This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2017 conference.

Design and Implementation of Low Cost Digital Forensic Laboratory for University

Md. Masud Parvez,[1] Syed Akhter Hossain[2] and Shaikh Muhammad Rizwan Ali[3]
[1,3]Bangladesh University of Professionals, Mirpur 12, Dhaka-1216, Bangladesh
[2]Daffodil International University, 102 Shukrabad, Dhaka-1207, Bangladesh
Email: [1]masud.parvez5@gmail.com [2]aktarhossain@daffodilvarsity.edu.bd [3]ripirami@yahoo.com

***Abstract*—At the present growth of Internet and the remarkable enhancement of information technology, the growing rate of Cyber Crime is very high. In order to safeguard and protect digital assets, every higher education institutions are badly in need of infrastructure to identify possible threats. This has raised demand of quality digital Forensic expertise. Besides, universities are required to offer courses on Digital Forensics and attempting to create qualified Digital Forensic experts. But the digital forensic courses in the university have always been a big challenge, particularly when the basic component of the course is hands-on labs and the course is entirely hands-on LAB oriented. Teaching Digital Forensic is based on theoretical and analytical aspects together with huge number of research and laboratory work. The Digital Forensic LAB lies with the software and hardware which are more expensive. Establishing a Digital Forensic Lab is an expensive affair in the University. This paper is proposed to build a low cost Digital Forensics Laboratory for the university that facilitate Digital Forensic course and hands-on exercise for their students and help the growing needs of the Digital Forensic experts for the future.**

***Index Terms*—Cyber Crime, Digital Forensic, Digital Forensic Lab, Digital Assets, Digital Forensic Education, Evidence, Forensic Expertise, Security Threat.**

I. Introduction

In the recent past there has been a tremendous boost in the information technology in educational sector. Most of the academic and administrative activities of the university have been digitized. Computers and internet are reaching all areas and the IT literacy rate is gradually increasing.

All the activities of the university are conducted online such as teaching, research, e-learning, e-library, email, student evaluation, Smart ID card, student database, ERP. Due to the improved variety of IT and computer relevant crime and cyber-crimes revealed in university, within the previously few years digital 'forensics' has become a key area of cyber-crime investigation [1].

Increased cyber-crime in University needs to be investigated properly. For that reason, Digital Forensic has now become a big issue. Digital 'forensics' is a field of science for collecting, analyzing, and presenting legal evidence that is found from digital devices. The main phases of the digital Forensic are shown in the Fig. 1.

Increased cybercrime, organization is planning to post incident investigation and developed to policy procedure and guideline for digital forensic investigation. This is called digital forensic readiness. The demand of the digital forensic expert is growing very high. That's the reason university are thinking for introducing different digital forensic courses. The courses are needs to be Lab based to provide fully hands on experience and digital forensic Lab is the basic component of these courses. Usually digital forensic Lab is a highly expensive and big budget lab. That's the big challenges to introduce digital forensic course for any university.

Fig. 1. Digital forensic phase.

The goals of this paper propose to build a low cost digital forensic laboratory for university which included a low cost forensic workstation, cost effective forensic hardware accessories and open source or education edition forensic software.

The remainder of the paper is organized as follows: in section two describes the purpose of the digital forensic laboratory that including a survey report. The section three describes the requirements of digital forensic laboratory including physical requirements and Lab room design. Section four and five describe the hardware requirement and software requirements of Forensic Laboratory and has also proposed solutions for low cost hardware and software. The section six has the compression between expensive and low cost Digital Forensic Lab. The final section concludes the research work.

II. Digital Forensics Laboratory

There are several benefits of Digital Forensic Lab that assist hands on exercise for university students and other security professionals. Students may use the Forensic lab in learning the following topics, just to bring up some:

(a) Hands on Digital Forensic Study.
(b) LAB for cybercrime and Investigation
(c) LAB for Computer and Mobile devices forensic
(d) LAB for Digital Forensic professionals training
(e) LAB for FTK software professionals training courses
(f) LAB for Encase software professionals training courses.

A survey has been done for identifying the interest of the university to setup low cost digital forensic lab. Ten universities of Bangladesh are taken part of this survey. The survey

978-1-5090-4442-9/17/$31.00 ©2017 IEEE

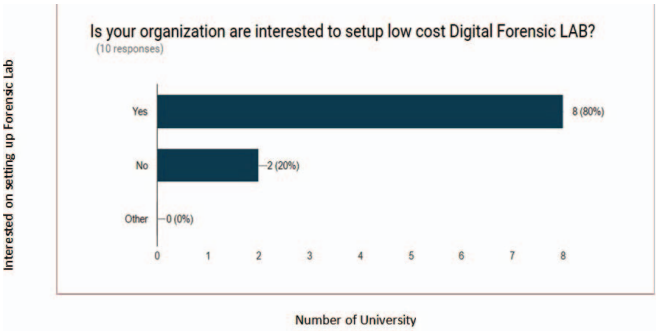

Fig. 2. Survey report for low cost digital lab.

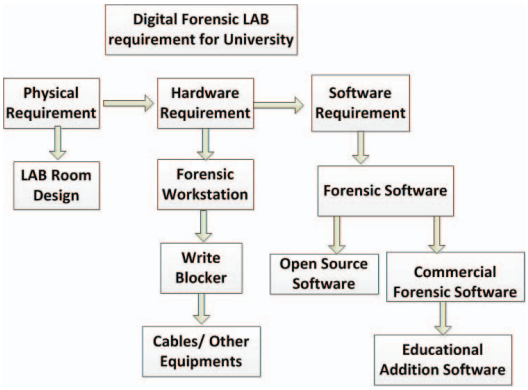

Fig. 3. Requirements of digital forensic laboratory.

question is "Is your organization is interested to setup low cost Digital Forensic LAB?" The result of this survey is shown in the Fig. 2.

III. The Requirements of the Digital Forensic Laboratory

To build a Digital forensic Laboratory need to maintain some steps and setups. The common requirements to setup digital forensic laboratory are physical, Hardware and software. Fig. 3 shows the requirement flowchart of Digital Forensic Laboratory.

A. Physical Requirements

Digital forensics laboratories come in a variety of configurations and preparations. Students have performed their most of the investigation process at the lab. Hence, The Lab is the secure physical location that preserves the evidence with integrity of evidence data and experimental data. The minimum actual physical requirements are [2]:

a. Mid-size room.
b. Door access
c. CCTV with DVR and Monitor
d. Projector with screen
e. Secure evidence room
f. Two containers for evidence
g. Four digital forensics workstations.
h. One Desktop PC with internet connection

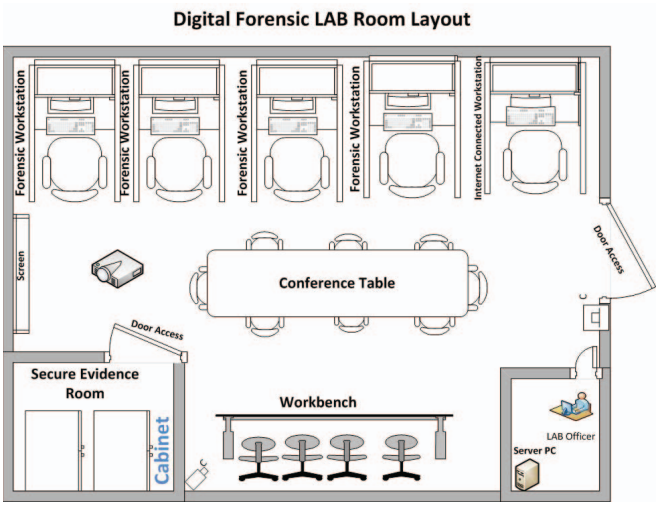

Fig. 4. Digital forensic lab room layout.

i. One server PC
j. One workbench
k. Conference table with chairs.
l. Communications options: Limited internet connectivity

B. Proposed Lab Room Layout

To build a digital forensic lab, a room design is very essential. In Digital forensic LAB we consider a mid-size room. Fig. 4 shows the Digital Forensic Lab room layout.

IV. Hardware Requirement

A. Digital Forensics Workstation

The major hardware requirement of Digital Forensic Lab is digital forensic workstation. Forensic workstation is the one which support all prerequisites for running different Digital Forensic Software. Forensic workstation should be selected according to the budget. Different organization used high cost special purpose forensic workstation for big budget Forensic Lab which has integrated Write blocker. In our research we have proposed customized low cost Digital forensic workstation for Forensic LAB which meets the requirement of all Digital forensic Software's.

B. High Cost Special Purpose Forensic Workstation

A special purpose forensic workstation which is builds only for forensic work and integrated with forensic processing platform that is capable of managing critical forensic investigation. The cost of this special workstation is very high. Some of special types of forensic workstation are integrated with Write blocker. The following write blocker typically is integrated with the forensic workstation [1]. The most common special types of workstation is FRED (**F**orensic **R**ecovery of **E**vidence **D**evice).

Specification

- 23 $3/4''$ High, 8 $3/8''$ Wide, 25 $1/4''$ Deep—80 lbs
- Intel Core i7-5820k CPU (Hex Core Processor), 3.3 GHz, 10 MB Intel Smart Cache, 5 GT/s DMI

TABLE I
SPECIFICATION FOR CUSTOMIZED FORENSIC WORKSTATION.

#	Types	Specification
1	OS	Windows 10 standard or Windows server 16 and Linux
2	CPU	I7-5820k Hex core 3.3 GHz
3	Motherboard	Gigabyte GA-X99-UD5
4	RAM	32 GB DDR4 2133 MHz
5	OS drive	SSD (256 GB)
6	Data drive	HDD (2 TB)
7	DVD	DVD-RW
8	Power supply	ATX 1200 W power supply
9	Video captured card	NVIDIA GeForce GT 710 GPU
10	Monitor	22″ Wide screen LED monitor with built-in Speakers
11	Casing (4 drive bays)	Mid tower workstation chassis

- 32 GB (4×8 GB)PC3-17000 DDR4 2133 MHz Memory
- 1×256 GB Solid State SATA III Drive—OS Drive
- 1×128 GB Solid State SATA III Drive—Temp/Cache/DB Drive
- 1×2.0 TB 7200 RPM SATA III Hard Drive—Data Drive installed in Hot Swap Bay1
- Nvidia GTX 750Ti 2 GB 128 bit DDR5 PCI-Express Video Card with 1 VGA (D-Dub), 1 HDMI, and 2 DVI ports—supports up 4 displays
- 22″ Widescreen Monitor.

C. Proposed Low Cost Customized Forensic Workstation

Integrated Forensic workstations are very costly for educational institute. The budget is not much for a lab so we can consider customize workstation. The customize workstation is not more expensive for university and its meet the forensic high end software requirements. But there is no integrated Hardware write blocker that's why we need to buy extra hardware write blocker. Table I shows the specification of customized workstation for low cost lab.

D. Write Blocker

In the Digital Forensic lab write blocker is very essential equipment's. A device that's only permits read-only access of storage devices like HDD, flash drive without compromising the integrity of the data. To maintain chain of custody of evidence write blocker need to be used properly. Two types of write blocker were used for Forensic Lab. One is hardware based write blocker and another is software based write blocker. Some hardware and software write blocker are very costly. Both cost effective hardware based write blocker and some open source software based write blocker has been proposed for low cost forensic lab.

E. Other Hardware and Cables

In the Digital Forensic Lab number of hardware peripherals and extension cables are required for connecting different devices and hardware's. These cables are very essentials to build the Lab. Table II shows the list of other hardware's and cables.

TABLE II
OTHER HARDWARE'S AND CABLES.

Other hardware's
1. Pen drive 32 GB
2. Pen drive 16 GB
3. Card reader
4. USB DVD writer
5. External HDD
6. 1 TB SATA drive
7. 150 GB SDD
8. 32 GB flash drive
9. Computer hand tools
10. Anti-static mats
11. Anti-static gloves

Cables
1. Power cords
2. USB3 cable 3 matter
3. Two USB A to mini 5 pin cables
4. HDMI cable
5. Mini HDMI cable
6. HDMI to VGA converter
7. VGA to HDMI converter
8. Serial to USB converter
9. DVI cable
10. Two eSATA cable
11. 12″ Micro SATA cable (long SATA cables)
12. One 8″ IDE interface cable
13. One 2″ IDE interface cable
14. Two SATA interface cable
15. Two SCSI-3 interface cable
16. One 1.8″ hard drive adapter
17. One 2.5″ hard drive adapter
18. One ZIF hard drive adapter
19. One micro SATA adapter
20. Pin hard drive Molex power plug to a Serial ATA power plug
21. SATA hard drive power cable
22. Twin serial ATA sata hard drive power cable for 2 drives
23. SATA and SATA HDD power extension cable
24. HDD power cable royalty free stock
25. SATA hard drive power cable

V. FORENSIC SOFTWARE

Digital forensic commercial tools are very costly for any university with an average cost of $5000–$5500 per license for any software and every year renewal is needed. That's the reason it's very difficult to maintain this Lab with limited budget, it is unrealistic to spend $60,000 to purchase commercial tools for one course [3]. For University it's a big challenge to build a big budget Forensic Lab and update it is each and every year. This paper has to propose commercial forensic software's educational version which is cost effective for university and think many open source and freeware forensics tools will perform similar or near to commercial forensic software. The main goal for this Lab would be provide students with the practical based forensic knowledge so that if they learn many open source and educational version forensic software they are likely to develop ability to work as a Forensic expert. The most popular tools for Computer Forensic investigation are Encase, FTK incase of Mobile Forensic investigation popular tools are Oxygen Forensic, Cellebrite and Paraben. There are some other open source Digital Forensic popular tools which are Sleuth Kit (Autopsy), ProDiscover Forensic Edition for low cost lab this open source tools are most effective.

EnCase introduced an academic program that supports universities students to grow their expertise in digital forensic with hands-on experience. It contains everything a university needs to successfully integrate into their curriculum. The academic Program includes: 12-user academic license, one EnCase Forensic security key for local server and supporting materials for both Teacher and students. That Security key is used in local lab server for licensing [4].

TABLE III
PROPOSED FORENSIC SOFTWARE'S LIST FOR LOW COST LAB.

Most popular digital forensic tools			
#	Tools	Features	License types
1.	Access data forensic Toolkit (FTK) [5]	Create image Registry analysis Password recovery Searching Data carving Reporting	Education edition
2.	EnCase [6]	Acquisition from different devices File recovery Signature analysis Analysis and hash analysis & reporting	Education edition
3.	ProDiscover forensic edition [7]	Deleted file recovery, exam slack space, image capture	Open source
4.	CAINE 7.0 [8]	User friendly four phase digital forensic investigation tools	Open source
5.	Helix [9]	Create image Password recovery Use for cookie viewer, internet history viewer Pictures analysis	Open Source
6.	Sleuth kit (Autophy) [10]	Make timeline of different file activity. Categories different files type, Hash database lookup etc.	Open source
7.	WinHex [11]	Work on disk editor, recovery, clone disk, compare file and encryption technique	Open source

Forensic Toolkit (FTK) is other popular tool from Access Data. It allows your lab to grow its forensic skills as you need to grow. FTK academic program are provide 12-user academic license for university. But one of your teachers needs to be qualified as Access Data Certified Examiner (ACE) [4].

A. Proposed Digital Forensic Sowtware for Low Cost Lab

See Table III.

B. Mobile Forensic

For Mobile Forensic there is very few open source and free version software. The commercial version software's are most costly that's the challenge for including Mobile Forensic for low cost digital forensic Lab. But this paper suggested to communicating different Mobile forensic software companies to introduce education version software for University. A proposal should be given for what the benefit is of the company if they are introducing education version software. The big challenge of those software companies are limited forensic expert so it's a big opportunity to produce more mobile forensic expert (see Table IV).

C. Other Tools for Forensic Lab

See Table V.

TABLE IV
PROPOSE MOBILE FORENSIC SOFTWARE'S LIST.

#	Tool	Feature	License types
1	Oxygen forensic [16]	• Evaluate contacts from several resources and applications also retrieves data	Proposed education edition
2	Cellebrite [17]	• Bypass user locks, recover application data and reveal deleted data. • Calls, SMS, MMS, Media, emails, calendar and contact files • Location information decoded from apps.	Proposed education edition
3	Paraben [18]	• Mobile forensic • Email investigation	Proposed education edition

TABLE V
OTHER OPEN SOURCE SOFTWARE'S LIST FOR LAB.

#	Tools	Feature	License types
1.	Cain abel	Password recovery for Windows	Open source
2.	John the ripper	Password recovery for Windows and Linux	Open source
3.	SAMinside	Password recovery for Windows	Open source
4.	7zip	Compression software	Open source

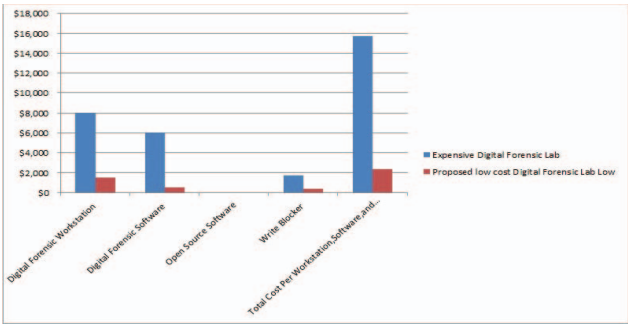

Fig. 5. Digital forensic lab cost compression.

VI. COMPRESSION BETWEEN EXPENSIVE AND LOW COST DIGITAL FORENSIC LAB

The Fig. 5 shows that the cost compression between expensive Lab and low cost proposed Lab for per Forensic Workstation, Software and Write blocker. The regular forensic Lab is more expensive as compare to proposed Forensic Lab and which affordable to the university.

CONCLUSION

A good number of universities introduce cyber security as their undergraduate and graduate level degree and digital forensic is the major course to fulfill the high demand of market. The Digital forensic course is fully hands-on and massive numbers of experimental work are needed. This paper explores several amounts of requirements and proposal to be able to build cost- effective Digital Forensic Laboratory for

University. The hardware and software requirements for laboratory will be different based on budget range. For affordable laboratory we have considered customize workstation, cost effective write blocker, education edition software's and open source software's to fulfill the requirements of Digital Forensic Laboratory.

REFERENCES

[1] Kasun De Zoysa, Keerthi Goonathillake, and Ravith Botejue, "Developing a digital forensic framework for a third world country," in *International Conference on Cybercrime Forensics Education and Training*, Canterbury Christ Church University, UK, 2008.

[2] Antonis Mouhtaropoulos, Chang-Tsun Li, and Marthie Grobler, "Digital Forensic Readiness: Are We There Yet?" *Journal of International Commercial Law and Technology*, vol. 9, no. 3, 2014.

[3] Hongmei Chi, Edward L. Jones, Christy Chatmon, and Deidre Evans, "Design and implementation of digital forensics labs," Department of Computer and Information Science, Florida A&M University, 1333 Wahnish Way, Tallahassee FL 32307-5100, USA.

[4] Mousa Al Falayleh, "Building a digital forensic laboratory for an educational institute," in *the International Conference on Computing, Networking and Digital Technologies*, 2012, pp. 285–293.

[5] Access Data, 'Forensic Toolkit' (n.d) [Online]. Available: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk. [Accessed: 10-Oct-2016].

[6] Guidancesoftware.com, 'Encase Forensic' (n.d) [Online]. Available: https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r. [Accessed: 11-Oct-2016].

[7] Accurate Reliable competent, 'Pro discover forensic edition', (n.d) [Online]. Available: http://www.arcgroupny.com/products/prodiscover-incident-response/. [Accessed: 11-Oct-2016].

[8] Caine, 'Computer Forensic Linux Live destrubution', (n.d) [Online]. Available: http://www.caine-live.net/. [Accessed: 15-Oct-2016].

[9] E-fense Carpe Datum, 'Helix', (n.d) [Online]. Available: http://www.e-fense.com/products.php. [Accessed: 01-Nov- 2016].

[10] Sleuth Kit, 'Open Source Digital Forensics', (n.d) [Online]. Available: http://www.sleuthkit.org/. [Accessed: 03-Nov-2016].

[11] X-Ways, 'WinHex Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor', (n.d) [Online]. Available: https://www.x-ways.net. [Accessed: 05-Dec-2016].

[12] Timothy M. Vidas, David A. Branch, and Alex Nicoll, "STEALing lab support for digital forensics education," in *the Hawaii International Conference on System Sciences*, 2008.

[13] Michael Mount and Adam Denmark, *Forensic laboratories: facility planning, design, construction, and moving*, National Institute of Standards and Technology Department of Commerce, Ed. US, 1998.

[14] Forensic Computer, 'Forensic Workstation', (n.d) [Online]. Available http://www.forensiccomputers.com/workstations/ [Accessed:11-Dec2016].

[15] FRED (Forensic Recovery of Evidence Device)', Forensic Workstation', (n.d) [Online]. Available: http://www.digitalintelligence.com/cart/ComputerForensicsProducts/ [Accessed: 11-Oct-2016].

[16] Oxygen-forensic-detective, (n.d) [Online]. Available: http://www.oxygen-forensic.com/en/. [Accessed: 30-Dec-2016].

[17] Celebrate, 'Mobile Forensic', (n.d) [Online]. Available: http://www.cellebrite.com/. [Accessed: 30-Dec-2016].

[18] Paraben, 'Mobile Forensic', (n.d) [Online]. Available: https://www.paraben.com/. [Accessed: 30-Dec-2016].