



Digital Forensic Lab

How Long We Have to Wait?

Mohammad Javed Morshed Chowdhury

Recent rise of cyber crime and hacktivism have been a serious concern for the overall law and enforcement situation in Bangladesh. We have experienced hacking of skype account of an honorable judge in recent past. Mobile phone voice scandal is also a very hot topics for new months in cyber space in Bangladesh. 19 district websites, popularly known as ‘Zela Tothobatayan’, have been hacked by Indian hackers in 2011. Last but not the least website of the law enforcement agencies including RAB and Bangladesh Police has been compromised.

Other than the website hacking, fake facebook account and MMS scandal are also a growing concern. Women specially unmarried women are the main victim of these heinous activities. Some teenagers have committed suicide due to this kind of activities.

Another concern is digital commerce. Bangladesh is now entering into the e-commerce arena. Without proper cyber security mechanism, investigation infrastructure and manpower it could be a nightmare for Bangladesh. This is the right time to think about the capacity building of the concern authority in terms of cyber security.

There are two phases of cyber security. In first phase we try to ensure the security of our digital assets by applying security mechanism. In second phase if our security mechanism does not work or compromised then we investigate the incident and try to identify the criminal and take him to law. And finally we solve the security problem that has been exploited. In this procedures investigation plays an important role to indentify the misdeed and criminal. It works almost same like physical forensic lab, it investigate the affected digital equipments.

What is digital forensic?

Digital forensics is currently one of the fastest growing laboratory sections in the crime lab. Most laboratories without

digital forensics capabilities in their old facilities are either remodeling existing spaces or planning space for digital forensics in their new facilities.

There appear to be two forensic disciplines pertaining to digital media, ‘digital forensics’ and ‘cyber forensics,’ which have not yet been formally separated and defined. These terms have been used as labels for these disciplines, yet not consistently, since much of the literature on this subject uses these terms

- * Digital video devices such as digital cameras, digital video surveillance devices, scanners, plotters, facsimile machines, and photocopiers.
- * Combination audio/video devices such as CDs, DVDs, floppy discs, and USB drives.
- * Communication devices such as cell phones, Blackberries, and iPhones.

Cyber forensics is the forensic investigation of unlawful security



Digital evidence in an investigation.

interchangeably between the two disciplines. For purposes of this article, these two disciplines will be generally defined and labeled as follows:

Digital forensics is the forensic investigation of devices capable of storing digital data, the purpose of which is to extract the digital data from such devices in order to assist in the investigation and prosecution of crime, and/or to be used as evidence in civil court cases. Examples of these devices include (but are not necessarily limited to):

- * Computers and their digital components.
- * Digital audio devices such as MP3 players, iPods, voice recognition devices, and audio surveillance devices.

breaches in computer network systems. This would include the investigation of cyber worms and viruses, and hacking into secure networks, whether they are government, military, or private industry networks. Cyber examinations also include cases pertaining to classified information, espionage, and digital investigative support for the war on terrorism. Pursuit of persons responsible for child pornography, narcotics transactions, internet fraud, and any other illegal activities involving cyber space fall under the purview of cyber forensics. When these investigations uncover those responsible for unlawful cyber activities the violator’s computer hardware, software, and any device containing digital information becomes digital forensics evidence. ▶

Digital Forensics Comes of Age

Law enforcement agencies are taking help from digital forensic lab and court has given legitimacy very recently. But the law enforcement community was aware of these facilities from 1960s and 1970s. In western countries, the investigation divisions in police departments began examining computers for digital data, and within a short period some crime labs began establishing a separate laboratory section for this purpose. At that time the facility design requirements for computer crimes included not much more than electronics laboratory bench space and a room for the storage of computer hardware exemplars and references.

Over the next two decades advances in digital technology led to a seemingly endless array of new digital devices which became available to business houses, the government, and the general public. All of these devices had the potential of becoming the subject of examinations as forensic evidence. The computer crimes section gradually became known as the digital forensics section and evolved to include several specialized spaces within this section, each with its own specialized design requirements.

Although many police agencies have limited digital forensic capabilities, the current trend is for digital forensics to become an integral and increasingly vital section of the crime labs, thereby keeping this investigative discipline under the forensic umbrella.

Facility Design Requirements: General

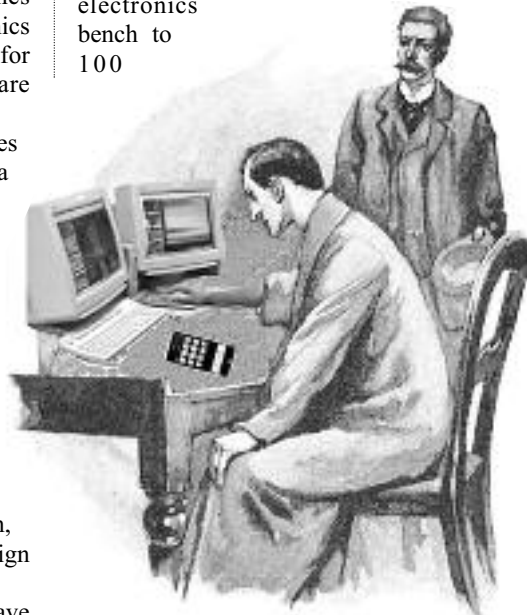
A fully equipped digital forensics laboratory contains numerous specialty spaces, each with its own unique and specific architectural/ engineering design issues that must be addressed. However, there are some general design requirements that are applicable for all of the spaces within the digital forensics unit. General requirements include laboratory casework, finishes, mechanical systems and electrical systems.

Facility Design Requirements: Specific Spaces

As a minimum, the ideal digital forensics laboratory should contain the following individual, special purpose rooms:

- * General examination
- * Audio examination
- * Video examination
- * Radio frequency shielded examination

General Examination : This is the portion of the digital forensics laboratory where each examiner will be provided his or her individual examination workstation. Multiple workstations should typically be laid out in an open laboratory design. A reasonable size for an individual workstation ranges from 15 linear feet of electronics bench to 100



square feet of bench space in a U-shaped configuration.

Audio Examination : 'An audio recording is subject to a number of possible distortions and artifacts. For example, the persistence of sound, due to multiple reflections from various surfaces in a room, causes temporal and spectral smearing of the recorded sound. The examination of digital audio media necessitates an acoustically isolated space to allow the examiner to concentrate on the evidence without any interference from outside noise.

Video Examination : With the increasing ease in digitally manipulating photo images, there is a significant need for mathematical and computational algorithms to aid forensic examiners to detect tampering in digital media. Video itself has always been a ground breaking weapon against crime, but now even poor-quality videos can be enhanced to provide even more valuable data through an extremely powerful, yet cost-effective, toolset for forensic video enhancement.

Radio Frequency Shielded Examination : The world today is increasingly electronic, with electronic devices producing millions of waves and signals permeating the air at any given moment. The electromagnetic waves generated by electronic devices may negatively affect other, similar, electronic devices. Such effects are called Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI). EMI and RFI cause suppression of signals generated internally in a device. It also causes external ambient interference with equipment operation and emissions generated internally that will interfere with equipment operation. Therefore, EMI and RFI are problems in forensic investigations where EMI and RFI can corrupt the digital evidence within a device.

Additional Examination Spaces

Depending on the established procedures, function, and examination policies for the digital forensics section, the following additional functions might be incorporated into the laboratory design:


Computer data recovery, Hard drive repair, Electronics laboratory, Electronics workshop, Biosafety/wet laboratory

Digital Forensic Software/framework

Drive acquisition is a fundamental process in the field of digital forensics, but the acquisition of an entire hard drive must be a forensically sound image that is a flat file bit stream image. Volatile data is extremely valuable evidence that can easily be lost, as it is data that is stored in RAM, a Window's page file, or other repository that is wiped clean when a computer is shutdown. Both of these items need to have their accuracy guaranteed through hashing, which is basically a digital signature from the original hard drive or volatile data that is matched to the exact mirror image backup of that data. If these hashes do not match, the copy of the data is not considered to be a true, forensically sound copy of the original data.

Conclusion

In today's reality, Bangladesh law enforcement agency needs to have a digital forensic lab to better investigate the cyber crime scenario. This will also help the court to deal with the cyber crimes.

[This article is prepared with the help of different online resources]. 

Feedback : jabedmorshed@gmail.com