PROPOSAL FOR THE DEVELOPMENT OF COMPUTER FORENSICS INVESTIGATION LABORATORY

IE4062

Cyber Forensics and Incident Response

4th Year, 1st Semester

Continuous Assessment - Individual

Proposal for the development of Computer Forensics Investigation laboratory

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

Declaration

I certify that without acknowledgment, this report does not include material previously submitted for a diploma or a degree from any university and does not include material previously published or written by another person to the best of my knowledge and belief unless the correct reference is made in text

IT Number : IT17083256

Name : Hashini Amarasena

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Computer forensics is in essence at the cutting edge not as an advanced high-tech specialty, but as a viable and crucial business function of the 21st century. As emerging technology and software continually introduced, companies have processed more and more information electronically. Part of this has resulted in legislation that guarantees that this information is collected and maintained in a way that ensures fair compliance with privacy, corporate integrity and a variety of other issues. The use of computers in traditional criminal activities such as drug trafficking, vice activities and "good old" robots and killings, computed crimes committed over the internet, information gained by the general public in general (for good or for bad), has made the computers the same company as traditional criminally active tool[1]. Industry needs to treat computers the same way it would treat any business risk, with knowledge and measured intelligence. The only method of curbing, tracing, and apprehending these cyber criminals is through a systematic investigation through computer forensics. Effective and efficient investigations rely on the establishment and maintenance of a computer forensic laboratory that end-to-end withstand and optimizes the entire investigative process and can address to optimizes any evidence-based challenges. In recent years, this ever evolving trend both in conventional and organized crime, including all facets of trafficking, has led to a resurgence of interest on the part of governments and the international community in strengthening or establishing laboratories for computer forensics Investigation laboratories.

A computer forensics lab is where you conduct investigations, store evidence, and do most of your work[2].In general, for your work, you need a variety of forensic hardware and software.[2].You are using the laboratory to house your tools, current software and conventional forensic workstations. You must also ensure that you have defined policies, processes and procedures before starting case work so as to ensure that the analysis and its results are comprehensive.[2]. Many organizations have developed guidelines to implement their own policies and processes [2].what's Most significantly, you follow the policies and procedures you have placed in place to ensure continuity in your output[2].

This proposal is to request the management to provide facility to establish computer forensic laboratory. The Digital Forensics Service offers an easy-to-understand cost-effective solution to today's business environment The practice concerns the delivery of a Computer Forensics Service on the high-tech market, targeted at law enforcement, government departments, major corporations, and small to medium enterprises. The demand is about to boom and we are prepared to exploit it. The guidelines and recommendations in the proposal are an overall resource to which anyone in cyber security field can refer when designing and developing a new computer forensic laboratory. Investment, workforce tools and proven skills and culture within the company play a major role in the strategy in this business case. The above includes adopting common laboratory measures, prevalent quality standards, benchmarking standards for all areas of concern, identifying and disseminating best practices, continuous metric monitoring and the use of cost-effectiveness reviews. The person occupying the building should be involved in the design / building company from the outset to explain their particular laboratory requirements. Flexibility is also an essential factor in driving a forensic laboratory's design and configuration[3].Investigation laboratories must be versatile to support adaptability and change or risk obsolescence in a few years. The driving factors are worker requirements and functional processes. Quality laboratory facilities are expensive and the buildings in which they are delivered are also often expensive. Cost cutting that affects the testing standard of the laboratory cannot be an option .It should be decided, at the outset of the process, whether the project is primarily driven by needs or budget? Or Will the laboratory requirements dictate the budget, or else will the budget preset and laboratory economically limited to a particular amount at the outset? Therefore need to Be prepared to defend against issues arising because of the costs involved..

The guidelines in this proposal have been designed to establish effective computer forensic laboratory which begun to provide insight into how a laboratory should carries out its mission without compromising quality to preserve the profession's integrity and objectives, maximize organizational efficiency, guarantee economic resource expenditure and provide employees with a safe work environment.

BUISNESS CASE FOR DEVELOPING A FORENSIC LAB

I CAN DELETE THE PHOTOS,

BUT FIRST YOU HAVE TO PAY

2. BUSINESS CASE FOR DEVELOPING A FORENSICS LAB

The explosive growth of computers and other digital devices has geometrically enhanced the severity and occurrence of cybercrimes worldwide. These cybercrime proliferations pose cyber and national security threats. Due of its dynamic existence the internet is totally changing crime inquiries. The dynamism of the Internet makes a website used to commit a crime different or missing the day following. The Computer Forensics Investigator has become imperative to find the missing link in such a cybercrime. Computers reveal a wide variety of criminal and illegal activities. Network-based criminals are not the only ones who store computer information Many criminals commit murders, abductions, sexual assaults, extortion, drugs, espionage, terrorism, gun trafficking, robbery, gambling, money laundering and economic crimes, criminal hacking, scams ,etc. The information on these criminals' computers are the keys to identifying suspects and the data provides the most important evidence in order to convict and punish them. In order to access digital information on different hardware, software and mobile devices it is therefore crucial to have the tools and the procedure [4]. The only way to combat cybercrime is to train competent experts in computer forensics who investigate and prosecute cybercrimes as well. Several official and organizations attempts to standardize and deal with digital investigations have been made[5].

For any number of different cases, forensics can be used.. Depending on the nature of the crime, any device could be used to provide evidence of what is, was or is going to happen. These types of investigations analyze the data extremely closely not only the files currently in existence, but also the metadata for almost any item on the device. This includes checking when the file was first created, when it was edited and saved, and who could have done that. Any number of cases can be resolved using this process. Here's just a couple of things to look at as an example:

- Intellectual Property Theft and Industrial Espionage.
- Investigation into bankruptcy
- Inadequate office email and Internet access.
- Regulatory Compliance.
- Employment Disputes.
- Investigations into fraud and forgery..

Computer forensics protects digital evidence against potential changes, destruction, corruption or design or carelessness infection. The development of forensic sound waves useful for data analysis by providing evidence duplication mechanisms[6]. As such, it prohibits complaints of corruption or abuse by investigators, with the exception of ensuring facts before the court. It can also remove any relevant files on suspicious systems, like accessible, secret, secured passwords, slack, swap, encrypted as well as certain deleted files[6].Adding the ability to practice sound computer forensics would help to guarantee the overall integrity and survival of entire network infrastructure.

2.1. The Business

- The ultimate goal of the Computer Forensics laboratory is to provide a reliable and competent service to its clients that meets the need for on-going operations and new legislation on law enforcement agencies and departments.
- Back A variety of customer services will be available, all of which are based on computer forensics. The lab will provide digital imaging tools and research facilities for the use of evidence in courts and industrial tribunals. The laboratory offers people as expert witnesses for the courts and, where necessary.
- will provide training, cite visits and workshops to organizations in Computer forensic techniques.
- The staff can know and benefit from the areas that sustain a broader organizational infrastructure by conducting the forensic investigations.

- Commercial Organizations
- Local Law Enforcement
- Government Departments etc;

CUSTOMERS

- Government Market
- Banking, And Financial Services Market
- Law Enforcement Community
- Retail Market
- telecommunication markets

MARKET

- Via Word Of Mouth
- Through Existing Customers And Contacts

CHANNELS

- Charged On A Per-job Basis
- Fees Will Be Based On The Range Of Services Required

PRICING

BENIFITS

As This is not based on extravagant sales expectations The business has a high potential profitability. In fact, the assumptions concerning the likely adoption of new customers were modest. A high profit is due to the fact that the Computer Forensic Service is a substitute company which has low marginal service costs compared with the potential income.

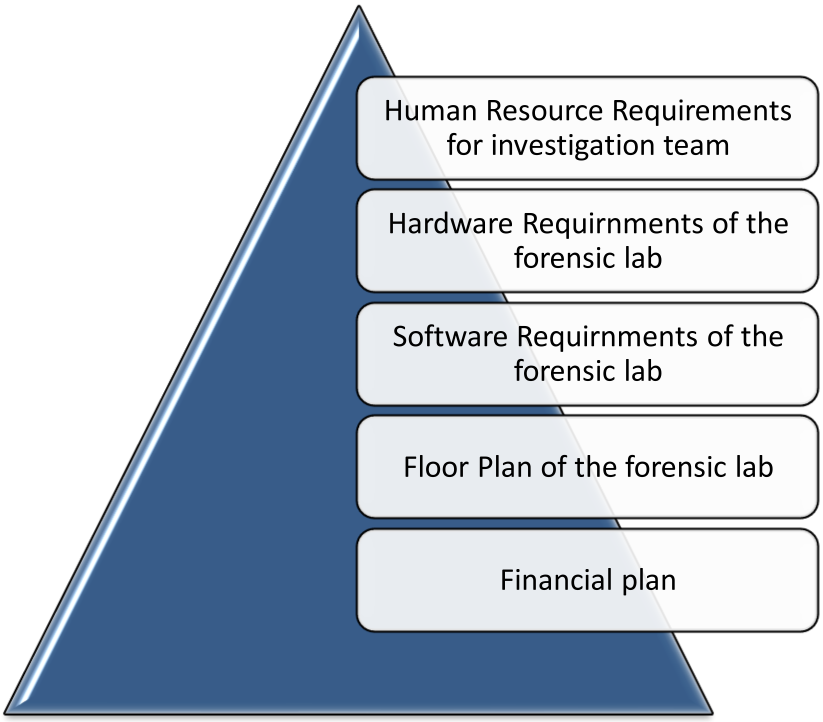
ANTICIPATED REVENUES AND COSTS

Refer Financial plan section for Three years budgetary projection, excluding taxes, of revenues and expenses, with analysis on the assumptions underlying the projections. The company will start trading on the first month of 20XX. These estimates did not include effort expended by staff. The startup costs are expected to be $110k.

RESOURCES

The availability of sufficiently trained employees is important to the success. This issue is the second biggest obstacle to the company's performance. The Laboratory is not supposed to have a crisis in the short term. The brutal reality, when it becomes extremely successful, is that the Computer Forensic Service business may experience problems currently facing law enforcement agencies in the longer term. The level of preparation and expertise required to become an effective Computer forensic investigator makes the potential for highly paying business employment a reality. There are no established specifications for external assets, equipment and materials suppliers other than free market operating tools, software and communications services.

The workflow and procedures that directly impact quality of the evidence discover. A key issue to consider is the accreditation of the Computer forensics laboratory. Accreditation shall ensure that the laboratory or one of its facilities complies with the agreed requirements of the Authority for using reliable procedures, appropriate hardware and software tools and professional personnel to perform its tasks [5]. The cost, quality and reliability of the equipment, software and other things should be assessed when the forensic laboratory is being accompanied. How the process is managed is the key to its success. Some of the most important laboratory management requirements are:


Human Resource Requirements for investigation team
Hardware Requirnments of the forensic lab
Software Requirnments of the forensic lab
Floor Plan of the forensic lab
Financial plan

This proposal concerns the establishment of a Computer Forensics laboratory and gives a short explanation about the significance of setting up a computer Investigation laboratory,A business case and a guidance to setting up an effective forensic investigation laboratory. Developing a business plan is a subjective matter The establishment of a Computer forensic investigation laboratory is not a trivial thing and will be subordinate to a set of considerations and regulations. The design and construction of a forensic lab is a complicated undertaking. [3]. Issues relevant to design include factors present in the construction of every building and with an enhanced regard and specific criteria concerning environmental health, safety and security, hazardous materials, management, operational performance, adaptability, evidence protection as well as budgetary concerns.

Here the proposal is about a laboratory that tends to focus on a particular niche, such as computer forensics. After the scope of a laboratory is defined, it will be better able to deal exactly with what issues and how relevant they are for the laboratory. In addition, the scope creep and expansion of services should also be taken into account in future. Beginning with an adequate laboratory and lab space for a wide range of operations, while evaluating current resources to ensure that the skills and equipment required for efficient forensic science services are available. But proper planning and preparation can help to strengthen the overall computer research process, including the functional requirements of the proposed forensics disciplines to be suited and of the equipment that will ultimately save money and time, productivity and procedural efficiency. It is also necessary properly maintained after it is built and to processed in compliance with appropriate regulations and good practices. In future, Computer forensics will play an increasing role in the criminal justice system as a range of innovations are continued to be integrated into our daily lives. As the Computer forensic discipline matures, criminal organizations can recognize and accept the contribution that they can make in identifying and processing evidence more readily. This proposal covers all areas, highlighting important considerations to consider in order to organize, control and manage a computer forensics investigation laboratory that is safe and efficient.

EXECUTION

- HUMAN RESOURCE REQUIREMENTS FOR INVESTIGATION TEAM AND THEIR TRAINING NEEDS.
- HARDWARE REQUIREMENTS FOR THE COMPUTER FORENSICS LAB.
- SOFTWARE REQUIREMENTS FOR THE COMPUTER FORENSICS LAB.
- FLOOR PLAN FOR THE COMPUTER FORENSIC LAB.
- ADDITIONAL REQUIREMENTS

3. EXECUTION

This section outlines the issues to be addressed and the justification for developing a business plan for the creation and operation of the forensic laboratory and more about the information on the potential throughput, the number of employees, and the amount and type of equipment needed to fulfill the expected workload. The staffing training requirement and the accomplishment of a balance between enough training to establish and maintain an efficient unit and excessive training, which can lead to unnecessary costs and to make the company vulnerable to wrestling by competing companies or organizations.

3.1. Human Resource Requirements for investigation team and their training needs

For any organization to secure its cyberspace effectively and efficiently, a well trained workforce is necessary In the face of increasing computer crimes losses, terror and security breaching due to growing cyber terrorism, cyber warfare, and hacking and cybercrimes, training is becoming essential for skilled computer scientists. In order to carry out computer investigations, the organization must be competent and effective in the identification and combating of cases of cybercrime. Such capable of managing cybercrime events is combined with technically skilled people, policies and techniques. Personnel in the team or the unit must be in a spot to identify and specify the computer forensic equipment and infrastructure specifications and to assess and configure the appropriate tools. It is important for forensic lab staff to gain skills not only in specific analytical techniques, but also in the fields of forensic sciences in which they are employed. As In every work domain, effective selection of staff is crucial. However, poor selection in the profession of Computer forensics can lead to catastrophic results as a result of poor processes. It is therefore vital that a well-considered process of selection of employees provides the best available candidates The laboratory should also be fitted with up to date equipment, forensic tools and software for all operating systems and all system files for investigation. The main roles to be undertaken within the laboratory are listed below.

LAB MANAGER

- Ensure that new staff are trained to the section's and in compliance with quality standards [9].
- Ensuring the proper working conditions of hardware, software and equipment in the laboratory[9].
- Establishes and promotes the quality management processes for laboratory staff to track, such as outlining of what to do when a case arrives, the registration of facts, who may access the laboratory, and the creation of reporting guidelines[2]. To ensure the lab's efficiency and sets reasonable production schedules for processing work[2].
- Establish and supervise laboratory policies for employees, provide a safe and secure environment for employees and evidence and accounts for all activities carried out by laboratory employees[2].
- ensure that all quality standards for the laboratory are met as needed [9].

COMPUTER FORENSIC EXAMINERS/ANALYST

A computer-forensic Examiner and Analyst are proficient at the expert level to use one or more forensic tools and processes[7][10]. This role usually has at least a forensic tool vendor certification,experiences on the job and documented professional experience for the particular products they use.[7][10]. These people will also need to have tertiary qualifications, for example in computer science or digital forensics, in a suitable discipline.

- Conduct Digital data extraction and recovery of ‘digital electronic devices’ [9].
- Write impartial test reports with details of how digital data was processed and/or recovered [9].
- Provide new personnel with training and guidance.

LAW ENFORCEMENT OFFICER

Law enforcement officer must be a lawyer with knowledge of general computer Skills.

- All the cybercrime laws must be known by the official.
- The officer must know how to write an appropriate warrant for searching and seizing of computers[2].

CASE INVESTIGATOR

- Accountable for the day-to-day functioning of the case, which will involve interaction within and outside the laboratory.
- The Investigator must be certified from the authorized organization.

LABORATORY TECHNICIANS

The Laboratory Technicians may not be a technical forensic expert, but a qualified cybercrime and computer forensic investigator They are the person who acts as a link or connection with the outside world and other agencies. The type of job that a laboratory technician normally performs includes underlying knowledge that is tacitly embedded in the logic of the device or process being used.

- A laboratory technician has a skill level that allows them to confidently and effectively perform a set of basic laboratory tasks well with regard to defined standards, procedures and metrics[7].
- These technician roles are performed in support of tasks that require higher levels of expertise or cognitive understanding[7].

In addition to the above facts, laboratory manager must recruit staff with enough academic qualifications and experiences, to provide them with the basic principles for work in the Forensic Laboratory and ensure that they are honest, frank and ethical in their personal and professional life. Staff should also have adequate experience to carry out their tasks.

Knowledge of software and hardware, including operating systems and file types and deductive reasoning, are required.

3.1.1. TRAINING REQUIREMENTS

IT and communications industries are both growing at near exponential levels, driven at a similar pace by new technologies, devices and systems. This strong growth has a huge effect for Computer forensics practitioners to be continuously trained. The lab manager must provide instruction in forensic science principles and detailed information in accordance to the demands of the forensic laboratory. The staff also need to maintain a record of the training that they have completed including the handling, preservation and integrity of the evidence their technical training for investigative and computer skills updating Prior to analyzes Investigations, appropriate preparation needs to be conducted in the methods, procedures and basic resources to be used[11]. A robust training program must be established for all analysts and researchers to provide the forensic team with sufficient generic and tool-specific certification to demonstrate their skill level[11]. The laboratory personnel must be adequately trained to do their job[5]. The following are minimum requirements for laboratory staff readiness

- Computer hardware.
- Networking basics
- An understanding of the relevant legal processes[7].
- General computer forensic knowledge[5].
- Forensic software-specific training (e.g. FTK, EnCase) Legal training concerning computer crime legislation enforced in various countries, search warrants, court evidence, and assessment of appropriate jurisdiction law while investigating a case[5].

It is crucial to ensure that the recruiting and personnel selection are accurate and that investment is worthwhile in the proper mix of staff. Note, the staff must work and function as a team, even in a stressful high pressure environment as well as acquiring and learning the right skills. From the outset, it is worth considering all steps to inspire and retain employees, because of the considerable effort and funding in recruiting, education and training, as the skills and qualifications that they have are limited and there is an overall shortage of skilled and experienced staff available.

While setting budgets, it should be taken into consideration that training is an ongoing process and not a one-time event. The laboratory must operate effectively and continue to develop its staff to ensure it is reliable and meet the demands it raises. The staff will have to operate effectively and develop their skills continuously. In this sense, they must have access to an ongoing training curriculum that takes into account technical advances and the improvements in the available tools. It would be costly, but must be embraced as failure to maintain employee training's currency would lead to disillusioned staff who are not properly skilled to perform their duties and inevitably the laboratory's failure to fulfill its role.

3.2. Hardware Requirements For The Computer Forensics Lab

Here in this section is about the Hardware Specifications for the Computer Forensics laboratory. In the business cause we already defined the scope of the computer forensic lab we proposed and it is focused on one peculiar niche such as computer forensics. The recommendations for forensic computer system hardware are as follows. A variety of hardware tools for laboratory operations are necessary. Another thing to keep in mind is that the technology is changing at an alarming rate thus In a very short time, any purchase may therefore become obsolete[6].The task's speed depends heavily on purchased hardware processing power. In essence, a dollar saved at the buying point can reach tens of thousands of dollars losses and delays that have been lost over the lifetime of the system. It is therefore necessary to use the fastest system available when setting up a laboratory and to review its output on a timely, typically quarterly basis.

Specifications For A Forensic Workstation

The number of forensic workstations required depends usually on the number of laboratory analysts. Here in this we have proposed to have four workstations. These four workstations need to connect to the internal network and Virtual machines are recommended on workstations. Digital machines can deliver several additional features but also additional networking options for a diverse test environment. The workstations would allow them to work on individual cases simultaneously and have access to the common devices and resources. Here's a high-level outline of what equipment a workstation requires to do forensic work properly.

Workstation Hardware	Description
Motherboard and Processor	A Pentium IV dual core processor with “hyper threading” (3.2+ GHz) or “AMD Athlon” 5000+ processor. You should strongly consider purchasing a “64-bit processor”[7].
Hard disk	As high-speed as possible.
RAM	DDR3 ECC 12GB.as much as possible. At least 4 gigabytes for virtualization.
CPU	The fastest money can buy(Depends on the budget); preferably with multiple processors. Preferably ‘64-bit”.
Peripherals	For high-speed text printing or black-and-white images a laser printer is recommended. For color images, we suggest either a color laser printer or a high quality inkjet printer [7].
Monitor	two 20” monitors
DVD/CD-RW/ DVD writer.	
Extra power cords, PCI expansion slots.	Two or three
Network equipment	switch, router, Two serial ports

In addition to above mention equipment two “256GB SSD”, two “3TB HD”, “webcam”, “headset”, “flash memory readers”, “Firewall”, “HD connection”, “Blu-ray recorder”, and four “3TB SATA II HD” are needed[1].

Other considerations

1. **Power Supply-:** A modular power supply of at least 400 watts is required. For exact power requirements, consult your motherboard and processor guides.

2. **Server Considerations**-: A number of computers are needed including a large storage network server (configured for regular hard disk removal) for handling documents and cases, saving distinct software resources and managing one-off hardware specialist. For example, devices like Rimage CD generators, TopPro floppy disk reading devices, printers are included in the hardware that must be controlled[9].

3. **Network Considerations**-:
    - Router and switch to connect forensic workstations to the storage server in the lab[5].
    - Internet network; the internal lab network should be separated. Require a firewall, a switch and a router (the three components can be combined in one device)[5].
    - “Networking cables”[5].

    Best practice is to have a single cable, switch and router network [5].This Laboratory network will allow all Laboratory devices to communicate in secure environments and to connect to the existing corporate network infrastructure and the Internet through secure ports and protocols. Depending on the equipment you want to implement and the cable installation costs, installing a laboratory-specific network can be carried out relatively cheap[5].

4. **Monitor-:** One “21-inch monitor” and “one 19-inch monitor” (preferable are “two 21-inch monitors”). LCD monitors are also preferable because less room is used and less heat is generated. Any of the newer displays provide “DVI data”.

5. **Hard Drives-:** “One Serial ATA hard drive” per operating system (that is, one for Win2 K, one for Linux, etc.). We suggest a total of “two 160 + gigabyte hard drives” for the forensic drives. For performance purposes, the hard disks should be “Serial ATA”[9].

6. **Devices -:** Biometric, handheld, multimeric, multifunctional and compact buying of DCs, scanners, printers, video camera, DVD printers.

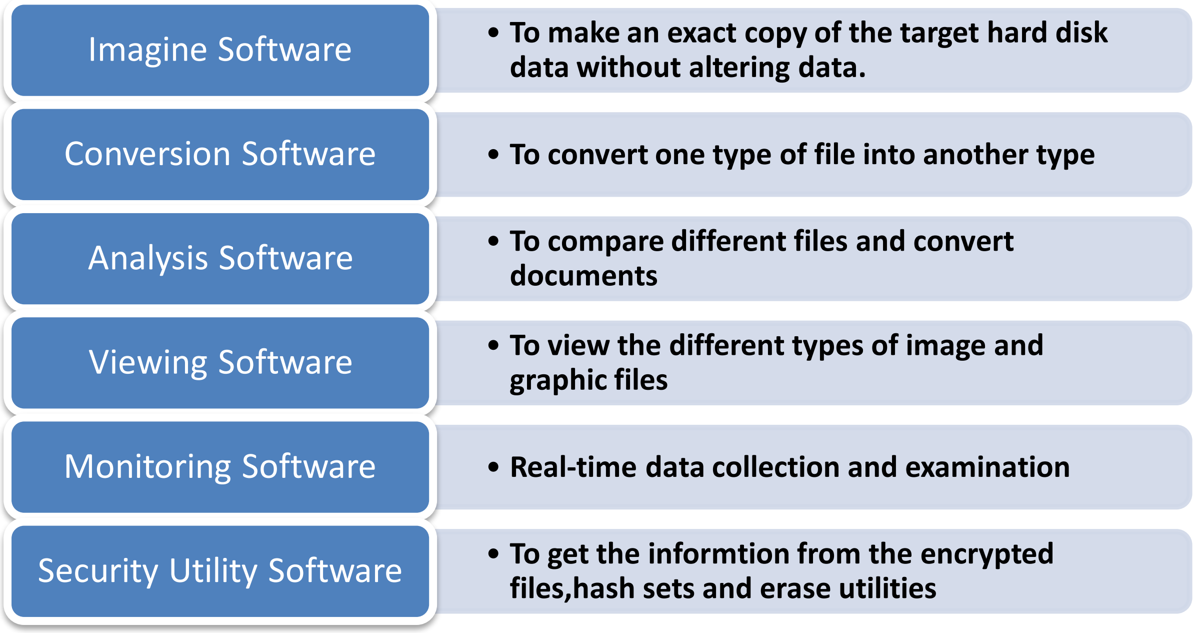
7. **Disk Imaging Stations**-:Computer-based imaging stations will provide hardwires and access connectors for common types of disk. For example, they must be able to connect both 2.5-inch and 3.5-inch disk profiles IDE (“PATA & SATA”), and SCSI (1, 2, 3, UW, U160, U320) as an absolute minimum, as well as FireWire and high-speed USB caddies[7].

8. **Additional Considerations-:** There is a persistent need to get “forensic bridges” (write blockers), forensic duplicators (imaging tools), data wiping/sanitation devices, media, cables, converters, and specialized media readers of various types, For experimental and multidisc acquisition purposes (e.g. SIMs, flash memory, buttons or hand tools like Philips and flathead, socket wrench, small flashlight) and other material, other than hard disks, and for the compilation of facts[3]. Naturally, a wide range of cables, adapters, conventional instrument kits and advanced tool kits are needed for the work on a number of evidence objects subject to the hardware and physical premises. However, this is a continuous process and funds must periodically be allocated for the acquisition of new equipment as it reaches the public arena[3].

3.3. Software Requirements for the Computer Forensics Lab

First, it is important to evaluate the operating systems for the operation of a drive that requires the same operating system as the operating system of the suspect to establish the same conditions. A range of operating systems are useful to have. The following are the lists: “Windows 98, Windows ME, Windows Home and Media Center, Windows XP Pro, Windows 2000 Professional, Windows 2003 Server, Linux”. Another essential fact is to define which type of OSs and applications are examined and then make purchases that suit them. Be aware that the more you spend on a forensic software package the more functionality and flexibility you can achieve. The field of computer forensic research uses instruments that allow practitioners to effectively and efficiently perform their tasks. In this segment will address some of the most widely used "Software devices" and why they are used.

Computer forensic lab should have the following basic software:



Imagine Software	• To make an exact copy of the target hard disk data without altering data.
Conversion Software	• To convert one type of file into another type
Analysis Software	• To compare different files and convert documents
Viewing Software	• To view the different types of image and graphic files
Monitoring Software	• Real-time data collection and examination
Security Utility Software	• To get the informtion from the encrypted files,hash sets and erase utilities

3.3.1. Imagine software

Choosing the right imaging tool is very important when performing computer forensics Investigations. Computer forensic imaging techniques or tools have no standard conformity.

Forensic examiners will never explicitly inspect the original media confiscated, except on a imaged hard drive. A forensic imaging tool is needed to create copies of the suspect data confiscated. Functionality of drive imaging helps the investigator to build and restore image drive files that are a bit-by-bit copy of a partition or disk or volume. Drive imaging is important to secure a precise copy of a storage device, so that it can be used without compromising the integrity of the original data for forensic analysis. On the other hand, an image file can be restored to the system disk[12].

Name	Description	Features
A. **R-Drive Image**	• Unique, powerful drive image software[13]. • It creates "disk *images*": files that contain exact, byte-by-byte, copies of hard drives, partitions, or logical disks[1]. Such images may be stored in any location: other hard disks or various removable media, such as CD-R(W) and DVD discs, "Iomega Zip" or :Jazz disks", including "network drives"[14].	• An entire disk can be copied directly to another disk. Data from these images can be recovered on original disks, on partitions or even in a free space on the drive at any time. • can connect the image as a read-only virtual drive and view and copy the contents. • The integrity of an image can be checked. • A built-in planner can start disk activities automatically at scheduled times.. • Support for backup sets[14]. • Can use for data duplication[14]. • Image files can be password-protected and comments can be included
B. **P2 explorer Pro**	forensic image mounting tool designed to help investigators manage and examine evidence. With P2 explorer, Once mounted, can explore the contents of the image using Windows Explorer or using forensic analysis tool[15]. Because images mount as physical disks, able to view the "deleted data", "slack", and "unallocated space" of the image[15].	• Mounts Paraben's Forensic Replicator images (PFR)[15]. • Mounts compressed & encrypted "PFR images"[15]. • Mounts "SMART images", Mounts "EnCase images" (up to v6). • Mounts WinImage non compressed images[15]. • Write-protection for preserving evidence[15]. • MD5 checksum verification[15]. • Supports both logical and physical images types[15].
C. **AccuBurn-R(CD DVD Inspector**	• •Make identical copies of photographs with a CD / DVD inspector. It supports all disk types and sizes[16].	• The accuracy of written data is checked. • Errors will be corrected automatically. • No network restrictions. Files existing anywhere on a network can be written to a CD[16].
D. **Flash Retriever Forensic Edition**	• Professional tool can produce reports, reports to HTML, CSV or printed for analysis, recovery and documentation on flash based media[17].	• Complete imaging in raw format of flash devices. It can be imported into all important forensic tools. In Flash Retriever Forensic Version, a raw image captured with any device may also be used[17]. • Use with "Encase E01 image files".

	• Support for multimedia. Examine several devices or image files in the same session simultaneously.

One thing to keep in mind about disk imaging is that if the copy is not as accurate as the original, the analysis can be incorrect or incomplete, resulting in unaddressed cases. New technologies and improved imaging methods have been invented from time to time. it really belongs to us to use adequate resources, particularly in the event of an emergency. [13].

3.3.2. FILE CONVERSION SOFTWARE

Name	Description	Features
A. FileMerlin	• Accurately converts word processing, “spreadsheet”, “presentation” and “data base” files between a very wide range of file formats. Widely regarded as the premier document conversion product[7].	• High accuracy and completeness of conversion. • Converts almost every file format that is popular. • Flexibility to name and placing converted files, including folder structure replication. [5]. • Preserves document logic and functionality, revision markings, tracked changes, etc.[6].
B. SnowBatch	• Conversion software for image conversion which converts large batches of files from one format to more common readable formats such as JPEG, TIFF or PDF.	• Allows you to delete partially converted files from the output and to view the deleted filenames in the log.
C. Zamzar	• Transform your albums, images, pictures and documents to various formats. Zamzar supports conversion between a wide variety of different file formats[18].	• convert between various compressed file formats[18]. • Document formats include: “csv, doc, docx, odp, ods, odt, pdf, ppt, pptx, PS, pub, rtf, wp”[18]. • d, wps, xls, xlsx[18]. • Image formats include: bmp, gif, jpg, pcx, png, tga, tiff, wbmp[18]. • Generate PDF document[18]. • URL to PDF.

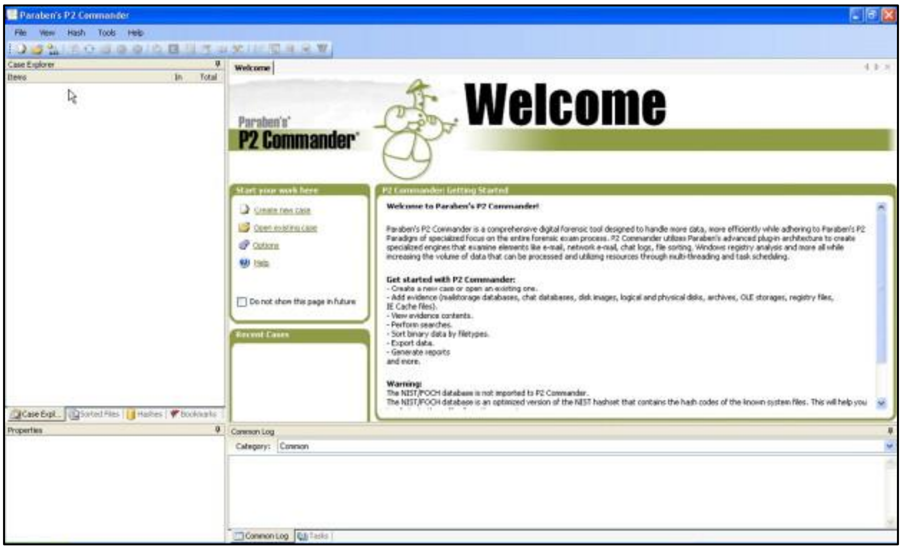
3.3.3. FILE VIEWER SOFTWARE

Name	Description	Features
File Viewer	• Free Windows utility for displaying any image. It displays over 150 of the most common file formats, including text files, tablets, PDFs, audio and video files[19].	• supports a large number of audio and video formats[18]. • Offer batch conversion. • Inspect contents of unfamiliar file types[18]. • View file metadata[18].
Quick View Plus(11 Standard Edition)	• Allows to natively display electronic stored information for the ultimate in legal tasks in almost any format.	• Metadata Extraction[20]. • Viewing Microsoft Word documents with tracked changes and hidden text.

3.3.4. ANALYSIS SOFTWARE

A. P2 Commander

P2 Commander is a court proven advanced emails and chat log review For examiners that need cost-effective, dependable digital analysis in computer forensic, which is designed to process large volumes in fast and efficient way.[21].



Welcome to Paraben's P2 Commander!

Paraben's P2 Commander is a comprehensive digital forensic tool designed to handle more data, more efficiently while adhering to Paraben's P2 Paradigm of specialized focus on the entire forensic exam process. P2 Commander utilizes Paraben's advanced plug-in architecture to create specialized engines that examine elements like e-mail, network e-mail, chat logs, file sorting, Windows registry analysis and more all while increasing the volume of data that can be processed and utilizing resources through multi-threading and task scheduling.

Get started with P2 Commander:
- Create a new case or open an existing one.
- Add evidence (mailstorage databases, chat databases, disk images, logical and physical disks, archives, OLE storages, registry files, IE Cache files).
- View evidence contents.
- Perform searches.
- Sort binary data by filetypes.
- Export data.
- Generate reports
and more.

Warning:
The NIST/FOCH database is not imported to P2 Commander.
The NIST/FOCH database is an optimized version of the NIST hashset that contains the hash codes of the known system files. This will help you

Investigators who use P2 Commander are assured they have documented, defended and presented their evidence in well-laid reports. P2 Commander focuses exclusively on the deep analytical level of e-mail, chat logs, internet history and different systems. It supports many industry standard forensics image and drive image formats. It also supports other file conversion and export functions. [21].

➢ **Specialized Email Analysis**[22]**.** E-mail history is one of the most pervasive places to find digital data on computers. P2 Commander has the ability to process millions of messages, including analysis of email attachments from private or corporate archives. Whether you are looking for easy single user emails like. “Pst files’ or “complex network email archives” with hundreds of gigabytes of messages, deep-level email test engines from P2 Commander that enable you to analyze emails, retrieve emails and sort them.P2 Commander goes further with built-in capabilities to analyze and recover deleted email, including deleted email from single file email archives[22].

- **Specialized Chat Analysis**[22]. It's not just a passing phase to chat online. More and more people are Continuing to communicate through chat. And that means loads of digital evidence. As an examiner, you need a specialized tool to perform a thorough analysis of chat logs. The Paraben's Chat Examiner is another advanced built-in component and P2 Commander feature that adds one more efficient toolkit system. If your case has ICQ, Yahoo, MSN, Trillian, Skype, Hello, or Miranda, you can deal with anything[22].

- **Specialized Registry Analysis**[22]. P2 Commander's data triage function saves you time by analyzing system and registry files and automatically parses out important data regarding the installed system , software, USB use and more[22].

- **Specialized Internet File Analysis**[21]. Internet Explorer, Firefox, and Chrome research engines are specialized analysis engines which allow investigators to work collaboratively on the Internet. The internet files are not going beyond P2 Commander from photos, web pages, history, cookies and more.. From images, to web pages, to history, to cookies and more, internet files won't get past P2 Commander[21].

- **Specialized Pornography Detection**[21]. Scan each image for possible pornographic content on a case by case basis. To over eleven different algorithms you can save time on your case to determine everything from skin color, body shapes and backgrounds with the illicit image detection capabilities in P2 Commander.

FEATURES

- Network folders and folders stored on the “CD/DVD disc” can be mounted as file system evidence[21].
- Availability of the feature, ability to open “vmdk split image” by selecting any part of it: now, you don't need to look through part numbers to find out where to start[21].
- Added the ability to export e-mail data to mounted Forensic Containers[21].
- Addressed potential export issues with large volume of search results data.
- Improved processing of Exchange 2010 email mail stores[21].
- Improved overall performance and stability

B. DriveSpy

DriveSpy is a forensic DOS-based tool which is designed to emulate and extend DOS ability to meet forensic needs . The logging capabilities of this business tool are a beneficial feature. Can configure DriveSpy to record how evidence is conducted and how every keystroke have made is logged. These are written into a log file and can later be used to include in a report what actions you have taken to acquire information. Can configure DriveSpy to document how the acquisition of evidence is conducted, Create -disk -to disk copy(support large disk drives)

- Create MD5 Hash for a drive, partition or selected files[23].
- Collect slack and unallocated space[23].
- Select files based on name, extension or attributes[23].

C. Paraben's SIM Card seizure

SIM Card Seizure from Paraben is a forensic analysis tool to acquire and examine data from a SIM card. Used by worldwide forensic experts. Card Seizure cannot only analyze card data, but also retrieve data that have been deleted, such as SMS/Text messages, check hash values of data integrity, and produce a full data report on the card that preserves information that is collected.

Fully data acquisition of the SIM Card included features. Recovers deleted email / text messages. PIN / PUK code management. Recovers text / SMS messages deleted. Control of PIN / PUK code. Reporting options for full html. Works with SIM card readers that are compliant with PC / SC. A compatible SIM card reader is part of the software. The entire catalog system with data is also given in a tree-view presentation through SIM Card Seizure. In addition, delete SMS data can be retrieved by unallocated region review as long as new data is not over-written.[24].

D. CD/DVD Inspector

"CD-R, CD-RW" and all types of "DVD media", including the "HD DVD "and "blu-rays", are a professional software for intensive analysis and extraction of data.

FEATURES

- New automatic collection of physical media to an image file and then processing the image file[25].
- Reader for CD / DVD is independent of any other application. There is no need for additional software for drag & drop disks.

- CD / DVD Inspection supports picture styles explicitly (i.e .. video,. bmp,.gif, .jpeg,.png,.tiff). Moreover, more than 125 raw (camera specific) digital camera (RAW) formats are supported .

E. Video Indexer

leading professional applications to capture images from video files. Extract single video frames to use for forensic analysis as well as to search wide catalogs of images. No matter how you want, Fast Video Indexer can help you easily and accurately capture still images of your videos and save them as JPEG or BMP.

Features

- Face detection
- Celebrity identification
- Account-based face identification
- Scene segmentation
- Shot detection

3.3.5. MONITORING SOFTWARE

Name	Description	Features
Device Seizure	• Physical phone data dumps can often be identified with deleted data and user data, such as text messages and images. Device Seizure was specifically designed from the ground up as a serious professional forensic tool that provided valuable and accepted evidence in numerous court cases.[26].	• The Following Data Can Be Acquired SMS History (Text Messages),Deleted SMS (Text Messages),Phonebook (In the memory of the phone and on the SIM card),Call History, Received Calls,Dialled Numbers, Missed calls, Call Dates & Durations,Datebook,Scheduler,Calendar. To-Do List, Filesystem (physical memory dumps),“System Files”, “Multimedia Files” (Images, Videos, etc.),Java Files, “Deleted Data”,”Quicknotes”,”GPS” Waypoints, Tracks, “Routes”, etc RAM/ROM[26].
DP2C	• A data triage and an imagery tool with which data is collected from a wide range of devices. This USB-based tool can be used by forensics or unskilled	• Auto-search scans can scan a chat log drive. • Advanced filtering and searching. • Comprehensive reporting features[28].

	Investigators to forensically soundly collect targeted data from a system [27].	• Quick Scan uses registry entries and system files to quickly target the “E-mail databases”, “Chat databases”, “Browser data”, ‘My Documents’ folder, Recently used files[28].
ThumbsDisplay	• ThumbsDisplay is a tool for examining and reporting on the contents of Thumbs. dB files used by Windows[29].	• Shows all thumbnail file: thumbs. dB, thumbcache_idx.db, thumbcache_32.db etc[29]. • Displays all thumbnail images with original file name and timestamp[29]. • Prints individual image and copies to the clipboard for inclusion in a document[29]. • Displays thumbnail in three sizes: 96x96 (original) 150x150 or 200x200[29].
Email Detective	• Controls the use of email on the corporate network, monitors all emails sent and received via the corporate mail server[30]. Mail Detective enables organizations to safeguard sensitive information, improve work discipline and reduce the time spent on personal emailing through corporate mail[30].	• Monitor and analyze incoming and outgoing emails[30]. • Trace information leaks and prevent them [30]. • Control personal/business email ratio[30]. • Evaluate employee’s email traffic[30]. • Receive periodic reports in “HTML”, “PDF” or Excel formats[30]. • Use with any popular email servers[30].

3.3.6. COMPUTER FORENSIC SOFTWARE

I. Data Lifter

A toolkit with a collection of nine devices for the investigation of forensics. The services listed in the data lifer include:

- Disk2File
- Image Linker
- File Extractor Pro
- Internet History Viewer
- Email Retriever
- Screen Capture
- FTK Imager
- PingTrace route/WHOIS tools
- Link fle Viewer

II. X-Ways Forensics

X-Ways Forensics is an advanced computer forensics work environment. X-Ways Forensics is more effective to use after a while compared to its rivals; far from being greedy for money it typically runs faster, discovers missing files and search hits that the competitors will miss.

FEATURES

- Disk cloning and imaging[1].
- Ability to read partitioning and file system structures inside raw (.dd) image files, ISO, VHD and VMDK image[1].
- Complete access to “disks”, “RAIDs”, and images more than 2 TB in size (more than 232 sectors) with sector sizes up to 8 KB[1].
- Automatic identification of lost/deleted partitions[1].
- Access to logical memory of running processes[1].
- Various techniques for data recovery, fast lightning and powerful file carving [1].
- Hard disk cleansing to produce forensically sterile media[1].
- Collect slack field, free space, space between pieces, and generical text from discs and images [1].
- Automated activity logging (audit logs)[1].
- ensure data authenticity with Write protection.

- Special identification of suspicious extended attributes ($EA) in NTFS, as used for example by Regin[1].
- Ability to collect Internet Explorer history and browser cache index.dat records that are floating around in free space or slack space in a virtual single file[1].
- Hard disk cleansing to produce forensically sterile media[1].
- Various data recovery techniques, lightning fast and powerful file carving[1].

III. LiveWire Investigator

Allows investigators to conduct live operating computers and servers on demand forensic examination. A broad range of applications for timely incident responses is provided by LiveWire Investigator. This is the main tool for responding to incidents, vulnerability, compliance audits and criminal investigations. No pre-installed software deployed on target computers is needed for LiveWire. Investigators can now collect information from all over the world (requires credential authentication) easily and quickly on live running target systems. Examine live computer systems easily and inconspicuously to enable vulnerabilities to be examined, suspect machines to collect evidence directly and enterprise-wide malware scans.

FEATURES

- Simultaneous enterprise wide discovery and triage[31].
- Physical memory imaging[31].
- Application and process state discovery[31].
- Windows service discovery, Active port mapping[31].
- Windows log discovery and analysis[31].
- Remote screenshots, File system blueprinting, Installed software cataloging, High assurance time stamped audit trail, Single User License[31].

As a research laboratory, whose performance is always reviewed and challenged, must be careful to ensure that any software license that use or keep in the laboratory is legitimate and up-to-date. Today technology is evolving at speed never witnessed before. Up-gradation and updates in both hardware systems and software capabilities have become a norm.

3.4. FLOOR PLAN FOR THE COMPUTER FORENSIC LAB

The first critical aspect is the location of the site and its inherent security, which must be balanced and in the development of computer forensic capabilities is the construction of a computer laboratory. Like in other areas of forensic analysis, the allocation of forensically comfortable private spaces is extremely important. Investigators should attempt to identify (and articulate) a safe environment for the investigators, equipment and evidence. You need a location to provide adequate space for your forensic staff, work areas, evidence storage, documentation, and equipment and tool storage Configuring. Once a location has been chosen, the floor plan of the lab begins. There are several important design issues to consider, including workstation location, work benches, power outlets, network ports, cabinets and storage rooms which are subject to the budget, the amount of floor space available and the amount of computers that are able to be allocated to each computer investigator. Here in this suggested Mid-size lab typically those in a private business:

- Have more workstations
- Should have at least two exists, for safety reasons
- Cubicles or separate offices should be part of the layout to reinforce confidentiality.
- Have a separate Evidence storage room
- Workbench
- Conference room
- Office room

Workspace

In the whole building, the forensic laboratory consists of different laboratories. Such specific labs are commonly known as laboratory units or sections. These include functional areas, facilities and appliances, which should be regarded when designing a layout to remind designers of the needs. Numerous of the mentioned products. The individual design needs of a computer for deep by 48 inches wide. Many of the items listed. Processing spaces with a forensic workstation, a controlled workstation, peripherals and printer are available. It should be approximately 30 cm deep by 60 cm wide or large enough to accommodate the printer, two monitors, case notes and an area of writing surface.
The following are considerations for the common space[1]:

- Containers should be included for Evidence Storage Room, extra hardware and software and computer systems that are not evidence[1].
- At a minimum, the workbench of the lab should equal approximately half the total square footage for the Investigators.
- Drawer safes are ideal for hard drives and other small peripherals storage. The cupboards should be locked separately on each drawer for single use.
- Make sure the space is not designed so that computer monitors face windows that can cause privacy problems or eye tiredness due to the brightness..

Shows below one layout for a laboratory and encompasses space for all of these functions. This would be adequate for a reasonably sized, computer forensics laboratory.

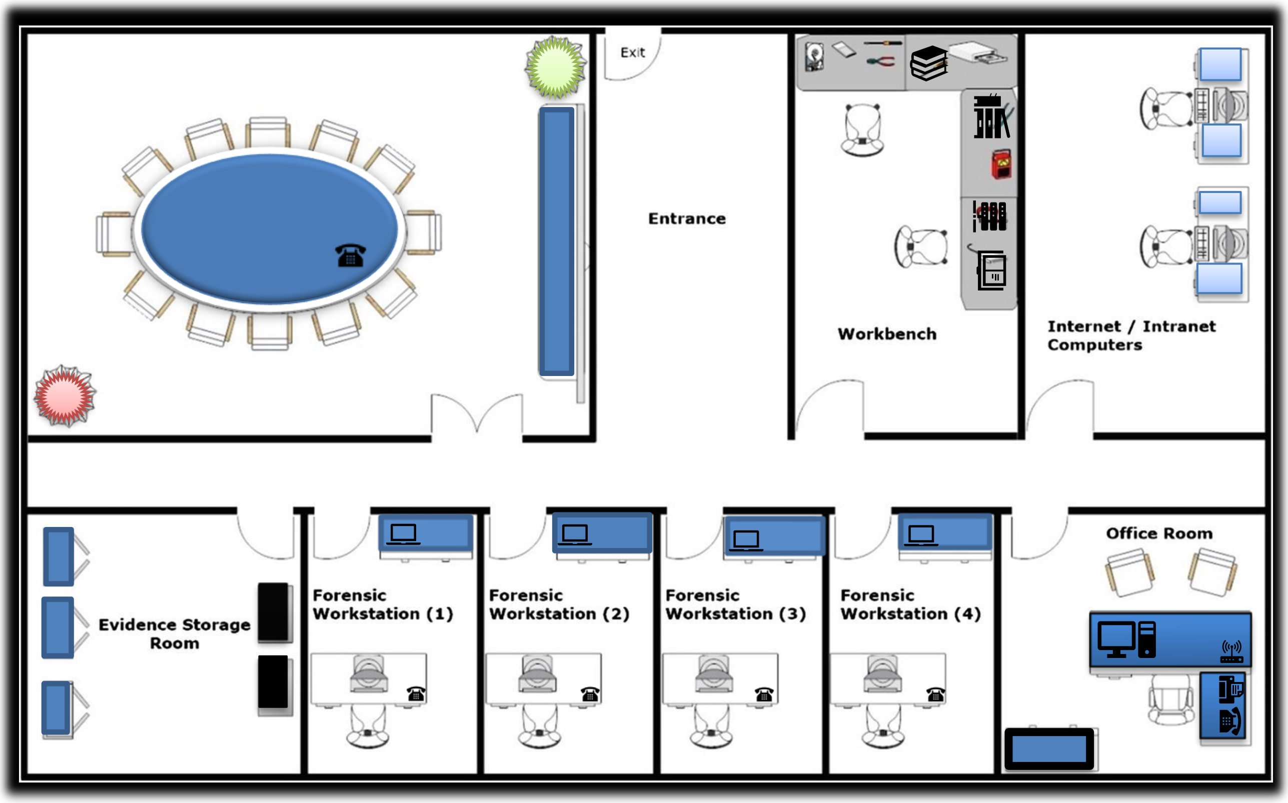


Figure 1 FLOOR PLAN OF THE LABORATORY

3.5. ADDITIONAL REQUIRNMENTS

3.5.1. Security Controls

Security is a topic of great concern in our world and it should not be overlooked when implementing your lab[32]. Next indentation is to obtain a laboratory accreditation, that will be an important topic. Security takes many forms and physical security and data security are the two most relevant for the lab. Data security has been mentioned briefly before and is about maintaining digital information. The processes and produces of the laboratory are safe. Information protection involves securing the data for its storage medium[32], securing data during network-wide transport, auditing the access of this data[32], limiting designated individuals' access to these data, and ensuring data integrity.

Physical security is securing your physical environment[32]. An essential part of physical security strategy must be the identifier of secure areas. Physical security involves the restriction on physical access to the lab and evidence items(allow only for authorized individuals), the installation of door security measures, implementing of man traps, records/log of all individuals accessing secure zones and implementing video surveillance where appropriate. Where necessary, physical security is a matter of concern. Be sure to remember the areas in which network and storage devices are stored when defining your secured areas. If access is made to these areas, it can compromise your data and the entire network infrastructure.

3.5.2.Environmental controls

Regulating laboratory environment can be a vital element that do not want to ignore or overlook .Whenever possible, it is highly recommended to enforce temperature and humidity tests. Use the necessary materials to build the laboratory in addition to those controls, including anti-static floors and countertops and enough lighting for the laboratory and individual workstations[7]. One final point is to address is power. Plan appropriately to have adequate power, conditioned power and emergency power. Large-scale building UPS systems are preferred but they are expensive and likely to only be used if the laboratory is installed in a far broader deployment. See rack-mounted UPS devices for your network and standalone UPS devices for your workstations, to a minimum.

- The lab must be well organized and clean. It must have healthy climate in terms of temperature, low humidity, and pure air[5].
- Good lighting in the entire lab and in each individual forensic workstation room[5].

3.5.3.Auditing a Forensic Lab

Audit should include reviews on the following components and procedures of the facility to ensure proper implementation of policies and audits:

- Evidence container logs
- Doors and Door locks[2].
- Ceiling ,floor, roof and exterior walls of the lab[2].
- At the end of every workday, secure any evidence that’s not being processed in a forensic workstation[2].
- Review visitor logs to see whether they’re being used properly[2].

3.5.4. Maintenance

Recognize your laboratory a new home. If well managed and properly maintained, it will be your lifetime, but you'll face major difficulties if you leave the windows open, let the appliances fall apart and ignore the leaking roof. It’s a must ensure that your lab is properly looked after by upgrading and maintaining the equipment, implementing new software when required, adhering to policies and retaining employee skills through a potent training program. At the end of the day, your success will be determined not by your sophisticated software applications and awesome hardware devices, but by the people who use them.

All hardware should be reviewed on an annual basis with the main forensic workstations having a review every six months[7]. Technology advances rapidly for instance, current quad core CPUs are now available that were not 12 months ago, and eight core CPUs are emerging. This type of advance in hardware can have significant operational impacts, namely the faster processing of tasks, which could result in reduced operational timelines[7]. A simple replacement or upgrade of a CPU may see as much as a 50- to 100-percent improvement in processing power[7]. At the end of a three-year cycle or the termination of the contract, all computer equipment should be removed. Hardware repair costs are now greatly diminished by the purchase of faster equipment. Often problems arise with the supplies of replacements for products outside their warranty, such as RAM or film. The warranty period is usually for a reason — that is, the engineers and risk analysts of manufacturers have determined that the risk of a device failure has increased to an unacceptable level since then.

4. FINANCIAL PLAN

Financial planning requires a strategic or long-term sustainability focus. In order to remain up-to-date with the technologies, it is critical for the equipment in a Computer forensic laboratory to periodically be updated. Avoiding this problem involves diligent long-term planning, The company is not subject to long-term strategic plans for the replacement and This involves decisions to tackle the resources of the laboratory and the resulting movement of capital within the organization. Costs should take account of factors such as the time taken to establish and enforce policies and procedures, the discovery and procurement and installation of equipment (software / hardware) and the construction of a facility, Salary pay, training and qualification for the staff.[33]. This is the cost of buying and receiving the accommodation and renovating the equipment and software. These are the 'one-off' expenses for purchasing and installing the systems and equipment.

The cost of training is not just the crude expense of training. The overall cost of training shall also include the cost of replacing the person who receives the training, travel allowance, accommodation, food and other costs, if necessary. Furthermore, as a result of not being able to perform their usual duties during training, it is impossible not to affect the lost company or operational capacity. These concerns also need to be taken into account when planning and Budgeting.

A Three-year budgetary estimate of revenues and costs, excluding taxes, with a commentary on the assumptions underlying the projections is provided. in the following Budget Deployment needs to Include Mainly:

TIME SPAN – 2020/6/20 – 2023/6/22

COSTS IN($)	INITIAL	POST LAUNCH
❖ Laboratory Equipment	(32,000)	10,000
❖ Software	12,000	9,000
❖ Training	13,000	6,000
❖ Staffing	12,000(Depend)	Depend(3000)
❖ Miscellaneous budget needs	10,000	5000
❖ Operational cost consideration (Emergency repair, Preventative maintenance, Routine maintenance, Technology renewal/upgrades)	12,000	5000
TOTAL	91,000	38,000

5. REFERENCES

[1] باقری. ح and فرهاد. خ, “No Titleتعیین رخسارههای الکتریکی بر اساس رخسارههای رسوبی و گونههای سنگی به کمک روشهای خوشهبندی با استفاده از نگارهای چاه پیمایی و اطلاعات مغزه حفاری در سازندهای کنگان و دالان، میدان گازی پارس جنوبی.”

[2] باقری. ح and فرهاد. خ, *No Title*□□□□ □□ □□□□□□□□□ □□□□□□□□□□ □□□□□ □□ □□□□□□□□□ □□□□□□□ □□□ □□ □□□□ □□□□□□□□ □ □□□□□□ □□□□□□□□□□ □□ □□□□□□ □□□□ □□□□□□□□ □ □□□□□□□ □□□ □□□□□□□□ □□ □□□□□□□□ □□□□□ □□□□ □□□□ □□□□□ □□□□□□□ □ □□□□□□ □□□□□□□□□□. .

[3] “Forensic Laboratories : Handbook for Facility Forensic Laboratories : Planning , Design ,” *Juv. Justice*.

[4] Brandon Bass, “No Title,” *https://study.com/academy/lesson/the-digital-forensics-lab-requirements-design.html*, p. 2, 2020.

[5] N. A. Hassan, *Digital Forensics Basics*. .

[6] M. Britz, *Computer Forensics and cyber crime: An introduction*. 2013.

[7] C. V. Andrew Jones, *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility*, Revised. Butterworth-Heinemann, 2011, 2011.

[8] S. Abdalla, S. Hazem, and S. Hashem, “Teams Responsibilities for Digital Forensic Process,” *Proc. Conf. Digit. Forensics, Secur. Law*, no. c, pp. 95–114, 2007.

[9] F. A. Division, “Digital Forensic Laboratory Section Guidelines.”

[10] C. C. Chigozie-Okwum, D. O. Michael, and S. G. Ugboaja, “Computer forensics investigation; implications for improved cyber security in Nigeria,” *AFRREV STECH An Int. J. Sci. Technol.*, vol. 6, no. 1, p. 59, 2017.

[11] D. Watson, A. Jones, D. Watson, and A. Jones, “Setting up the Forensic Laboratory,” *Digit. Forensics Process. Proced.*, pp. 25–37, Jan. 2013.

[12] RAJ CHANDEL, “How to Create Forensics Image of PC using R-Drive Image,” *How to Creat. Forensics Image PC using R-Drive Image*, vol. 1, 2015.

[13] Sans, “InfoSec Reading Room An Overview of Disk Imaging Tool in Computer tu , A ho ll r igh ts,” 2001.

[14] U. Manual, “R-Drive Image,” no. c, 2020.

[15] insectraforensics, “Paraben P2 eXplorer Pro,” *Paraben P2 Explor. Pro*, vol. 3, no. 2020, p. 3, 2019.

[16] infinadyne, “AccurBurn-R,” *Bus. Rec. reports...Digital Photogr. files...Internet downloads*, 2020.

[17] infinadyne, “Flash Retriever Forensic.” .

[18] “Zamzar,” pp. 13–15, 2020.

[19] O. Streaming, E. Plain, M. Office, and M. Project, “File viewer.”

[20] Q. View, “Quick View,” 1995.

[21] “Paraben P2 Commander v2,” *Paraben P2 Command. v2*, vol. 1, p. 1, 2019.

[22] T. H. E. Solution and F. T. H. E. Evidence, “P2 COMMANDS THE ATTENTION.”

[23] N. B. Micah Solomon, Diane Barrett, “Computer Forensics JumpStart,” *Launch Your Career Comput. Forensics—Quickly Eff.*, vol. 308, no. 2006, p. 309, 2008.

[24] Paraban, “SIM Card Seizure,” *SIM Card Seizure*, vol. 2, no. 2020, p. 1, 2019.

[25] infinadyne, “CD/DVD Inspector,” *CD/DVD Insp.*, vol. 1, 2020.

[26] 2020 Intellisphere Ltd, “Mobile Phone Device Seizure,” *Mob. Phone Device Seizure*, no. 2020, 2019.

[27] AdvanceIT and T. M. T. Work, “DP2C – Deployable P2 Commander,” *http://advanceit.biz/home/products/forensic-tools/forensic-hardware/dp2c/*, vol. 1, no. 1019, 2017.

[28] Paraben Corporation, “DP2C-Drive Triage and Imaging,” *insectra*, vol. 3, no. 2019, p. 4, 2018.

[29] EC-Council, “Course Hero,” 2019, p. 1142.

[30] ADV soft, “AN EFFECTIVE LOG ANALYZER AND REPORTING TOOL FOR MICROSOFT® EXCHANGE SERVER AND MDAEMON EMAIL SERVERS,” *MAILDETECTIVE*, vol. 2, no. 2019, p. 3, 2018.

[31] Forensicswiki, “LiveWire Investigator,” *LiveWire Investig.*

[32] T. In and T. Issue, “Capturing Known Print Standards,” vol. 14, no. 1, 2016.

[33] P. B. Tarigan, *済無No Title No Title*, vol. 53, no. 9. 2013.

6. APPENDICES

6.1.1. Books

Below is list of books you can refer to learn more about computer forensics;

- *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As an Expert Technical Witness*, by F.C. Smith and R.G. Bace (Addison Wesley Professional, 2003)
- Handbook of Digital Evidence: Reliable Forensic Computing, by P. Sommer (Springer Verlag, 2006)
- Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition, by A. Marcella and D. Menendez (Auerbach, 2007)
- Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors, by A. Reyes, R. Brittson, K. O'Shea, et al. (Syngress, 2007)

6.1.2. Journals

https://www.journals.elsevier.com/forensic-science-international-digital-investigation

https://www.elsevier.com/journals/digital-investigation/1742-2876?generatepdf=true

https://dblp.org/db/journals/ijde/index

http://ijofcs.org/policies-peer.html

https://books.google.lk/books?id=F5IU7XXKwCQC&pg=PA271&lpg=PA271&dq=Small+Scale+Digital+Device+Forensics+Journal:+www.ssddfj.org/%5C&source=bl&ots=7C-WTARpJr&sig=ACfU3U1FzGh-v7y67MfTUcsSQqPl5D2iXg&hl=en&sa=X&ved=2ahUKEwjGiPa-25TpAhWZV30KHdSSA1sQ6AEwAXoECAoQAQ#v=onepage&q=Small%20Scale%20Digital%20Device%20Forensics%20Journal%3A%20www.ssddfj.org%2F%5C&f=false

6.1.3. Forums and Blogs

https://niiconsulting.com/checkmate/

http://www.datatriage.com/blog/

http://www.datatriage.com/blog/?s=interrogatories

https://leahycenterblog.champlain.edu/