and networks (Nets).
  - □ Ensure the material states that a user should have no expectation of privacy when using company ISs and Nets.
  - □ Obtain a copy of the POI's acknowledgement to retain for own records, as permitted by the client organization.

NOTE: Your organization should consider setting-up a "go" / "no-go" criteria in moving forward with a cyber forensics investigation. Criteria consideration may include whether you are able to obtain a POI signed AUP, if the AUP contains language that is permissive of a search into e-evidence, and whether or not the e-evidence can be stored in a secure location.

- Create a pack-up kit (PUK) that includes the following:
    - ☐ Pelican case, hard exterior with compartments and foam lining.
    - ☐ Clean media, for example:
        - External drive.
        - USB.
        - CD ROM.
        - DVD R.
    - ☐ Pad lock with key or combination.
    - ☐ Forms identified in Chapter 1 of this TTP (e.g. NDA, authority to collect and search).
    - ☐ Pens.
    - ☐ Pencils.
    - ☐ Markers.
    - ☐ Chalk.
    - ☐ Rulers.
    - ☐ Stickies.
    - ☐ Index cards.
    - ☐ Scotch tape.
    - ☐ Nitrile gloves.
    - ☐ Freshly ghosted imaged laptop.

- □ Non-static evidence bags.
- □ Evidence tags.
- □ Tamper tape.
- □ Computer hard tools, for example:
  - Computer screw driver, Phillips and flat-head.
  - Pill-box for small screw storage.
  - Spare small screws.
  - Wrist grounding strap.
  - Shorting probe.
- □ Spare hard drive case.
- □ Camera.
- □ Chain of custody sheet.
- □ Hardware based write blocker.
- □ Forensics acquisition device or software that is defensible and read only (e.g. Tableau TD3 forensic imager, Forensic Toolkit® (FTK®), Forensic Talon®, Forensic Falcon®, EnCase).
- □ Network taps (e.g. Gigamon, Ixia, Network Critical, Niagara Networks).

- Make requests for assistance, technical or administrative, from the other organization through the client POC.
- Have the client organization sign an authorization to collect and search evidence (see Appendix B).
- Locate and be prepared to present the client POC the Chain of Custody Form (for example, see Appendix C) for signature in releasing the evidence into your custody.

The following is a sample Chain of Custody flow chart:

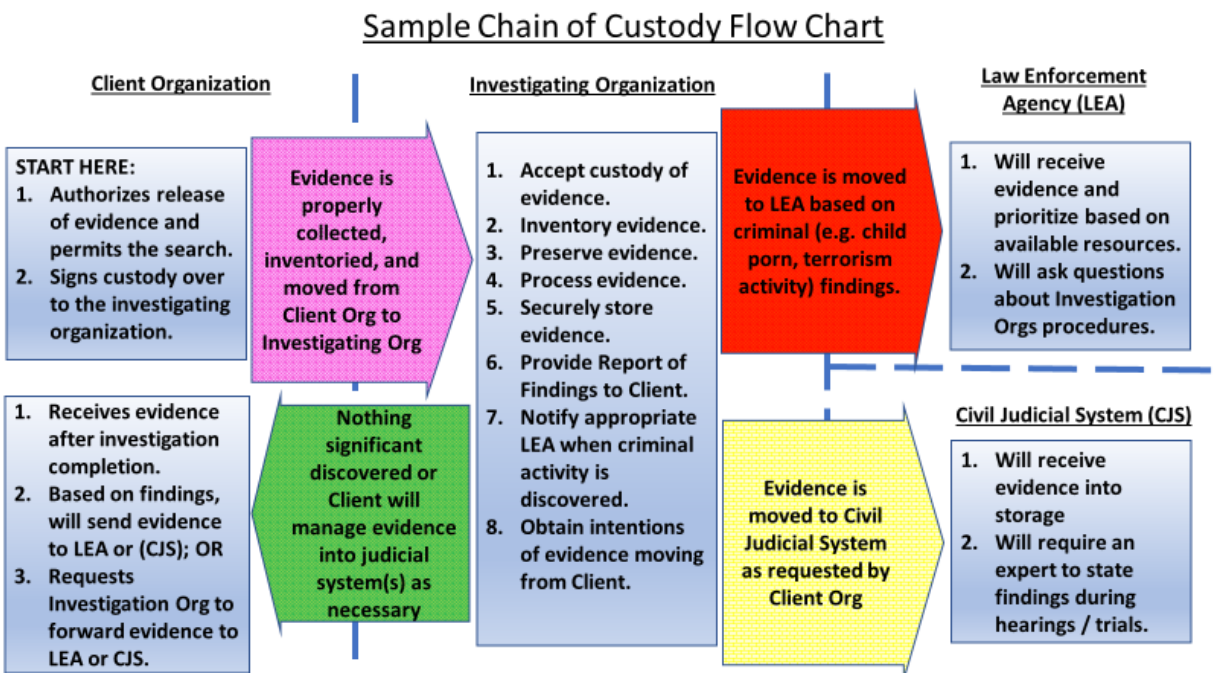


Figure 2. Sample Chain of Custody Flow Chart. The figure illustrates the possibilities of how evidence chain of custody might flow under various circumstances.

NOTE: CONTINUE TO LOG EVERY STEP YOU TAKE INTO THE CASE LOG.

2.1 Electronic Evidence Collection.

NOTE: Use this section if you are not permitted to take the hardware evidence into custody for the purposes of examining and analyzing the resident information.

NOTE: If permitted to collect the hardware evidence for examination and analysis into your custody, you should skip 2.1 Electronic Evidence Collection and start with 2.2 Pictures of the Hardware, Peripherals, and Scene.

- If the computer is found "Off":
    - □ Take pictures as described in 2.2 Pictures of the Hardware, Peripherals, and Scene.
    - □ Continue to the next step upon completion of pictures.

NOTE: If the computer is found "On", the immediate collection of electronic evidence for the purposes of capturing volatile data has the highest priority.

- If the computer is found "On":
    - □ Leave the computer "On".
    - □ Photograph the computer screen if the computer is found "On" to include:
        - Screensaver view.
        - Desktop view to include any desktop icons.
        - Desktop view to include any open files, folders, programs, and associated activity (e.g. typing).
    - □ Collect and store, on an external drive from the toolkit, live (in use) data such as:
        - Central Processing Unit (CPU).
        - Cache.
        - Register content.
        - Routing table.
        - Address Resolution Protocol (ARP) cache.
        - Process table.
        - Kernel statistics.
        - Memory.
        - Temporary file system.
        - Swap space.

- Hard disk.
- Log data (local and remote).
- Archival media.
- Network connection state.
- Logged on user(s).

□ Executing processes.

□ Obtain passwords and store as a separate file and/or place in the case file.

□ Find the hash value of the hard drive by using software (e.g. File Checksum Integrity Verifier (FCIV)).

□ Image the hard drive onto the external drive in which you have placed the previous data associated with the case and label it as "Primary Copy."

- Ensure you do not overwrite the existing data on the external drive.
- Correctly label

□ Place a copy of the image from the external drive (primary copy) onto another external drive (working copy).

- The initial (primary copy) image should remain untouched unless additional copies of e-evidence is required (e.g. working copy was compromised)
- The second (working copy) image is the working copy from which cyber forensics examination and analysis should be performed.

□ Correctly shutdown the hardware after you have verified you have working copies of electronic evidence.

□ Disconnect the power cord for hardware without rechargeable batteries; OR

- □ Disconnect the power cord and dismount any rechargeable batteries for any hardware with rechargeable batteries.
- □ Disconnect any external devices.

2.2 Pictures of the Hardware, Peripherals, and Scene.

NOTE: When taking pictures, use an index card with the case and item number in the photo. Additionally, place a ruler next to the edges of the evidence to demonstrate dimensions of the object(s). Use stickies to label the items by their parts for easy identification in the pictures.

- Take pictures of the area (environment) where the hardware evidence was normally used (e.g. desk area) and other areas made known during the investigation.

NOTE: Pictures must be taken of the external drives that are storing the electronic evidence (e-evidence). This includes taking pictures of the external drives while connected to the hardware from which e-evidence was being collected.

- Take pictures of the hardware (e.g. laptop, desktop, hard drives) being collected, to include the following exterior features:
  - □ Brand name.
  - □ Model number.
  - □ Model code.
  - □ Serial number.
  - □ Operating system.
  - □ Processor type.
  - □ USB ports.
  - □ HDMI ports.

- ☐ Power cable.
- ☐ Ethernet port.
- ☐ Microphone / speaker connections.
- ☐ CD / DVD Drive.
- ☐ Speakers.
- ☐ SD drive.
- ☐ Other items not previously covered.

  (Describe)_____

- Take pictures of the peripheral and connected devices such as:
  - ☐ Cameras.
  - ☐ Microphones.
  - ☐ Power cord.
  - ☐ Ethernet cable(s).
  - ☐ External drive(s).
  - ☐ Router, firewall, switch, modem, and / or phone line(s).
  - ☐ Printer(s).
  - ☐ Other items not previously covered.

    (Describe)_____

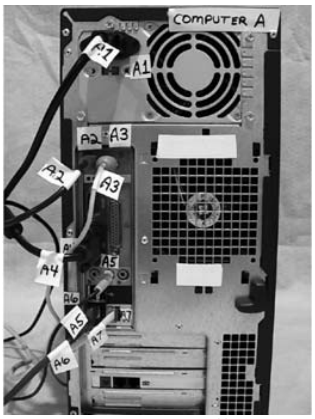


image @ https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Figure 3. Sample labeling of computer and peripheral evidence. This picture show the label tagging of evidence that would be used as Item numbers on an evidence tag. The label tagging includes the computer and all items connected to the computer.

2.3 Evidence Custody Processing.

- Tag items with evidence tags and assign unique serial numbers for evidence tracking. See Figure 4.

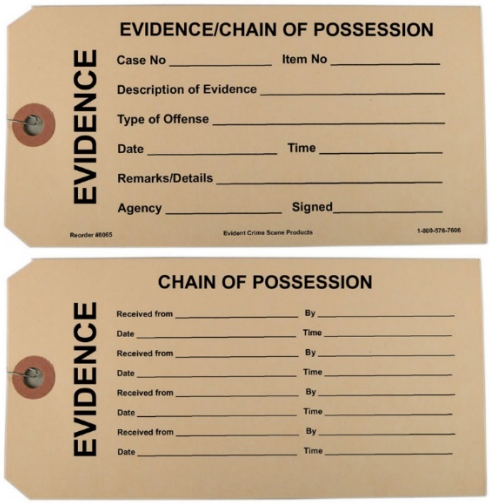


Image @ https://www.shopevident.com/category/evidence-labels-tags/evidence-tags

Figure 4. Evidence / Chain of Possession Tags. This figure is a picture of Evidence / Chain of Possession, synonymous with custody, tags to include fields for required information.

- Tag the external drives used from your toolkit to collect electronic evidence in addition to any other hardware collected as evidence.
- Tag the evidence bag with evidence tags of the same information in which the evidence is being tagged.
- Use non-static bag(s) or container(s) to transport and store the hardware. See Figure 5.

Image @ https://www.shopevident.com/category/evidence-bags/resealable-anti-static-laptop-computer-bags

Figure 5. Non-static bag. This figure is a picture of a non-static bag.

- Use tamper resistant tape and ensure properly labeled. See Figure 6.

Image @ https://www.novavisioninc.com/pages/prd_tamper_proof_security_tape.html

Figure 6. Tamper resistant tape. This figure is a picture of tamper resistant tape that shows "opened" when the tape has been compromised or opened.

- Inventory all evidence and place results in the case log.
- Log every movement (to / from a space, room or location) of the evidence in the case log.
- Log who has custody of the evidence when it is being moved from one location to the next.
- Log each time the evidence enters and exits the restricted and controlled storage area in a controlled space log. See Figure 7.

Organization or Company Name: _____

Controlled Space Manager (Name, phone number): _____

Controlled Space Log – Space Name and Number _____

Log Opened: _____**(Date)** **Log Closed:** _____**(Date)**

Date /Time: (YYYYMMDD / HHMM (PST)	**Case Number:**	**Item Number:**	**"Enter"ing OR "Exit"ing the Space**	**Provide Printed Name and Signature**
Ex.20170501	***Ex. XCGH2***	***Ex. H2-A***	***Ex. Enter***	***Nancy Investigator***__Print) (Signature)
				_____(Print) (Signature)
				_____(Print) (Signature)
				_____(Print) (Signature)
				_____(Print) (Signature)

Figure 7. Controlled Space Log. This picture is an example of a controlled space log for movement of evidence to include the necessary information fields.

2.4 Questioning Witnesses.

The circumstances as to whether or not the organization has identified a person or persons of interested will certainly vary. The decisions in your approach to the investigation and approach to questioning potential witnesses may come down to your level of comfort and experience, the personality of the POI, and comfort of the client organization. The number of people being questioned should be as minimal as possible.

NOTE: One of the objectives to conducting a cyber forensics investigation is to identify who was responsible for the negative cyber activity. Going into the investigation, you may already have a name of the person suspected of the negative cyber activity, but you may have to ask as to why or how was the name obtained as the subject of the negative cyber activity. In the end, you may be looking for the name of the POI based on the e-evidence provided to you.

NOTE: Questioning of witnesses may be done anytime during the investigation and there may be need to re-question witnesses to deconflict facts or findings as the investigation progresses.

NOTE: It is highly recommended that the client POC receive your questions and obtain the answers to provide you.

NOTE: If not addressed in your communications plan or agreement with the client organization, you must determine:

- If the POI remains employed by the client organization.
- Does (or did) the POI only work certain hours?
- Will your presence be during those POI's working hours or different from those hours?

- Has your purpose and assignment been disclosed to the POI or others who may be involved?
- How will the client organization explain your presence if discovered? Your presence could be that of an analyst or systems engineer who is troubleshooting an information system.

NOTE: In the circumstance in which the client organization has identified a Person of Interest (POI), there may be value in interviewing the POI:

- Questioning the POI must be coordinated and approved by the client POC.
- The client POC should review and approve your questions.
- You must record the interview and / or make comprehensive and detailed notes.

- Identify who should be questioned and prepare to question those individuals. Some examples of those to be questioned might be:
  - □ Personnel who were regularly in vicinity of the POI.
  - □ Personnel at the site who have identified themselves as friends with the POI.
  - □ The POI's supervisor(s), if applicable.
  - □ Information technology (IT) system administrators.
  - □ The POI.
- Build a positive and professional rapport with those you intend to ask questions.
- Use a voice recorder when receiving answers to questions concerning the investigation.
- Start the recording by stating:
  - □ Your name as the investigator.
  - □ Applicable case number.
  - □ Name of person you are interviewing.

- ☐ Role of the interviewee.
- ☐ Date of interview.
- ☐ Time of interview.
- ☐ Time zone of interview.
- ☐ Location of interview.
- ☐ Name of anyone else present during the interview (if applicable.)
- ☐ Other pertinent information. _____

- Conduct questioning in a room, away from other people and with a closed door.
- Ask the following questions of the client POC for the client POC to gather the answers for you in supporting the investigation:
  - ☐ Is there evidence of a crime?
  - ☐ What evidence of a crime was committed by the person of interest (POI)?
  - ☐ What is the chronology of the POI's access to the building?
  - ☐ What is the chronology of the POI's access to company workstations or other IT equipment?
  - ☐ What are the damages associated with any incidences or alleged crimes?
  - ☐ What has the POI done to make him/her a suspect?
  - ☐ What is the impact resulting from the POI's actions?
  - ☐ When did the first incident occur?
  - ☐ When was the first incident discovered?
  - ☐ Who has investigated the incident?
  - ☐ Is the person who investigated the incident expected to continue?
  - ☐ What are the names of all users of the computers and devices?

- ☐ What is all of the computer and internet user information?
- ☐ What are all of the login names and user account names?
- ☐ What is the purpose and uses of the computer and devices?
- ☐ Does the POI regularly borrow a laptop when the POI has regular access to a desktop?
- ☐ Does the POI regularly borrow external drives when the POI's job requirements make information accessible via the cloud or server data storage locations?
- ☐ What are all of the passwords associated with the accounts for the computer and devices?
- ☐ What automation applications are in use?
- ☐ What type of internet access is on the computer and devices?
- ☐ What offsite storage is available?
- ☐ Who is the internet service provider (ISP)?
- ☐ What documentation shows the installed software?
- ☐ What are all of the email accounts?
- ☐ What security provisions are in use?
- ☐ What is the Web mail account information?
- ☐ What data access restrictions are in place?
- ☐ What are all of the instant message screen names?
- ☐ What is the Network Address Translation (NAT) history of the device(s) the POI accessed during and since the time of the incident(s)?
- ☐ What is the Dynamic Host Configuration Protocol (DHCP) history of the device(s) the POI accessed during and since the time of the incident(s)?

- □ What are all of the destructive devices and software in use?
- □ What are all of the MySpace, Facebook, LinkedIn or other online social networking Website account information?
- □ What other relevant information can be provided?

- In the situation where a previous investigation may have taken place:
  - □ Does the previous investigator know that we are about to conduct our own investigation?
  - □ Did the previous investigator keep a record of all actions performed through the course of their investigation?
  - □ Did the previous investigator establish a chain of custody log?
  - □ Will I (or my team) have access to the previous investigator's record and custody logs?
  - □ What previous actions have been taken to identify, collect, preserve, and analyze the data on the suspect IT equipment?
- Write the responses to your questions in the case log file.

3. Examination and Analysis.

NOTE: Evidence integrity must be maintained throughout the course of the handling and analysis of the equipment and the associated data. You should be very familiar with the requirements and standards of the labs within the jurisdiction(s) you operate to ensure you meet their standards in case you must turn over the suspect equipment and associated data to law enforcement for further processing and possible prosecution. Examples of lab standard organizations are:

- International Organization on Computer Evidence (IOCE)
- American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB)
- American National Standards Institute-American Society for Quality (ANSI-ASQ) National Accreditation Board (ANAB)
- American Association for Laboratory Accreditation (A2LA)

NOTE: CONTINUE TO LOG EVERY STEP YOU TAKE INTO THE CASE LOG.

- Use the following steps if not completed in Section 2.1 and you have the hardware in custody as evidence:
  - □ Use hashing software appropriate to the host's operating system to find the hash value of the hard drive.
    - Verify and use the hash type (e.g. MD5, SHA version) that is acceptable in your jurisdiction if hashing is required.
  - □ Record or take a picture of the hash value of the hard drive to place in the case file.
  - □ Image the hard drive to an external drive, USB, or DVD disks.
  - □ Verify the collected image's hash matches the hash on the hard drive.
  - □ Label the storage device of the imaged e-evidence with the same case number of the hardware.
  - □ Recommended: Use a write blocker on the hard drive to ensure there is no incidental writing to the hard drive / e-evidence.

NOTE: From this point forward, conduct examination and analysis on the "working copy" (second copy) image. It is recommended that you make a copy of the image to have a backup readily available and avoid the need to return to the primary image copy.

NOTE: If available, use cyber forensic tools for easier collection, examination, and analysis of the e-evidence. Use correct procedures associated with the cyber tool to be used.

- Ensure you can access all files and folders.
    - Work with the client POC to obtain passwords or remove passwords from password locked files.
    - Work with the client POC to remove any multi-factor requirements in accessing any files and folders.
    - Log any original passwords and/or multi-factor authentication (mfa) requirements to access e-evidence folders and files.
    - Log any changes to passwords and/or mfa in accessing the e-evidence folders and files.
- Have the customer identify and draw via Microsoft Office products or Visio the relevant services architectures – local, cloud, hybrid
- Have the customer identify and draw via Microsoft Office products or Visio the relevant network architecture – local, cloud, hybrid
- Have the customer provide a copy of the log retention policy.
- Have the customer identify and record trends in the Network traffic logs. Examples of trends are:
    - Periods of time large files were transported.
    - File names of files transported.
    - Username who initiated file transporting.
    - Source of files being transported.
    - Destination of files being transported.

  - Anomalies in file destinations.
  - Anomalies in file sources.

- Identify and record activity of storage logs.
- Identify and record where the POI has access to cloud storage.
- Identify and record the applications accessed and used by the POI.
- Identify and record any deleted files that are recoverable.
- Identify and record activity in the Event Log.
- Identify and record browser history.
- Identify and record email exchanges, application and cloud.
- Identify and record the POI's access on the information technology (IT) infrastructure (e.g. hardware, software, databases, networks, mobile, personal device(s)).
- Identify and record the services architectures of the POI's accounts to include local, cloud, and, hybrid.

4. Reporting

- Classify the report for dissemination control (e.g. Confidential, For Official Use Only (FUOU), Business Sensitive).
- Ensure a copy of the report is made for your organization and is archived in a restricted and controlled area, physical room or electronically, appropriate to the form in which the report was generated, hard copy or electronically. For example, see Appendix D.
- Provide a copy of the report to the organization requesting the cyber forensics investigative services.

NOTE: Although the report may be with your own organization, the client organization is at liberty to do what they want with the report. The client organization will have full rights to the report, except to the copy that must be retained by the investigating organization. If the client organization does not want you or your organization to retain a copy, you should inform client organization you may not be able to validate the findings of the investigation if, in the future, the client organization desires to pursue legal action against the POI.

- Report any discovered illegal activity that requires immediate reporting by law (e.g. child porn, terrorism related, human trafficking) to the appropriate law enforcement agency (LEA).
    - Ensure client POC is aware of requirements to report to illegal activity that requires immediate reporting to law enforcement.
    - Obtain any new direction concerning the investigation from the contacted LEA and proceed as instructed.
    - Obtain and enter into the log any assigned case number, date, LEA POC information (e.g. name, phone number(s), email(s), address(es)), and intentions with the e-information or equipment and proceed as instructed.
    - Notify the client POC of any changes to custody or the direction of the investigation as a result of contact and instructions from the LEA.

GLOSSARY

TERM	DEFINITION
Analysis	A breakdown of the data sets or structure to lead to an interpretation of the information provided in the data sets.
Adversary	An opponent in a conflict or dispute. Sometimes called the "enemy."
American Association for Laboratory Accreditation (A2LA)	A nonprofit, nongovernmental, public service, membership society with an internationally accepted accreditation programs associated with cyber forensics labs.
American National Standards Institute-American Society for Quality (ANSI-ASQ) National Accreditation Board (ANAB)	Provides internationally recognized accreditation associated cyber forensic labs.
American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB)	A not-for-profit corporation that provides accreditation to private and public crime labs, to include labs associated with cyber forensic investigations.
Case Log	A log of events that may be used in the court of law concerning an assigned case file and number.
Chain of Custody	The chronological written recording showing the collection, custody, control, transfer, and relinquishing of physical or electronic evidence (e-evidence).
Chronology	The order of events with dates, as the events sequentially occurred.
Cloud	An over-the-internet availability of services to include server, application, and storage.
Collection	The process of collecting evidence in a systematic manner.
Communications Plan	Usually developed as part of an overall program or project management plan, is a plan that formalizes who, what, when, and pathway (e.g. phone, email, face-to-face) in exchanging information or requests.
Controlled Access	Controls what items enters and exits the space. May be controlled in the form of a log or radio frequency identification (RFID) tracking system. Cameras are usually installed in these spaces and restricted access is enforced.
Cyber Forensics	Investigative procedures used to collect, examine, analyze, and report findings associated with computing devices and networks, and is made suitable to enter such evidence into the court of law.
Cyber Incident Response	A methodical approach to managing a security breach with the intent of limiting damage, reducing recovery time, reducing costs, and developing a lessons-learned report. The lessons-learned report is used to stop or mitigate the impact of similar events as they occur in the future.

Delayed Response	A response occurring after an event has already taken place.
Dimensions	A measurable aspect of an object as in length, width, depth, or height.
Dissemination	The share, transfer, or circulate, usually information.
E-evidence	Evidence deriving from electronic sources.
E-information	Information deriving from electronic sources.
Event Log	A record found on a computer and is a record of alerts and notifications.
Examination	A detailed investigation.
External Drive	A portable storage device that can be attached to a computer through a wired, usually USB, or wireless connection.
File Checksum Integrity Verifier (FCIV)	Downloadable software used through the command-prompt to compute and verify hash values of files.
Ghost Image	The copying of a hard disk into a compressed file or set of files for the purposes of copying onto many other computers or supporting the reuse of computers after it has been wiped.
Hash	A technique used to produce a value for a storage point of the hard drive. A change in the hash means the information has changed since the previous hash. The hash number is significant in ensuring the integrity of the collected e-evidence.
Image	An exact copy of the contents on a hard drive and is stored on another device, and not stored on the hard drive from which the copy was made.
Incident	An event that is an anomaly to normal operations or goes against policy and may disrupt operations.
International Organization on Computer Evidence (IOCE)	Provides an international forum for law enforcement in the subjects of cyber forensics for exchanging information to include equipment used and test methods used to measure performance.
Interviewee	The person being interviewed.
Internet Service Provider (ISP)	A company that provides internet availability to subscribing customers.
National Institute of Standards and Technology (NIST)	A non-regulatory agency of the United States Department of Commerce that has provided a cybersecurity framework to be used by other entities of the federal government and any organization in need of a framework for developing policies, procedures, and techniques.
Non-Volatile Memory	Long-term, persistent storage and can be found on a computer's hard disk drive (HDD), solid state drive (SSD), or external drive.
Person of Interest (POI)	A person who may be the subject of an investigation, but it is not necessarily a "suspect."
Point of Contact (POC)	A person or organization that acts as a liaison for specific subject areas or function(s) on behalf of an organization or entity.
Real-time Response	Responding to event as it is happening.

Restricted Access	Access is managed with policy and controls the entering and exit of people.
Suspect	A person believed to have been involved in criminal activity.
Target	A person, place, or thing that is the aim of effort or an attack.
Tactics, Techniques, and Procedures	A publication or instruction that incorporates a series of processes with technical and procedural approaches.
Transport	The process of moving (transmitting and receiving) information across an IT infrastructure.
Volatile Memory	Memory that sits on Random Access Memory (RAM)
Witnesses	Personnel who may have witnessed event(s) or able to provide key facts relevant to the investigation.
Write Blocker	A hardware or software used to inhibit the writing, deliberately or inadvertently, of hard drives.

REFERENCES

Luttgens, J. T., Pepe, M., Mandia, K. (2014). *Incident Response & Computer Forensics 3ed.* McGraw-Hill Education.

Widup, S. (2014). *Computer Forensics & Digital Investigation with EnCase Forensic v7.* McGraw-Hill Education.

Scheindlin, S. A., Capra, D. J. (2009). *Electronic Discovery and Digital Evidence in a Nut Shell.* West, a Thomas Reuters business.

Cole, E., Ring, S. (2006). *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft.* Syngress Publishing.

Cappelli, D., Moore, A., Trzeciak, R. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Addison-Wesley.

Kent, K., Chevalier, S., Grance, T., Dang, H. (2006). *NIST Special Publication 800-86, Guide to Integrating Forensics Techniques into Incident Response.* U.S. Department of Commerce.

(April 2004.) *National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* U.S. Department of Justice.

https://info.publicintelligence.net/NITROstudentV2.pdf. Retrieved April 17, 2017.

APPENDIX

Appendix A: Sample Non-Disclosure Agreement (NDA).

Source: http://oz.stern.nyu.edu/startups/nda2.pdf

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

THIS CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT (the "Agreement") made this

_____day of_____,_____(the "Effective Date") by and between

_____a_____corporation, and

_____a

_____corporation, (collectively, the "Parties" and

each individually a "Party").

The Parties are exploring the possibility of engaging in one or more mutually beneficial business relationships (collectively, the "Business Relationship"). The Parties recognize that in the course of their discussions to further the Business Relationship, it will be necessary for each Party to disclose to the other certain Confidential Information (as defined below). Each Party desires to set forth the terms that apply to such Confidential Information.

NOW, THEREFORE, for and in consideration of the foregoing, of the promises and covenants set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties do hereby agree as follows:

1. The Parties shall (i) use reasonable efforts to maintain the confidentiality of the information and materials, whether oral, written or in any form whatsoever, of the other that may be reasonably understood, from legends, the nature of such information itself and/or the circumstances of such information's disclosure, to be confidential and/or proprietary thereto or to third parties to which either of them owes a duty of nondisclosure (collectively, "Confidential Information"); (ii) take reasonable action in connection therewith, including without limitation at least the action that each takes to protect the confidentiality of its comparable proprietary assets; (iii) to the extent within their respective possession and/or control, upon termination of this Agreement for any reason, immediately return to the provider thereof all Confidential Information not licensed or authorized to be used or enjoyed after termination or expiration hereof, and (iv) with respect to any person to which disclosure is contemplated, require such person to execute an agreement providing for the treatment of Confidential Information set forth in clauses (i) through (iii). The foregoing shall not require separate written agreements with employees and agents already subject to written agreements substantially conforming to the requirements of this Section nor with legal counsel, certified public accountants, or other professional advisers under a professional obligation to maintain the confidences of clients.

2. Notwithstanding the foregoing, the obligation of a person to protect the confidentiality of any information or materials shall terminate as to any information or materials which: (i) are, or become, public knowledge through no act or failure to act of such person; (ii) are publicly

disclosed by the proprietor thereof; (iii) are lawfully obtained without obligations of confidentiality by such person from a third party after reasonable inquiry regarding the authority of such third

Appendix A (Cont.): Sample Non-Disclosure Agreement (NDA).

3. party to possess and divulge the same; (iv) are independently developed by such person from sources or through persons that such person can demonstrate had no access to Confidential Information; or (v) are lawfully known by such person at the time of disclosure other than by reason of discussions with or disclosures by the Parties.

4. All Confidential Information delivered pursuant to this Agreement shall be and remain the property of the disclosing Party, and any documents containing or reflecting the Confidential Information, and all copies thereof, shall be promptly returned to the disclosing Party upon written request, or destroyed at the disclosing Party's option. Nothing herein shall be construed as granting or conferring any rights by license or otherwise, express or implied, regarding any idea made, conceived or acquired prior to or after the Effective Date, nor as granting any right with respect to the use or marketing of any product or service. The Parties shall use the Confidential Information only for the Business Relationship.

The obligations of the Parties under this Agreement shall continue and survive the completion or abandonment of the Business Relationship and shall remain binding for a period of two (2) years from the Effective Date.

5. As a violation by either Party of this Agreement could cause irreparable injury to the other Party and as there is no adequate remedy at law for such violation, the non-breaching Party may, in addition to any other remedies available to it at law or in equity, enjoin the breaching Party in a court of equity for violating or threatening to violate this Agreement. In the event either Party is required to enforce this Agreement through legal action, then it will be entitled to recover from the other Party all costs incurred thereby, including without limitation, reasonable attorney's fees.

6. Neither Party makes any representation or warranty with respect to any Confidential Information disclosed by it, nor shall either Party or any of their respective representatives have any liability hereunder with respect to the accuracy or completeness of any Confidential Information or the use thereof.

7. Any provision of this Agreement held or determined by a court (or other legal authority) of competent jurisdiction to be illegal, invalid, or unenforceable in any jurisdiction shall be deemed separate, distinct and independent, and shall be ineffective to the extent of such holding or determination without (i) invalidating the remaining provisions of this Agreement in that jurisdiction or (ii) affecting the legality, validity or enforceability of such provision in any other jurisdiction.

8. Any notice required or permitted to be given hereunder shall be (a) in writing, (b) effective on the first business day following the date of receipt, and (c) delivered by one of the following means: (i) by personal delivery; (ii) by prepaid, overnight package delivery or courier service; or (iii) by the United States Postal Service, first class, certified mail, return receipt requested, postage prepaid. All notices given under this Agreement shall be addressed to the addresses stated at the outset of this Agreement, or to new or additional addresses as the Parties may be advised in writing.

9. This Agreement is to be governed by and construed in accordance with the laws of the state of __. Neither Party shall be deemed to waive any of its rights, powers or remedies hereunder unless such waiver is in writing and signed by said Party. This Agreement is binding upon and inure to the benefit of the Parties and their successor and assigns.

10. This Agreement constitutes the entire agreement and understanding of the Parties with respect to

Appendix A (Cont.): Sample Non-Disclosure Agreement (NDA).

the subject matter hereof, and is intended as the Parties' final expression and complete and exclusive statement of the terms thereof, superseding all prior or contemporaneous agreements, representations, promises and understandings, whether written or oral. Neither Party is to be bound by any pre-printed terms appearing in the other Party's form documents, tariffs, purchase orders, quotations, acknowledgments, invoices, or other instruments. This Agreement may be amended or modified only by an instrument in writing signed by both Parties.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized officers on the day and year first above written.

_____	_____
(Signature)	(Signature)
_____	_____
(Printed Name, Title)	(Printed Name, Title)

Appendix B: Sample Authorization to Collect and Search Electronic Evidence.

From: {Authorizing Person's Name, Title, Name of Company, Address, Phone number(s), Fax number(s), and Email Address(es)}

Date: {Place today's date}

Subj: AUTHORIZATION TO COLLECT AND SEARCH ELECTRONIC EVIDENCE FOR {INVESTIGATOR'S NAME} OF {COMPANY NAME}

I hereby authorize {Investigator's Name} to collect, take pictures, and search suspected evidence concerning {Name of person of interest (POI) or a particular location}.

It is possible the company property collected for evidence may not be returned in the near future.

You will find a copy of {Investigator's Name} identification enclosed, which you may use to confirm {Investigator's Name} identity when {he | she} signs to take custody of the evidence in question.

Please, know the investigator is unable to disclose anything concerning the case, intentions, investigation status, or possible outcomes. Please, refrain from these lines of questioning.

Please, be prepared to answer questions posed by the investigator.

Your cooperation and professionalism are greatly appreciated.

If there are questions, please, contact me at {my phone number}.

Sincerely,

{Your signature}

{Your printed name, Title}

Enclosed: Identity proof of {Investigator's Name}

Appendix C: Sample Chain of Custody Form.

Source: https://www.nist.gov/document-5202

ACME Investigative Agency
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____

Item Number: _____

Submitting Investigator: (Name/ID#) _____

Victim: _____

Suspect: _____

Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location & Storage Info** (Safe or Locker and Drawer #)

Appendix C (Cont.): Chain of Custody Form.

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM

(Continued)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the ACME Investigation Agency.

Appendix D: Sample Cyber Forensics Investigation Final Report.

Source: https://publicintelligence.net

Computer Forensic Analysis Report

MEMORANDUM FOR {Client POC Name}, {Client Organization Name} **Date:** {Report Date}

FROM: {Investigator Name}, {Investigator Title}

{Investigating Organization Name}

{Investigating Organization Address}

SUBJECT: Cyber Forensic Investigation Analysis Report

Person of Interest (POI) / Subject(s) Name: John M. Smith

Born: {Date of birth of POI} (Additional identifiers of POI may be added)

Case Number: {Place case number}

1. Support Requested

{Client POC}, {Client Organization} requested the examination of the submitted digital media seized as a result of suspected criminal behavior related to the theft and subsequent sale of company proprietary information. The request asked that the submitted media be examined for any evidence related to the theft and/or sale of proprietary information, particularly cancer preventing trial medicines, and the existence of possible co-conspirators who participated in, or facilitated the unlawful activity.

2. Status: Pending (or closed)

3. Summary of Findings

The examination of submitted media, which was conducted during the period of {start date} and {end date} resulted in the discovery of numerous image files depicting transporting of proprietary information indicated in the Request for Analysis. A number of the image files also showed the suspect, {POI's last name}, in possession of the materials. Additionally, a review of Internet activity resulted in the discovery of a number of instances where the suspect's computer was used to access Internet auction sites in an attempt to sell proprietary information. While the suspect received numerous email correspondences from individuals apparently responding to his auction advertisements and participated in newsgroup conversations regarding the sale of proprietary information, little information was found which indicates the existence of a conspiracy between the suspect and any other individuals in this activity.

Released by

_____

{Investigator's Name}
Computer Forensic Analyst

Appendix D (Cont.): Sample Cyber Forensics Investigation Final Report.

Items Analyzed

Tag # 01 Western Digital Caviar 31600 Hard Drive
Serial #: WT2891586134
Size: 40GB
Hash Provided: 1234567890ABCDEF1234567890ABCDEF

Tag # 02 One Memorex DVD-R disk containing image files derived from a Fujitsu M1636TAU Hard Drive, Serial #: 08613105, Size: 1226MB:

Suspect_dvd.e01
Suspect_dvd.e02
Suspect_dvd.e03
Suspect_dvd.e04

Hash Provided: ABCDEF1234567890ABCDEF1234567890
Verified Hash: ABCDEF1234567890ABCDEF1234567890
Hash values indicated above are for the entire device image. Individual file hash values were not provided.

Relevant Software

Analysis Software:

Program Name/Version	Program Description
LiveWire Investigator 2007	Live Forensic Analysis Suite
Sawmill Professional 7.2.14	Forensic Log Analysis Tool

Suspect Software:

Program Name/Version	Directory Location	Program Description
AOL Instant Messenger	C:\Program Files\AIM	Internet Chat Application
Microsoft Internet Explorer	C:\Program Files\Internet Explorer	Internet Browsing Application
Microsoft Outlook Express	C:\Program Files\Outlook Express	Email Application

Glossary

Term	Definition
HTML (Hypertext Markup Language)	One of the authoring languages used to create documents on the World Wide Web.
IRC (Internet Relay Chat)	A multi-user chat system, which is real-time communication between two users via computer. Once a chat has been initiated, either user can enter text by typing on the keyboard and the entered text will appear on the other user's monitor. It is often used on the Internet
JPG (Joint Photographic Experts Group)	A graphic image file format.

Appendix D (Cont.): Sample Cyber Forensics Investigation Final Report.

Details of Findings

A complete analysis of all computer and peripheral hardware analyzed (listed above) revealed the following information pertinent to the Request for Analysis and/or of evidential value to this investigation.

Analysis of the Tag #1, image files Suspect.E01 through E04 from 3.0262GB Maxtor hard drive revealed:

Partition 0, NTFS 2.0GB

[Detail your findings in this section relative to the indicated partition located on the hard drive specified. Use narratives, tables, lists, etc. to describe what you found, where, and relevance to the case, etc.]

Partition 1, FAT32, 1.0GB

[Detail your findings in this section relative to the indicated partition located on the hard drive specified. Use narratives, tables, lists, etc. to describe what you found, where, and relevance to the case, etc.]

Disk Free Space, 0.0262GB

[Detail your findings in this section relative to the indicated disk area located on the hard drive specified. Use narratives, tables, lists, etc. to describe what you found, where, and relevance to the case, etc.]

Analysis of Tag #2, black Memorex floppy disk revealed:

[Detail your findings in this section relative to any items of evidentiary value located on the floppy disk. Use narrative, tables, lists, etc. to describe what you found, where, and relevance to the case, etc.]

Analysis of Tag #3, SONY CD-R media labeled "My Plan" revealed:

[Detail your findings in this section relative to information located on the CD. Use narrative, tables, lists, etc. to describe what you found, where, and relevance to the case, etc. In the event of multiple session CDs, it may be necessary to further subdivide this information by specific session.]

Cyber Forensics Investigation Tactics, Techniques, and Procedures (TTP)

JAJA O'NEIL
M.S. CYBERSECURITY CANDIDATE
CALIFORNIA STATE UNIVERSITY – SAN MARCOS

Image @ http://computerforensiclabsinc.com/

Effort

"A good plan, violently executed now, is better than a perfect plan next week."

"Good tactics can save even the worst strategy. Bad tactics will destroy even the best strategy."

-General George S. Patton, Jr. (USA)

ACKNOWLEDGEMENTS

- Teresa Macklin, JD, CSUSM CISO and M.S. Cybersecurity Program Director
- Darren Bennett, Agent with San Diego Office of the Federal Bureau of Investigations (FBI)
- Yi Sun, PhD, Professor of Information Systems
- CSUSM College of Extended Learning (EL) and College of Science and Mathematics
- CSUSM Student Veteran Center
- CSUSM Faculty and Staff

Image @ http://www.csusm.edu/communications/brand-style-guide/logo/

Image @ https://en.wikipedia.org/wiki/Flag_of_the_United_States

DEDICATION

- Family and Friends
- Men and Women of the United States (U.S) Armed Forces (Active, Reserve, and Veteran)
- Men and Women of the various Law Enforcement Agencies (LEA), local to federal, throughout the United States
- Men and Women throughout the world who work diligently to maintain a cyber-safe planet

GENESIS OF THE CYBER FORENSICS INVESTIGATION TTP PROJECT

Image @ bioaccent.org

- Pharmaceutical company requested cyber forensics assistance
  - Request was based on perceived insider threat forwarding proprietary information to external nodes
- Unable to locate a step by step guide on how to successfully execute a cyber forensics investigation
  - There were many references and book, but no complete document with task level guidance and processes
- Opportunity to embark on something new!

Image @ publicdomain pictures.net

INTRODUCTION

- Tactics, Techniques and Procedures (TTP)
  - Historically a military or law enforcement type of publication
  - Reduces need for external guidance in executing tasks
- Role of TTP
  - Reference for Cyber Forensic Investigators, Incident Responders, and Managers
  - Starting point for which to mature the subject area down to the task level
- Scope of TTP
  - Framework of National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86)
  - Investigating insider threat movement of controlled information to external sources
  - Not malware or intrusion related

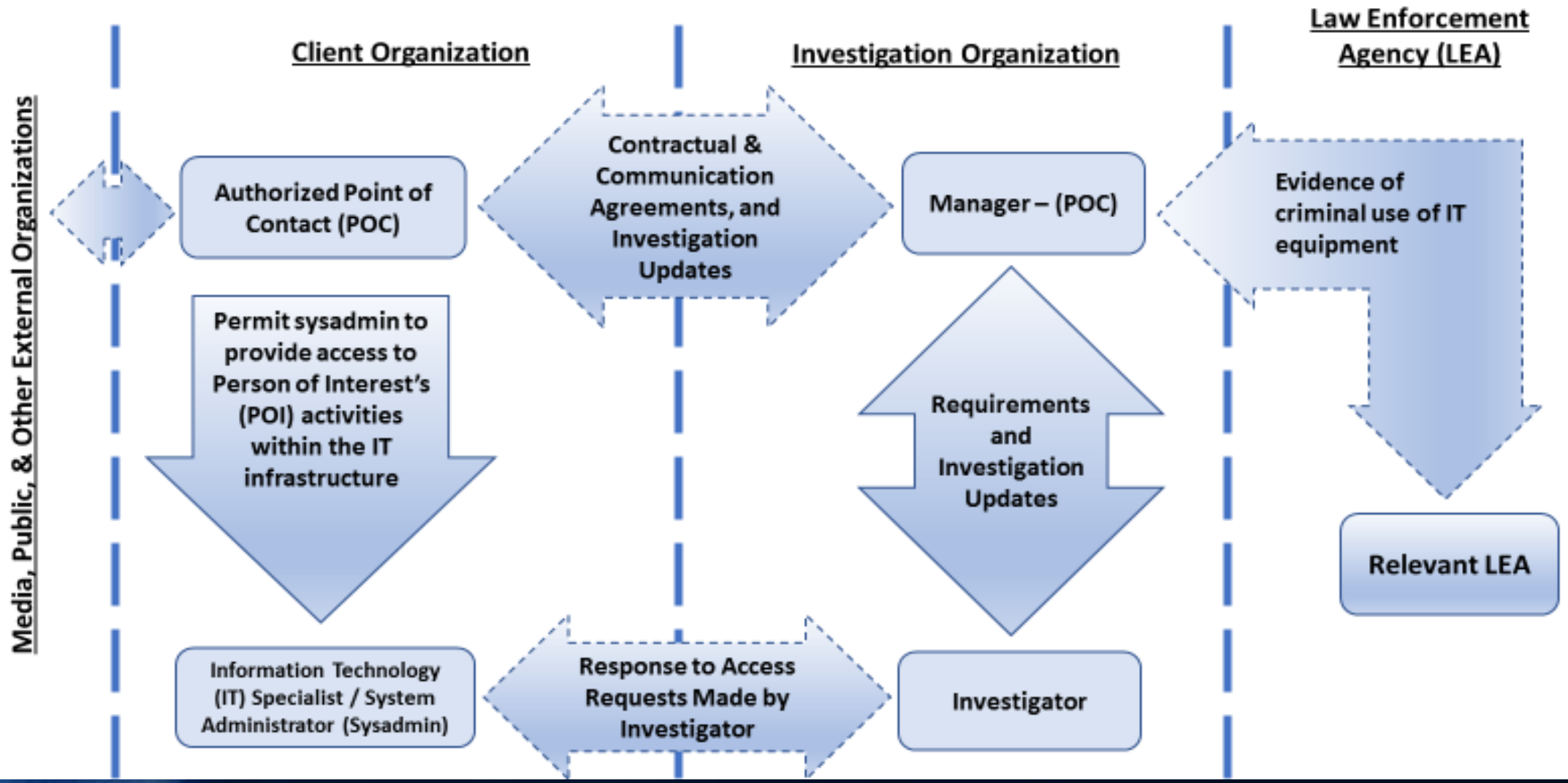
DEVELOPING THE TTP

- Considered framework options … NIST was easier to digest and was selected
- NIST four basic phases:
  - Collection
  - Examination
  - Analysis
  - Reporting
- A front-end phase was added to assist the investigator getting started:
  - Initial Communication
- Examples of concepts, documents, and material were added throughout the TTP

INITIAL COMMUNICATION

- Utilize a Communications Plan to establish boundaries
  - OR use NIST SP 800-86 to guide communication efforts
- Establish a log for recording information related to the case
- Identify the client's Point of Contact (POC) for your needs with the client
- Provide the client POC an overview of investigation expectations

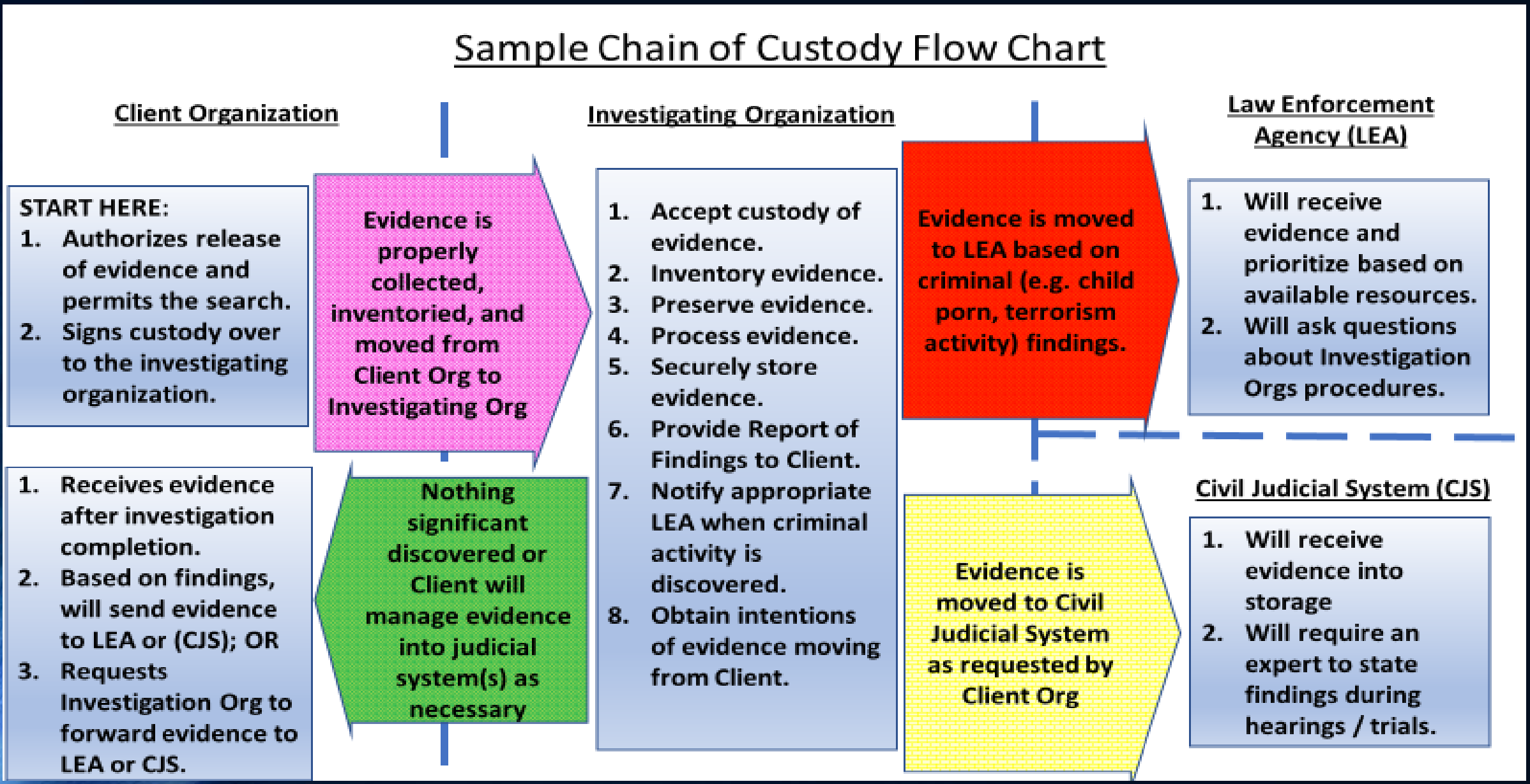
Sample Cyber Forensics Investigation Communication Flow Chart



COLLECTION

- Ensure client has a signed acceptable use policy (AUP) from the subject POI
  - No expectation of privacy on company computers and networks in AUP before work starts
- Have client sign an authorization to collect and search evidence
- Identify controlled storage space for the evidence
- Inspect pack-up kit (PUK) for tools and materials needed to:
  - Properly collect evidence, and possibly
  - Examine and Analyze evidence
- Log collection efforts
- **Establish chain of custody when acquiring evidence**

Sample Chain of Custody Flow Chart



Electronic Evidence Collection

- These steps may be taken onsite if hardware must remain with the client
- Special consideration is given to power status of the hardware, On or Off
  - Power On – Extra steps are involved to capture live memory and network information
  - Power Off – Collection efforts are focused around
    - Imaging of drives and files
    - Capturing log files
    - Capturing data on peripheral devices
- **Data integrity efforts are important, will keep the findings believable**

Pictures of Hardware, Peripherals, and Scene

- Take pictures of the area from which the hardware normally operates
- Label each piece of hardware that is the evidence
- Label each piece of hardware that contains collected

  electronic evidence (e-evidence)

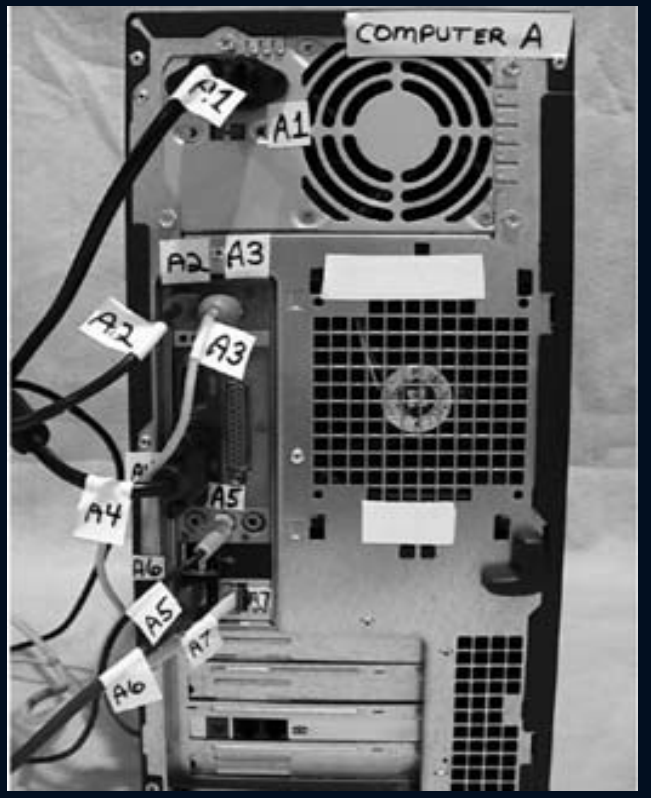


image @ https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Evidence Custody Processing (1 of 2)

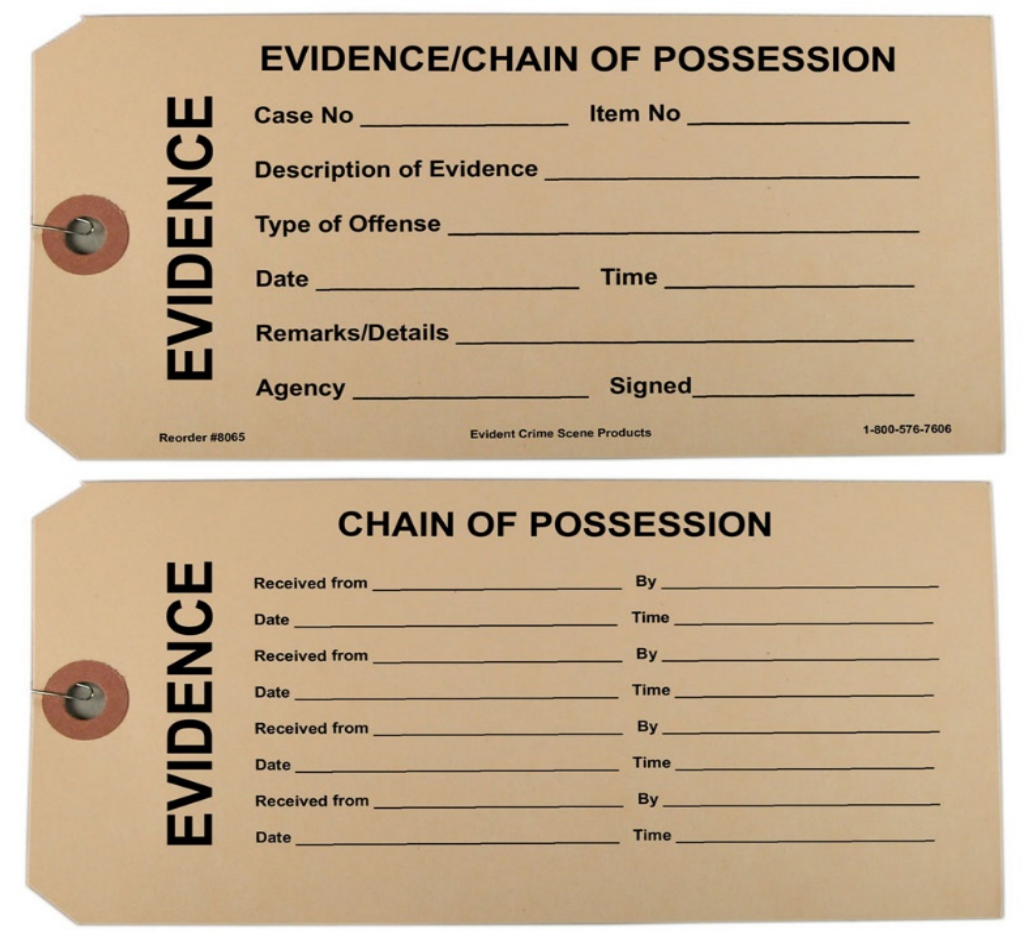


Image @ https://www.shopevident.com/category/evidence-labels-tags/evidence-tags

Image @ https://www.shopevident.com/category/evidence-bags/resealable-anti-static-laptop-computer-bags

Image @ https://www.novavisioninc.com/pages/prd_tamper_proof_security_tape.html

Evidence Custody Processing (1 of 2)

- Inventory all items
- Log movement of e

Organization or Company Name: _____

Controlled Space Manager (Name, phone number): _____

Controlled Space Log – Space Name and Number _____

Log Opened: _____**(Date) Log Closed:** _____**(Date)**

Date /Time: (YYYYMMDD / HHMM (PST)	Case Number:	Item Number:	"Enter"ing OR "Exit"ing the Space	Provide Printed Name and Signature
Ex.20170501	Ex. XCGH2	Ex. H2-A	Ex. Enter	Nancy Investigator__Print) (Signature)
				_____(Print) (Signature)
				_____(Print) (Signature)
				_____(Print) (Signature)
				_____(Print) (Signature)

Questioning Witnesses

- Questioning may be after Examination and Analysis is complete, to focus the effort
- Identify who should be questioned
  - Client point of contact (POC) should obtain most answers for investigator / responder
- Build a positive and professional rapport with interviewees
- Have list of questions prepared
- Use a voice recorder and state relevant information
- Know whether or not a previous investigation took place and what transpired

EXAMINATION AND ANALYSIS (1 of 2)

- Become familiar with acceptable lab standards with the jurisdictions in your area of operations (AO)
- Examination and Analysis are separate subject areas
  - Examination – Extracting data of particular interest
  - Analysis – Analyzing the results of the examination
- Examination and Analysis combined based on how cyber forensic tools quickly parse through and provide results of the information
- Obtain and record (incl. pictures) hash
- Recommend write blocking hardware and image
- Create two copies of electronic evidence (e-evidence)
  - Second e-evidence copy should be the working copy

EXAMINATION AND ANALYSIS (2 of 2)

- Obtain, examine and analyze relevant local, cloud, or hybrid…
  - Services architecture
  - Network architecture
  - Network traffic logs
  - Event logs
  - Emails
  - Browser history
  - Recoverable deleted files
  - Peripheral data
  - Mobile device data

REPORTING

- Classify the report for dissemination control, e.g.:
  - Confidential
  - For Official Use Only (FOUO)
  - Business Sensitive
- Establish a format
- Provide a copy to:
  - Client POC
  - Own records
  - Applicable law enforcement agent (LEA) as required by law, e.g.:
    - Terrorism (Domestic or Foreign) related activity
    - Child Porn
    - Trafficking of Persons

CONCLUSION

- Task level instruction for incident responders and cyber forensic investigators
- Not related to malware or intrusion detection
- Does not specify which examination and analysis tool to use
- Focused on the insider threat behavior of moving controlled information to external nodes
- Phases are modeled from NIST SP 800-86

FUTURE OF CYBER FORENSICS INVESTIGATION TTP

- Can be expanded into:
  - Malware forensics
  - Intrusion forensics
  - Operating system specific approaches
  - Network system specific approaches
  - Use of specific cyber forensic tools
    - Tableau TD3 Forensic Imager
    - Forensic Toolkit®
    - EnCase
  - Network taps

REFERENCES (1 of 2)

- Luttgens, J. T., Pepe, M., Mandia, K. (2014). *Incident Response & Computer Forensics 3ed*. McGraw-Hill Education.
- Widup, S. (2014). *Computer Forensics & Digital Investigation with EnCase Forensic v7.* McGraw-Hill Education.
- Scheindlin, S. A., Capra, D. J. (2009). *Electronic Discovery and Digital Evidence in a*
- *Nut Shell.* West, a Thomas Reuters business.
- Cole, E., Ring, S. (2006). *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft.* Syngress Publishing.

REFERENCES (2 of 2)

- Cappelli, D., Moore, A., Trzeciak, R. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Addison-Wesley.
- Kent, K., Chevalier, S., Grance, T., Dang, H. (2006). *NIST Special Publication 800-86, Guide to Integrating Forensics Techniques into Incident Response.* U.S. Department of Commerce.
- (April 2004.) *National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* U.S. Department of Justice.
- https://info.publicintelligence.net/NITROstudentV2.pdf. Retrieved April 17, 2017.

QUESTIONS and THOUGHTS