Midterm

CYSE 407 Digital Forensics

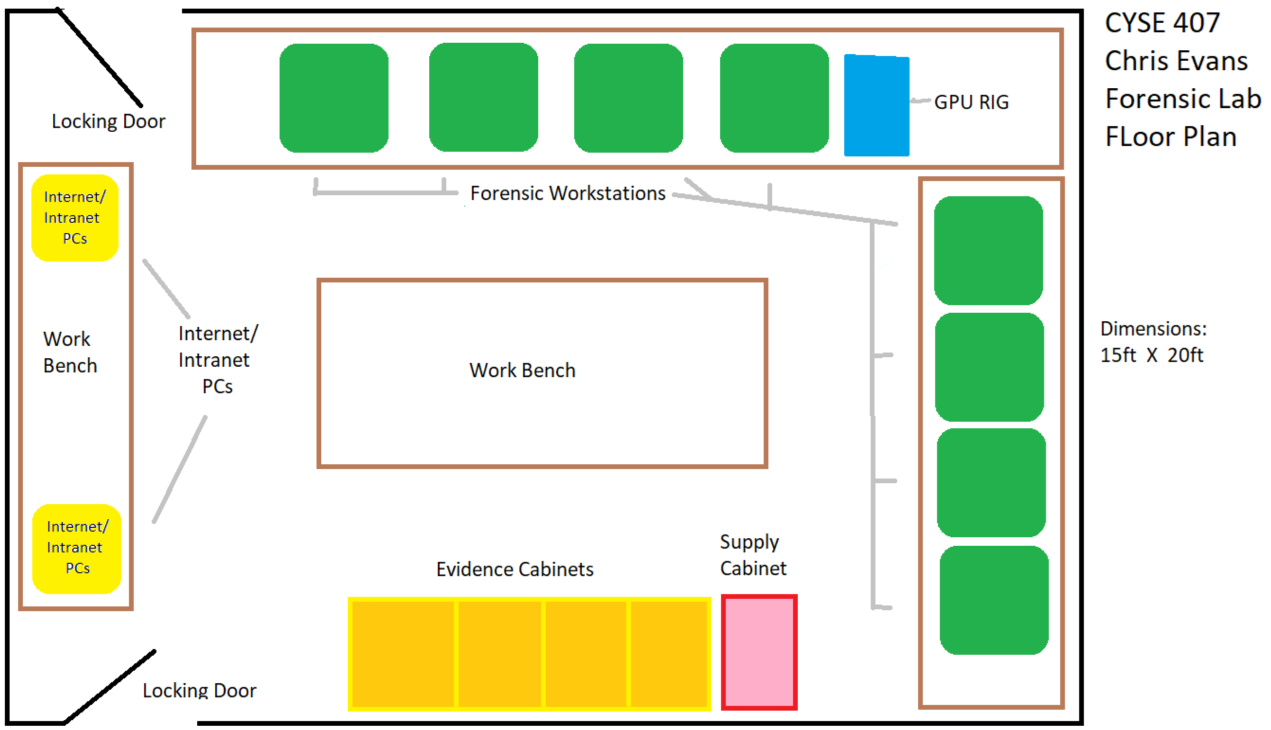
Chris Evans

01206431

Summary: This document outlines the creation of a Digital Forensics Lab for the Metropolis Police Department. This document is designed to be a guide for the function and operation of the Metropolis Digital Forensics Lab for 3 years from the date of finalization. The Digital Forensics Lab will be a dedicated lab to digital investigations, searching for and recovering evidence from various hardware devices, operating systems, and software systems for the use of law enforcement investigations and in assistance of the District Attorney's office. Defined in this document is the policies, processes, and procedures that are used to ensure integrity of analysis and results. The Digital Forensics Lab will be in compliance with leading industry standards like ISO/IEC 17025 and accredited by the ANSI National Accreditation Board (ANAB). Further this document will outline a physical diagram of the Digital Forensics Lab, Inventory considerations, Lab maintenance plan, and Staffing plan.

Diagram

The diagram below shows the set up and positions of our hardware and workstations. Space is necessary to preform forensic work on hardware and so large desks and workbenches are available throughout the lab. The two doors are equipped with physical locks and keys are only given to authorized users. These door locks can be upgraded to key card locks in the future if desired. The forensic lab should have floor to ceiling walls to prevent unauthorized access. The evidence cabinets will also lock and can contain any evidence currently being examined which will increase the security of the chain of custody. There are eight forensic workstations for use by investigators and two internet/intranet connected PC's that can be provided by the Metropolis Police Department. The additional GPU rigs will be available to any investigator staff who requires their increased power, and its allocation will be decided by the lab manager. Evidence cabinets will contain locks and can only be accessed by logging the chain of custody with the lab manager. The supply cabinet will contain hand tools, extra data drives, connecting cables, evidence tags, anti-static bags, software and laboratory manuals, and any other items needed. Additionally the forensics lab will have CCTV cameras that will allow us to see any intrusions or non-professional behavior in the laboratory.



Inventory

Our inventory will be split into hardware and software needs. Our Hardware is designed to last longer than the recommended 1.5 year life cycle for Digital Forensic Labs. We believe we will be able to stay technologically capable with this set up for 4 years before we begin searching for new hardware solutions. Our forensic workstations are repurposed gaming computers which will afford our lab the ability to use powerful hardware in analysis and cryptographic hashing. Additionally, we will require 4 additional video cards to be used as a support for intense cryptographic workloads and to serve as spare parts should a workstation video card need to be replaced. The lab manager will be responsible for maintaining inventory and functional state of workstations, as well as upgrades and replacements if necessary.

-Hardware Inventory

8 X Forensic workstation computers with following specifications

CPU:	Intel Core I9-12900k
CPU Cooler:	Artic Liquid Freezer II 280
Motherboard:	MSI PRO Z690-A AYX LGA 1700
Memory:	Crucial 32 GB DDR5-4800
Storage:	Seagate FireCuda 520 2Tb M.2-2280 NVME Solid State Drive
Video Card:	Gigabyte GeForce RTX 3090 24GB Gaming Video Card
Case:	Fractal Design Torrent ATX Mid Tower Case
Power Supply:	Super Flower Leadex III Gold 850 W 80+ ATX Power Supply

2 X Internet/intranet connected workstations as supplied by the Metropolis Police Department

4 X Gigabyte GeForce RTX 3090 to assist in heavy workloads

4 X Digital Cameras for record collection

4 X External CD Drives

1 X External Floppy Drive

2 X Hand Tool set

8 X External Solid State Drives to be used for collecting evidence. To be replenished as used or worn

8 X 256 GB Thumb drives. To be replenished as used or worn.

2 X SCSI Card

4 X Hard Drive Write Blockers

Various Connection cables, anti static evidence bags, and office consumables.

-Software Inventory

In order to have a fully functional Digital Forensics Lab we will need multiple software and operating systems. Additionally, we will need a personal library of older versions of some software if compatibility is an issue. We may need Operating System specific versions of the same software packages. Some enterprise software will require multiple software licenses to be used in our lab environment.   Software and Operating systems are listed below.

Microsoft Windows 11 and older versions

Apple Macintosh OS 12 Monterey and older versions

Kali Linux and other Linux based Distributions.

WinHex

Microsoft Office

Visual Studio,

Perl

Python

Quick View

ACDSee

ThumbsPlus

IrfanView

OSForneiscs

FTKImager

ProDiscover

Mini-WinFE

SANS Investigate Forensic Toolkit

Helix Pro

Wireshark

Autopsy

Sleuth Kit

Forecepoint Threat Protection

Magnet AXIOM

Lab Accreditation Plan

In order to stay compliant with the highest digital forensic standards set by ISO/IEC 17025 we will be achieving and maintaining a ANSI-ASQ National Accreditation Board (ANAB) accreditation for our forensic laboratory. This is an industry leading certification providing worldwide forensic labs a certification that their task and functions are correct and consistent for all cases investigated. We will begin the certification process by reviewing requirements and documenting compliance with them. The accreditation process will then include: Quote, Application, Document Review, On-site Assessment, Resolution of Non-conformities, Accreditation Decision, and finally Conformance Monitoring and Reassessment.

We will also be working toward National Institute of Standards and Technology accreditation as a Forensic Science Service Provider. This is a multi-step process which involves our lab implementing the following steps:

1. Written procedures for secure evidence identification, collection, preservation, and maintenance.
2. Written reports with results of examinations and clear reports procedures.
3. Technical and Administrative review of reports and supporting records.
4. Testimony monitoring
5. Note taking
6. Technical procedures written to include information regarding instrument and equipment maintenance.

7. Training program including goals and objectives, materials covered, assessment mechanisms, and training topics.
8. Proficiency testing
9. Corrective and Preventative action process.

Lab Maintenance

Lab maintenance should be conducted constantly to make sure staff are safe and healthy. Damages to walls, tables, or floors should be repaired in a timely fashion and cleaning crews should only be allowed to enter the lab with supervision of staff. Dust should be removed as much as possible to prevent damage to hardware from congesting airports or conducting static charges. Trash should also be separated into sensitive and non-sensitive materials, with sensitive materials being disposed in a secure manner and with their destruction confirmed.

Staffing

-Lab Manager: Create process for managing cases and review those processes as well as creates and monitors lab policies. General manager of the laboratory, will be responsible for the needs of the lab, enforcing ethical standards, budget considerations, and planning updates and acquisitions for hardware and software. The lab manager will ensure quality of work performed in the lab and maintain physical security procedures for lab access, evidence handling and report filing. The lab manager will be responsible for scheduling staff for investigations that require long hours. Requirements that the lab manager have digital forensics certifications and training from certifying organizations, this will require continuing education as well. Acceptable certification organizations include, ISO, CompTia, GIAC, ISC2, IACIS, ISACA, and Cisco.

-Lab Staff: Should possess skills to perform tasks at direction of the Lab Manager, including but not limited to hardware knowledge, software knowledge, Operating Systems knowledge, and deductive reasoning. Staff should be familiar with investigative software tools as well as posses technical digital forensic training to update their skills. Staff should also be certified with an approved certification organization and possess technical skills required to perform duties assigned by the lab manager. Acceptable certification organizations include, ISO, CompTia, GIAC, ISC2, IACIS, ISACA, and Cisco.