Summary

As a side effect globally of COVID-19, many people have been forced to work from home that "causes spike in cybercrime"[1], which leading a trend in cybercrime that how cybercriminals adapted to this situation and take advantage of it. The brand-new digital forensics lab for mid-sized police department come up with a plan for the lab for the next three years. In order to stop "cyberthreats from evolving to take advantage of online behavior and trends,"[2] ISO/IEC 27037:2012 is the information technology security techniques. This is the guidelines for "identification, collection, acquisition and preservation of digital evidence." [3] ISO/IEC 27037:2012 also provides guidance to help individual to handling process and assist organizations that associated to digital evidence in their disciplinary procedures or the exchange of potential in facilitating to jurisdictions. [4] Designing and building a brand new digital forensic lab for med-sized police department is more complicated that meet the requirement of a Med-size digital forensics labs. For addition, INTERPOL (International Criminal Police Organization) guidelines will help to outline the procedures for establishing and managing the digital forensic lab but also help to processing digital evidence.[5]

Accreditation Plan

This section will explain the accreditation of digital forensic lab for INTERPOL a lab must apply the digital forensic laboratories outlines procedure on how to managing the lab and processing the digital evidence of ownership of the prior document to applying for accreditation. This plan also uses the ISO/IEC 27037:2017 standard and ISO 17025 for accreditation. There are the following steps will used to start the accreditation process:

> First step, the digital forensics lab must ensure confidence in the forensic result. When the lab receives numerous cases each year, it will be difficult for the lab to detect the

---

[1] David Klein, "Europol: COVID-19 Causes Spike in Cybercrime," OCCRP, October 8, 2020. https://www.occrp.org/en/daily/13214-europol-covid-19-causes-spike-in-cybercrime.

[2] "COVID-19 Cyberthreats," INTERPOL, accessed October 11, 2020, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

[3] "ISO/IEC 27037:2012 – Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," ISO/IEC 27037 eForensics, accessed October 11, 2020, https://www.iso27001security.com/html/27037.html.

[4] "ISO/IEC 27037:2012 – Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," ISO/IEC 27037 eForensics.

[5] "Global Guidelines for Digital Forensics Laboratories," INTERPOL, May 2019, https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

forensic work. The ISO 17025 has been defining as the process of monitoring the quality of digital forensic process result. Besides, the ISO 27037 provides guidance to collecting and identifying evidence. This process will maintain its performance and the procedure of examining of evidence that follow the international standard.

Second steps, the digital forensic lab must ensure that each examiner follow the same processes and produce quality results. It is very essential that to find out the standard processes but also make sure that examiners implement them. Because the ISO 27037 is promoted good practice methods and procedures for capturing and investigating, it is easier for examiner to compare, combine or contrast the digital forensic results. To produces quality results, ISO 17025 will conduct an improvement to the lab procedures. This implement will continuously be improving and ensuring that the procedures of the lab more quality. For example, the examiners can practice and try to improving their methods or apply ISO 27037.

Third step, there is a completion of the site assessment and skillset checklists for digital forensic lab examiners. The checklist must include skillset for the examiner. They must take note and update their skills.

Here is one of the Approved Accreditation Organizations in the US

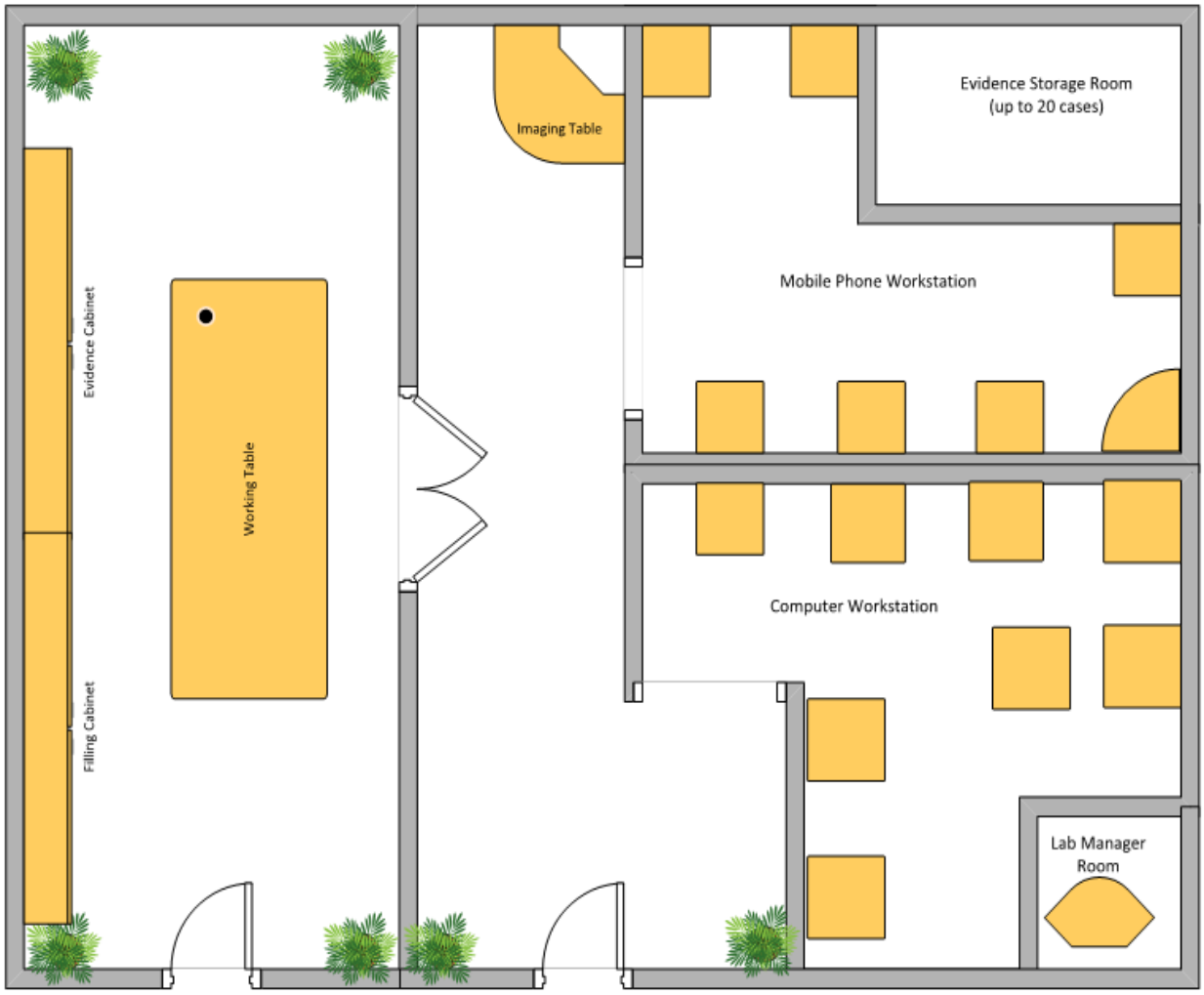
- ANAB is the ANSI National Accreditation Board, which is the longest established provider of accreditation. It based on ISO/IEC 17025 standard.

There is a table below that is the checklist of skillset of INTERPOL for staff (examiners):

Category	Topic	Skillset	
Foundation	Computer Foundation	Organization of computer; How computer stores data; Bits & bytes; Evolution of digital media and storage system.	
	File System	Decimal, hexadecimal, binary; Little endian, big endian; Sectors, cluster, slack space; Metadata, data, filename; FAT, NTFS, EXT, HFS.	
	Introduction to Investigation and Digital Forensics	Law enforcement and regulators; Introduction to forensic science, electronic evidence, and its nature; Categories of electronic evidence; Methodology; Forensics terminologies.	
Identification	Information Gathering	Gather facts of the case online; Preserve the gathered facts	
Collection and Examination	Collection and Examination	First responder roles and SOP; Dead acquisition and live acquisition; Choosing the best data acquisition method; Triage method; Triage tool.	
Analysis	Data Recovery	Storage technology; Damaged hard disk and flash drive symptoms; Logical and	

		physical recovery; Data recovery tools; Recovery of data using tools.	
	Computer Forensics	Operating systems technology; Metadata, registry, artefact; Data Extraction; Data analysis; Data hiding technique; Analytics for large sets of data; Memory Analysis.	
	Mobile Phone Forensics	Mobile phone Technology and evolution, User, telecommunication provider technology, types of data, acquire and analysis tools, preservation of data.	
	Network Forensics	Network Types; Internet history files and Cookies; User Credentials; Network forensic tools; Reading packets.	
	Audio, Video and Image Forensics	Understanding the technology; Enhancement; File Authentication; Comparison.	
	Emerging Technology: - Social Media Forensic - Database Forensic - Drone Forensic - Vehicle Forensic - Shipbourne forensic - Cryptocurrency Forensic - Biometric Forensic	Understanding the technology; Accessing data from the device; Data Extraction; Data analysis; Data interpretation; Reporting the findings.	
Presentation	Report Writing	The format of the report; Effective result presentation to stakeholders.	
	Law & Mock Court	Laws related to cases; International Law; International Collaboration; Presenting expert testimony in court; Introduction to Court structure; Submitting electronic evidence in court.	
Etiquette	Etiquette	Professional Code of ethics, ethical & nonethical code of conduct.	
Lab Management	Quality Management	Understanding standards; Conducting Audit; Quality Management System.	
	Health & Safety	Identify hazards; Health and Safety measures; Self-protection.	

Forensic Laboratory Floor Plan



Inventory

Hardware

The hardware must be working properly that maintained from time to time. Because the storage of digital evidence is very essential to the digital forensic lab, the laboratory need a powerful and speedy server that can handling a large amount of data and digital evidence (original evidence, forensic copies, and data generated while analysis).

Software

For the software purchase, the initial price, yearly license fees, training fees and maintenance fees are needed to be consider for an advance. For example: Helix Pro, Kali Linux, JusticeTrax, ect.

There is a list of equipment below:

- Laptops
- Computer analysis software
- Data recovery software
- Mobile device analysis software
- Internet artefacts analysis software
- Virtual machine software
- Imaging Hardware
- Docking system
- Write blocker
- Secure storage room and storage media (to store data from extracted digital evidence)
- PC toolkit
- Power cable extension
- Printer
- Document shredder
- Computer chairs
- Fluke Network Cable Tester
- Etc.

Maintenance Plan

These practices establish calibration and maintenance requirements to ensure the accuracy and reliability of digital forensic lab. By following guidelines and requirements, the lab managers and technicians can improve their skillsets and perform work properly (meet the requirements) of INTERPOL and general standard of ISO/IEC 27037:2017.

Definitions

The meaning of the following term below:

- DFS is Department of Forensic Sciences
- AFF is the Advanced Forensic Format
- DCO is the Device Configuration Overlay

- DF is Digital Forensic
- DFL is Digital Forensic Laboratory
- EWF is Expert Witness Format
- HPA is Host Protested Area
- IDEN is Integrated Digital Enhanced Network
- IMEI is International Mobile Equipment Identity Number
- MEID is Mobile Equipment Identity Number
- PDP is Personal Development Portforlio
- RAM is Random Access Memory
- SIM is Subscriber Identity Module
- SWGDE is Scientific Working Group on Electronic evidence

Scope

These practices apply to the DFL of police department with guideline and equipment that will prevent potential of cyber threat by the improvement of cyber protection.

Role/Responsibilities

The number staff in the laboratory will depend on how big of the mid-sized police department. The lab manager will in charge of all the case and take responsibility after each analysis. They must review and revise all case for the last result done by technician. Each of technician must understand their roles and their job descriptions that need to be prepared for their team, so they can understand their job profile. Experience and skills are very need for each staff here. There must a set out of clear direction show each staff member understand well and follow it.

Maintenance

While the lab manager keep track of all the unit maintains record of the equipment and instructions, the skill maintains for each staff member are very important. The staff members should understand or strong fundamental; however, they have interest in this field and to the new advanced technology. The staff should update their knowledge and skill regularly. The staff member needs to update their knowledge for the new advance technology. This will keep instruments and equipment well maintain as newly arrival. The lab manager should get scheduled and list of equipment checklist regularly to prevent any potential damage to procedure.

Bibliography

"COVID-19 Cyberthreats." INTERPOL. Accessed October 11, 2020. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

"ISO/IEC 27037:2012 – Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence." ISO/IEC 27037 eForensics. Accessed October 11, 2020. https://www.iso27001security.com/html/27037.html.

"Global Guidelines for Digital Forensics Laboratories," INTERPOL. May 2019. https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf.

Klein, David. "Europol: COVID-19 Causes Spike in Cybercrime." OCCRP, October 8, 2020. https://www.occrp.org/en/daily/13214-europol-covid-19-causes-spike-in-cybercrime.